OS/390 and z/OS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 5, Release 1

Volume 2 of 2

21 January 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS (B)

Page

LIST OF TABLES (B)

Page

SUMMARY OF CHANGES (B)

Changes in this document since the previous release (Version 4, Release 1) in July 2003 are listed below beginning with *Section 8* (see *Volume 1* of the *OS/390 STIG* for changes to all previous sections).

General

Minor wording, grammar, formatting, and typographical changes and corrections are not included in the Summary of Changes.

The major changes to Volumes I and II involved the addition of bullets for the PDIs (Potential Discrepancy Items) identified in the VMS database. These changes were made to keep the OS/390 and z/OS STIG in line with the STIGs published for all other technologies. Additional changes included the creation of new PDIs for breaking apart Roman Numeral PDIs.

The following sections contained in the STIG and not having any PDIs and not referenced in any of the ACP Check Lists have been removed from the body of the STIG and placed in Appendix F for future research and analysis.

IMS/DB/DC
MICS
FDR Fast Dump Restore
ICKDSF
CA Examine
CA Sysview
System Maintenance Software SMP/E

The following sections were removed from the STIG:

9.5	ORACLE	was removed since it was included in the Data Base STIG
15.2	XDC	was removed since it was no longer being used at any of the sites.

Other sections have been renumbered to fill in removed sections.

11.2.2 External Security

Changes were made to add new parameter setting for CA-1 Version 5.3

11.2.6 ACF2

Changes were made to add new parameter setting for CA-1 Version 5.3

11.2.7 RACF

Changes were made to add new parameter setting for CA-1 Version 5.3

11.2.8 TOP SECRET

Changes were made to add new parameter setting for CA-1 Version 5.3

Section 13. Spool Access Software

All the Associated bullets were assigned PDI numbers.

Appendix A. Related Publications

Updates and deletions of publications were made.

Appendix E. Forms

The Acknowledgment of Risk Letter(AORL) was removed from this section and this STIG.

Appendix G. List of Acronyms and Definitions

Made changes and additions as required.

8. TRANSACTION PROCESSORS

8.1 General Considerations

Transaction processor software products provide programmers with the facilities required to develop interactive and on-line applications. These systems may interact with other database management systems. (Refer to *Section 9, Database Management Systems*, for further information.)

To gain access to a transaction processor session, I&A checking is performed. This is a requirement that provides protection against unauthorized access to an on-line system or region.

Consideration should be given to securing resources within the transaction processor environment. Resources (such as files, programs, transactions, storage, etc.) are reviewed for potential security exposures and to prevent unauthorized access.

Some transactions are powerful and offer the potential to breach security. These transactions are generally used to manage and administer the system, or they provide a key function for an interfacing product. Access to transactions of this magnitude are prohibited from general use, and access is only granted to authorized personnel.

Product interfaces installed within transaction processor systems are carefully evaluated for possible security exposures. These interfaces may offer their own internal security, provide the capability to circumvent ACP security controls currently in place, or expose weaknesses in protection.

Many transaction processor products comes with their own internal security. These features are reviewed and analyzed to determine if implementation is warranted. However, ACP security controls are never compromised by any internal security component.

Use the following recommendations when securing access to transaction processor systems:

(1) Control access to software product data sets, and restrict access to system-level support personnel only.

(2) All transaction processor systems in use at DOD sites perform I&A checking during the logon process. I&A validation is performed using the services of the ACP.

(3) Restrict user access to resources within the transaction processor environment to those necessary for users to accomplish their assigned responsibilities. These resources include, but are not limited to, files, programs, transactions, and storage.

(4) Product interfaces (e.g., debugging software, file management tools, Print management products, etc.) are reviewed for potential security exposures and documented. Notify DISA FSO and the vendor of any possible vulnerability resulting from the analysis.

(5) Evaluate transaction processor internal security for possible use, providing it does not replace or compromise existing ACP security controls.

8.2 CICS

Vendor: IBM Corporation

The Customer Information Control System (CICS) allows programmers to develop application code to perform interactive processing, without the cumbersome overhead of writing the terminal control language to support the interactive process. CICS, with the development of flexible, multi-platform information systems and the implementation of easy to use high-level inquiry languages, has evolved into a dynamic medium that can allow a wide community of terminal access to major data systems.

Through the use of OS/390 System Authorization Facility (SAF) to route authorization requests to the ACP, CICS can provide multi-leveled access and resource protection. Implement CICS security management with an approved ACP. Apply the following recommendations to the security implementation for each CICS region defined on a platform:

(1) A unique userid will be associated with each individual CICS region.

- *(ZCIC0040: CAT II) The IAO will ensure that each CICS region is associated with a unique userid and that userid is properly defined.*

(1) A CICS environment may include several data set types required for operation. Typically they are CICS product libraries, which are usually included in the STEPLIB concatenation but may be found in DD DFHRPL. CICS system data sets can be identified with DFH DD statements, other product system data sets, and application program libraries. Restrict *alter* and *update* access to CICS program libraries and all system data sets to systems programmers only. Other access must be documented and approved by the IAO. The site may determine access to application data sets included in the DD DFHRPL and CICS region startup JCL according to need. Ensure that procedures are established; documented, and followed that prevents the introduction of unauthorized or untested application programs into production application systems.

- *(ZCIC0010: CAT II) The IAO will ensure that update and allocate access to CICS program libraries and all system-level data sets is limited to system programmers only, unless a letter justifying access is filed with the IAO.*

(2) The CICS initialization program, DFHSIP, runs in an authorized state. It is typically installed in the SDFHAUTH library. This library is defined to the operating system as APF authorized. Refer to *Section 2.1.2.1, Authorized Program Facility (APF)*, for security control information.

(4) Ensure security is enabled for the region. This will be done by coding the following parameter in either the SIT or the SYSIN startup parameter file for the region:

SEC=YES

- *(ZCIC0030: CAT II) The IAO will ensure that CICS System Initialization Table (SIT) parameter values are specified in accordance with STIG requirements.*

(5) Unique interfaces, designed internally in application-level code to provide enhanced security, should be allowed only as long as the base-level requirements are not circumvented. These interfaces shall be documented and provided to the IAO.

(6) Control terminal access validation to a particular CICS region by parameters associated with a person's userid defined to the ACP. One access validation mechanism may be used for a group of CICS regions that constitute a Multiple Region Option (MRO) environment. However, ensure that access validation is maintained at attach time across all regions.

(7) For non-terminal access (i.e., PLT processing and triggered transaction), ensure that a valid user is identified. This can be accomplished by the definition of a default user. Specify that the default userid for the region is set to a known, specific userid with very few privileges. The default userid for a region will under no circumstances be the same as the region's assigned userid, because this would pose a critical and immediate security risk to the entire domain.

(8) The STIG standard for this userid will be specified as follows, and will be the same for all regions. This will be done by coding the following parameter in either the SIT or the SYSIN startup parameter file for the region:

DFLTUSER=CICSUSER

- *(ZCIC0030: CAT II) The IAO will ensure that CICS System Initialization Table (SIT) parameter values are specified in accordance with STIG requirements.*

The specified value was selected because CICS assigns this userid if none is specified in the region startup parameter list. Specifying this value mitigates the risk of inadvertent omission of the parameter during region startup.

The default userid will be granted the absolute minimum privileges necessary. It should only require the following privileges:

(a) Access to transactions CESF and CESN and the transactions specified in the GMTRAN and GNTRAN parameters for the region

(b) Permission to access the CICS region

- *(ZCIC0041: CAT II) The IAO will ensure that the default CICS user is restricted and properly defined.*

(9) To further ensure that the default userid cannot be inadvertently misused, the default userid will require a surrogate profile. This will be enforced by coding the following parameter in either the SIT or the SYSIN startup parameter file for the region:

XUSER=YES

- *(ZCIC0030: CAT II) The IAO will ensure that CICS System Initialization Table (SIT) parameter values are specified in accordance with STIG requirements.*

(10) Depending on the environment in which application code change control is handled, additional authorization checking may need to be implemented for files, programs, MRO/Inter-Systems Communication (ISC) connections, and other CICS-based resources. A thorough evaluation of the change control process is key to the necessity of implementing other resource verification.

(11) Use ATTACHSEC=IDENTIFY as part of the CICS CONNECTION definition parameters for any ISC/MRO environments. This ensures that userid information is passed across all connections.

(12) Enforce a CICS time-out time limit, which is implemented based on 15 minutes of user inactivity.

- *(ZCIC0042: CAT II) The IAO will ensure that all CICS users have a 15 minute time-out limit specified.*

(13) The CICS multiple sign-on capability may be used in test regions for application development and debugging. This option is only authorized for test and development purposes. The IAO maintains the documentation describing the requirements and the justification for its use. The CICS multiple sign-on capability is not used in production regions.

(14) At a minimum, implement transaction-level checking in all CICS regions. Generally there are three major sources of transactions in a CICS environment:

- CICS-supplied transactions
- COTS-supplied transactions
- GOTS-supplied and site-developed transactions

These three major sources of transactions are described as follows:

(a) CICS-supplied transactions are used in the initialization, operation, and control of a region. These transactions offer the ability to circumvent ACP controls for resources managed under CICS. These transactions can be divided into three categories:

- Category 1 transactions are for CICS internal use only. Restrict access to CICS region userids.

- Category 2 transactions are initiated by a terminal user and are restricted to appropriate personnel.

- Category 3 transactions are exempt from security checking. For performance reasons, each of the ACPs allows trusted transactions to be exempted from security checking. Only transactions that do not present a security exposure (e.g., sign-on/sign-off, menus, etc.) are exempted from security checking.

  Control the following transactions, and restrict appropriately.

Table B-1. CATEGORY 1. TRANSACTIONS FOR CICS INTERNAL USE ONLY (8.2 a)

CATA	CATD	CDBD	CDBF	CDBO	CDBQ	CDTS	CESC	CEX2	CFCL
CFOR	CFQR	CFQS	CFSL	CFTL	CFTS	CGRP	CIOD	CIOF	CIOR
CITS	CLSG	CMTS	COVR	CPLT	CRMD	CRMF	CRSQ	CRSY	CSFR
CSFU	CSGX	CSHA	CSHQ	CSKP	CSNC	CSNE	CSOL	CSPQ	CSQC
CSSX	CSSY	CSTE	CSTP	CSZI	CTSD	CWBG	CWXN	CXCU	CXRE

Table B-2. CATEGORY 2. CICS AND OTHER PRODUCT TRANSACTIONS (8.2 b)

(Must be restricted to Systems Programming staff only unless otherwise noted.)

CAFB	CAFF	CBAM	CDBC	CDBI	CDBM	CDBT	CDFS	CEBR[1]	CECI
CECS	CEDA	CEDB	CEDC	CEDF	CEDX	CEHP	CEHS	CEMT*	CEOT[2]
CESD	CEST	CETR	CIND	CIRP	CMAC	CMSG	CPMI	CREA	CREC
CRPA	CRPC	CRPM	CRTE	CRTX	CSFE	CSGM	CSM1	CSM2	CSM3
CSM5	CSMI	CTIN	CVMI	CWBA	CWBM	CWTO	DSNC		

***** The CEMT transaction can be secured at the command level allowing for a more inclusive authorization. See Paragraph (12) below.

[1] Provide access to Application Development Staff.
[2] Provide access to Operations and Help Desk Staff.

Table B-3. CATEGORY 3. TRANSACTIONS EXEMPT FROM SECURITY CHECKING (TRUSTED TRANSACTIONS) (8.2 c)

CATR	CCIN	CEGN	CEJR	CESF	CESN	CIEP	CLQ2	CLR1	CLR2
CLS1	CLS2	CLS3	CLS4	CMPX	CPSS	CQPI	CQPO	CQRY	CRSR
CSAC	CSCY	CSHR	CSPG	CSPK	CSPP	CSPS	CSRK	CSRS	CSSF
CXRT									

(b) COTS-supplied transactions are used to support and administer vendor products. Some of these transactions may offer the ability to bypass ACP controls for resources managed under CICS. These transactions are considered sensitive and are identified as Category 4 transactions. Category 4 transactions are restricted to systems programming personnel and are minimally described below:

Table B-4. CATEGORY 4. COTS-SUPPLIED SENSITIVE TRANSACTIONS (8.2 d)

(The list is not all-inclusive.)

TRANSACTION	***DESCRIPTION***
ACFM	CA-ACF2 Master Transaction
ACFA	CA-ACF2
ACFT	CA-ACF2
ACUL	CA-ACF2
DBOC	CA-DATACOM
LOOK	CA-LOOK
OMON	OMEGAMON/CICS
TMSU	CA-1
TSEU	CA-TOP SECRET
TSSC	CA-TOP-SECRET

(c) GOTS-supplied and site-developed transactions are written generally to support user applications. These transactions are controlled at the discretion of the site IAO.

Any GOTS-supplied and site-developed transaction that provides the ability to bypass ACP controls for resources managed under CICS are considered sensitive. Access to these transactions will be restricted to a minimum number of authorized personnel and documented with the IAO. Implementation of any sensitive transaction will be subject to the requirements as stated in *Section 2.1.2, Software Integrity***.**

- *(ZCIC0050: CAT II) The IAO will ensure that CICS transactions for internal, terminal user, trusted and sensitive are protected in accordance with the above STIG requirements.*

(15) To facilitate CICS administration, CICS provides the master terminal transaction (CEMT) as well as systems programming interface (SPI) commands. These SPI commands are for managing the CICS system and its resources. SPI commands either retrieve information about the system and its resources, or modify them. These commands provide a command-level equivalent to the function of CEMT and also the trace control transaction (CETR), and an alternative to the CEDA transaction for defining resources. This means that transaction can be written for administering the running CICS system.

These master functions are extremely sensitive, but sensitivity can be diminished with the use XCMD and CMDSEC parameters. This allows application developers and other users partial use of CEMT functions, depending on their job and duty requirements. Use the following specifications:

In the SIT:

XCMD=YES	CICS to perform command security checking
CMDSEC=ASIS	CICS honors the CMDSEC option defined in a transaction's resource definition

In the Transaction resource definition:

CMDSEC=YES	Security checking is to be applied on Systems Programming commands

The use of System Programming Interfaces are justified and evaluated by Security and CICS personnel to ensure CICS region security before access is granted.

8.2.1 ACF2

Every CICS region is secured using the ACF2/CICS sub-product. This allows both I&A processing and the verification of resource access within CICS.

8.2.1.1 ACF2/CICS Security Related System Initialization Parameters

ACF2/CICS initialization is determined by checking for a privilege bit called ACF2CICS in the CICS region logonid. All CICS region logonids will be granted the ACF2CICS privilege. Restrict this privilege only to CICS region logonids.

To prevent privileges granted for one CICS region from applying to another region, assign every CICS region a unique set of the following definitions:

(1) A unique @MUSASS and @MLID macro pair in the ACF2 ACFFDR for each region

- *(ZCICA021: CAT II) The IAO will ensure that each CICS region is associated with a unique @MUSASS and @MLID macro pair in the ACFFDR.*

(2) The CICS region logonid

(3) The ACF2/CICS parameter data set

- *(ZCICA022: CAT II) The IAO will ensure that each CICS region procedure has the ACF2/CICS parameter dataset specified.*

(4) The four default region logonids wherever applicable:

(a) Terminal
(b) Non-terminal
(c) Implicitly signed-on terminal
(d) MRO

(5) The eight CICSKEY resource types wherever applicable:

(a) File
(b) Program
(c) Transaction
(d) Transient data
(e) Temporary storage
(f) PSB
(g) MRO System In
(h) MRO System Out

(6) Any USERKEY resource type required by the site

(7) CICS region sign-on authorization flag in the LID record

The ACF2/CICS parameter data set, associated with a given CICS region, controls the security mechanisms in effect for that region. Protect the parameter data set via standard data set rules, and restrict access only to systems and security personnel. Several key ACF2/CICS parameters have the ability, depending on their setting, to corrupt the security posture of the CICS region. To avoid this exposure, code the parameters listed below with the following keywords:

- *(ZCICA011: CAT II) The IAO will ensure that update and allocate access to the ACF2/CICS parameter data set is limited to system programmers and security personnel, unless a letter justifying access is filed with the IAO.*

PARAMETER	KEYWORD(S)	DESCRIPTION
CICSKEY*	OPTION=VALIDATE, TYPE=*ttt*,** RESOURCE=TRANS	The CICSKEY parameter establishes CA-ACF2 CICS control over a CICS resource.
DEFAULT	Terminal= *unique-id* Nonterminal=*unique-id*	Ensures that every CICS task has a valid user identified.
EXIT	MROIN MROOUT	Any MROIN or MROOUT exits are validated and approved by DISA FSO.

PARAMETER	KEYWORD(S)	DESCRIPTION
OPTION	CONSOLE=VALIDATE	Security controls are in effect for transactions being processed at the console.
	DISCONNECT=YES	When the violation limit is reached, disconnects the terminal from CICS and returns it to VTAM.
	MAXVIO=3	Maximum number of security violations allowed.
	MODE=ABORT	Aborts the transaction if access is denied.
	TIMEOUT=5	Number of minutes between each scan for inactive terminals
INHERIT	TDJOB=YES	Batch jobs submitted to an internal reader through extra-partition transient data queues inherit the logonid of the submitting task
SIGNON	ENQSCOPE =NONE***	Multiple sign-on within the same CICS region (*use only with test or development regions*)
	ENQSCOPE=CICS***	Single sign-on within the same CICS region
	QUICK=NO	Disallows quick sign-on format, which enables the user to enter the password in clear text at the same time as the logonid is entered.
	REQUIRE=YES	Specifies that a user must sign-on before executing transactions.
SUSPEND	PASSWORD=YES	Suspends user during sign-on if the password violation count reaches the established threshold.
	RULE=YES	Suspends users during resource validation if the CA-ACF2 violation count reaches the established threshold.
VERIFY	IDLE=YES	Re-verify password after terminal idle time is exceeded.
MRO	TRANSMIT=YES RECEIVE=YES	This assures that logonid inheritance is performed.

**At a minimum, enforce transaction-level protection.*

***The default ACF2/CICS type for transactions is CKC, but is unique for each region, as specified above. An exception would be the situation where regions are grouped together in an MRO environment that may share a common transaction type with that unique MRO environment.*

**** Ensure that users cannot sign on more than once to a production CICS region within single sign-on within the same CICS region a single OS/390 image, or a sysplex.*

- *(ZCICA023: CAT II) The Systems Programmer and IAO will ensure the ACF2/CICS parameters are coded with values specified in the above table.*

- *(ZCIC0041: CAT II) The IAO will ensure that the default CICS user is restricted and properly defined.*

ACF2/CICS uses a combination of SAFELIST and PROTLIST parameters in the ACF2/CICS parameter data set to facilitate resource protection without unduly affecting CICS performance. The SAFELIST specifies resources that are trusted, and for which no validation needs to be performed. The PROTLIST specifies exceptions to the SAFELIST for which validation is still performed. These lists work in conjunction with the CICSKEY and USERKEY parameters discussed above.

Resources specified in the SAFELIST are not masked. All such resources are discretely identified in the SAFELIST.

- *(ZCICA024: CAT II) The Systems Programmer and IAO will ensure the ACF2/CICS parameter SAFELIST are coded with values specified above.*

PROTLIST processing should not be used, as all resources exempt from security validation is discretely specified in a SAFELIST entry. Validate all resources not specified within a SAFELIST parameter through standard resource verification, as specified in the associated CICSKEY or USERKEY parameter.

- *(ZCICA025: CAT II) The Systems Programmer and IAO will ensure the ACF2/CICS parameter PROTLIST is not coded.*

Strictly control the ability to update the SAFELIST and PROTLIST specifications for a CICS region.

8.2.1.2 CICS Region Logonid Controls

Logonid inheritance control is in effect for each CICS region. Under no circumstance will a user's batch job submitted from a CICS region inherit the authority and privileges of the CICS region logonid.

If the CICS region has the requirement to submit jobs on behalf of its users, the CICS region logonid will have the JOBFROM attribute specified.

If the CICS region has the requirement to update information in the ACF2 database on behalf of its users, the CICS region logonid will have the MUSUPDT attribute specified.

All CICS region logonids will have the MUSASS and NO-SMC attributes specified.

Do not grant the NON-CANCEL privilege to a CICS region logonid.

- *(ZCIC0020: CAT II) The IAO will ensure that each CICS region is associated with a unique userid and that userid is properly defined.*

8.2.1.3 CICS User Control

Grant all logonids associated with a CICS region the minimum privileges necessary to accomplish their functions. This applies equally to the region's logonid and to the default logonids associated with the region.

Strictly control CICS default logonids. Grant these logonids the minimum access authorities necessary to perform their functions.

The following ACF2 logonid field and associated value will be specified for all CICS users to include the CICS default user:

IDLE(15)

Number of minutes that must elapse since the last terminal I/O before ACF2 performs password re-verification.

- *(ZCIC0042: CAT II) The IAO will ensure that all CICS users have a 15 minute time-out limit specified.*

8.2.1.4 CICS Transaction Control

Transactions in *Table B-1, Category 1. Transactions for CICS Internal Use Only (Section 8.2, CICS)*, are only for CICS internal use. Access validation to these transactions are performed using the CICS region logonid, not the CICS end-user logonid. Define these transactions with the following specifications:

(1) ACF2 rule(s) restricts access only to CICS region logonids.

(2) CICS transaction resource definitions use RESSEC (NO) and CMDSEC (NO.

Transactions in *Table B-2, Category 2. CICS and Other Product Transactions (Section 8.2, CICS),* have an explicitly defined resource rule restricting them as noted in the table.

Transactions identified in *Table B-3, Category 3. Transactions Exempt from Security Checking (Trusted Transactions) (Section 8.2, CICS)*, are eligible for exemption from validation due to CICS functional requirements. Their exemption is defined by placing them in the ACF2/CICS SAFELIST system initialization parameter using the SAFELIST RESOURCE=TRANS ENTRY=*xxxx* keyword. CICS transaction resource definitions may use RESSEC(NO) and CMDSEC(NO).

Other transactions that execute within CICS and do not run under the authority of a user may also be included in the list. Examples of such transactions may include the OMEGAMON/CICS background task or the task that performs print services. In such cases, these transactions may be added, but, as an example, the transaction that actually initiates the print transaction is protected. All other transactions are validated.

The use of the SAFELIST list should be kept to a minimum. Only transactions that do not present a security exposure (e.g., sign-on/sign-off, menus, etc.) should be included. Transactions for applications and COTS software should be placed in unique resource rules. Where required, multiple resource rules should be created to provide for more granular control and separation of capabilities. For example, for a COTS product that provides administrative, technical support, and user transactions, each of these functional areas would be provided with a separate resource rule to allow the assignment of access based on functional requirements.

The ACF2/CICS master terminal transaction (ACFM) provides the on-line, real-time capability to effect changes to the security environment of the CICS region. Protect the transaction via ACF2 resource rules, and restrict its use to security and Systems staff.

The ACF2/CICS environmental utility transaction (ACFE) provides the capability to examine CICS security-related information. Restrict access to the ACFE transaction only to security staff.

8.2.2 RACF

CICS external security utilizing RACF is accomplished in the manner described in this section. Use the recommendations and guidelines outlined in the following sections to control access to CICS.

8.2.2.1 CICS Security-related System Initialization Parameters

(1) Associate a unique userid with each individual CICS region. If the region is run as a started task, define it to the STARTED resource class with a matching profile. For example:

```
RDEFINE STARTED CICS*.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCCICS) TRUSTED(NO))
```

(2) Specify the following CICS system initialization parameter and associated values for each CICS region:

SECPRFX=YES|NO CICS resource name prefixing

Specify one of the following values:

SECPRFX=YES Prefix resource names with the CICS region userid.

SECPRFX=NO Do not prefix resource names.

SNSCOPE=NONE|CICS|MVSIMAGE|SYSPLEX CICS sign-on scope

Specify one of the following values appropriate for the CICS region configuration. Ensure that users cannot sign on to more than one CICS production region within the scope of a single CICS region, a single OS/390 image, or a *sysplex*:

SNSCOPE=NONE	Multiple sign-on within the same CICS region (*use only with test or development regions*)
SNSCOPE=CICS	Single sign-on within the same CICS region
SNSCOPE=MVSIMAGE	Single sign-on within a set of CICS regions on a OS/390 domain
SNSCOPE=SYSPLEX	Single sign-on within a set of CICS regions within an OS/390 *sysplex*
XTRAN=YES|*ssrr*TRN	Transaction resource class names

Specify one of the following values:

XTRAN=YES	Use the TCICSTRN and GCICSTRN resource class names for transaction security checking.

NOTE: Region identity is maintained between multiple regions regarding resource rule definitions. Therefore, XTRAN=YES may only be used if SECPRFX=YES is specified.

XTRAN=*ssrr*TRN	Use site-defined resource class names for transaction security checking.

NOTE: Refer to *Section 8.2.2, RACF*, for information on defining CICS transaction resource class names.

- *(ZCIC0030: CAT II) The IAO will ensure that CICS System Initialization Table (SIT) parameter values are specified in accordance with STIG requirements.*

(3) Implement CICS transaction security by utilizing two distinct and unique RACF resource classes (i.e., member and grouping) within each CICS region. If several CICS regions are grouped in an MRO environment, it is permissible for those grouped regions to share a common pair of resource classes. Member classes contain a RACF discrete profile for each transaction. Grouping classes contain groups of transactions requiring equal protection under RACF. Ideally, member classes contain no profiles, and all transactions are defined by groups in a grouping class.

Specify the following CICS system initialization parameters and their associated values for each CICS region:

XTRAN=*ssrr*TRN

Resource class names should be similar to the following sample naming standard. Each class name can be in the form of *x*ssrrTRN, *where*:

x - RACF prefixes a letter to the XTRAN= value to build the RACF member and grouping class names. The possible values are as follows:

T - Member class for transaction security
G - Grouping class for transaction security

ss - Two-letter system identifier
rr - Two-letter region identifier

- *(ZCICR021: CAT II) The IAO will ensure that each CICS transaction resource class pair is active.*

(4) MRO partner regions have appropriate profiles in the RACF Facility. Facility class must be active and prevent the binding of unauthorized CICS regions. User authorization is controlled by the ATTACHSEC=IDENTIFY.

8.2.2.2 Propagation Control

Utilize propagation control for each CICS region. Under no circumstance should a user's batch job submitted from a CICS region execute under that CICS region's userid. To prevent this from occurring, define a profile in the PROPCNTL resource class for each CICS region. The following is an example:

RDEFINE PROPCNTL *cics-region-userid*

The PROPCNTL class must be active and *RACLISTed* for this protection to be in effect:

SETROPTS CLASSACT(PROPCNTL) RACLIST(PROPCNTL)

- *(ZCICR041: CAT II) The IAO will ensure that each CICS region userid is defined to the PROPCNTL resource class.*

8.2.2.3 Surrogate Job Submission Controls

Surrogate job submission is used to allow CICS to submit jobs while specifying another userid in the job's JCL. If CICS automatic journal archiving is used, a profile is defined to the SURROGAT resource class using the userid specified in the archive JCL. For example:

RDEFINE SURROGAT *archive-userid*.SUBMIT UACC(NONE)

Permit the CICS region's userid to submit the archive job using the *archive-userid* as the job's execution userid:

PERMIT *archive-userid*.SUBMIT CLASS(SURROGAT) ID(*cics-region-userid*)
ACCESS(READ)

The SURROGAT class must be active and *RACLISTed* for this protection to be in effect:

SETROPTS CLASSACT(SURROGAT) RACLIST(SURROGAT)

NOTE: SURROGAT authority is restricted only to the CICS region userid. Any exceptions are documented describing the requirements and justification for its use.

8.2.2.4 CICS User Controls

(1) All CICS region userids are defined as PROTECTED userids For example:

AU CICSPROD NAME('CICS PROD STC') NOPASSWORD
OWNER(*admin*) DFLTGRP(STCCICS)

(2) Grant all userids associated with a CICS region the minimum privileges necessary to accomplish their functions. This applies equally to the CICS region userid and any CICS default userids. Under no circumstance should the OPERATIONS attribute be granted to the CICS region userid.

(3) Strictly control CICS default userids. Grant these userids the minimum access authorities necessary to perform their functions.

(4) All CICS terminal-user data is defined in the CICS segment of RACF user profiles. The following CICS segment parameter and associated value will be specified for all CICS users to include the CICS default user:

TIMEOUT(0015)

The TIMEOUT parameter specifies the elapsed time since the user last used the terminal before CICS times out the terminal.

- *(ZCIC0042: CAT II) The IAO will ensure that all CICS users have a 15 minute time-out limit specified.*

8.2.2.5 CICS Terminal Controls

Specify SIGNOFF(YES) or SIGNOFF(LOGOFF) on the CICS TYPETERM resource definition for all terminals. Do not specify the SIGNOFF(NO) option for any terminal.

8.2.2.6 CICS Transaction Controls

The STIG requirement is to run with SEC=YES and XTRAN=YES (or XTRAN=*ssrr*TRN) specified in the CICS system initialization parameters. With these values, CICS issues a security check to validate access authority for every transaction.

The following lists of transactions have specific and unique access authorization requirements:

(1) Transactions in *Table B-1* are only for CICS internal use. Access validation to these transactions are performed using the CICS region userid, not the CICS end-user userid. Define these transactions with the following specifications:

RACF profiles:

UACC(NONE)
Restrict *read* authority only to CICS region userids.

CICS transaction resource definitions:

RESSEC(NO)
CMDSEC(NO)

(2) The transactions in *Table B-3* may be exempt from security checking, and CICS permits any terminal user to initiate these transactions. RACF profiles for these transactions do not affect processing:

Define these transactions with the following CICS transaction resource definition specifications:

RESSEC(NO)
CMDSEC(NO)

(3) Other transactions may exist that execute within CICS and do not run under the authority of an individual user (e.g., background transactions). If so, these transactions should be fully documented and may be defined with the following specifications:

RACF profile:

UACC(READ)

CICS transaction resource definitions:

RESSEC(NO)
CMDSEC(NO)

8.2.3 TOP SECRET

8.2.3.1 CICS Security-related System Initialization Parameters

Uniquely define each CICS region to the Facility Matrix Table. All controls for CICS security is specified using the Facility Matrix options. The CICS SIT table is not used to specify security requirements for an individual region.

Every CICS region processes in FAIL mode using the TSS installation options. Access to an individual CICS region or a group of CICS regions defined in an MRO environment is determined by having access to the appropriate facility. A user-defined facility is modified to perform CICS security controls for each region or MRO grouped regions.

To maintain attach time security, define all CONNECTIONS with ATTACHSEC=IDENTIFY.In defining the Facility for use with a CICS region, set the following options:

TOP SECRET INITIALIZATION PARAMETERS

DEFACID(*NONE*)	No default ACID
NOABEND	For multi-user address space
RES	Allows storage of access authorizations for all resources within the online user region.
MODE(FAIL)	All unauthorized facility or resource access is denied unconditionally.

Ensure that users cannot sign on to more than one CICS production region within the scope of a single CICS region, a single OS/390 image, or a *sysplex*.

SIGN(S)	Single sign-on within the same CICS facility
SIGN(M)	Multiple sign-on within the same CICS facility (*use only with test or development regions*)
SHRPRF	Allows a copy of the profile to be shared by all users in the multiuser facility.
XDEF	Sets protection in place by default for all commands and transactions controlled by the facility.
PCTEXTSEC=OVERRIDE	CA-TOP SECRET does not honor the PCT EXTSEC= and RSLC= parameters and forces a security call.
EXTSEC=YES	CA-TOP SECRET security is invoked for this region
FACMATRX=YES	Controls for CICS security are specified in Facility Matrix.
LOCKTIME=0	This parameter is set to zero since the OPTIME parameter (refer to *Section 8.2.3.4, CICS User Controls*) provides a more efficient method for managing idle time.
XTRAN=YES	Transaction checking is performed.

- *(ZCICT050: CAT II) The IAO will ensure that control options for the Top Secret CICS facilities meets minimum requirements.*

8.2.3.2 System Data Set Controls

The CICS initialization program, DFHSIP, runs in an authorized state. It is typically installed in the SDFHAUTH library. This library is defined to the operating system as APF authorized. Refer to *Section 2.1.2.1, Authorized Program Facility (APF)*, for security control information.

8.2.3.3 Propagation Control

Utilize propagation control for each CICS region. Under no circumstance should a user's batch job submitted from a CICS region execute under that CICS region's ACID. To prevent this from occurring, define each CICS region ACID to the PROPCNTL resource class.

The following command example shows a CICS region ACID being owned to the PROPCNTL resource class:

TSS ADD(*deptacid*) PROPCNTL(*cics-region-acid)*

- *(ZCICT041: CAT II) The IAO will ensure that each CICS region userid is defined to the PROPCNTL resource class.*

8.2.3.4 CICS User Controls

(1) Grant all ACIDs associated with a CICS region the minimum privileges necessary to accomplish their functions. This applies equally to the CICS region ACID and any CICS default ACIDs. Under no circumstance should the BYPASS privilege be granted to the CICS region ACID. Strictly control CICS default ACIDs. Refer to *Section 8.2, CICS, Paragraph (8).*

(2) For all CICS users, to include the CICS default user, specify the parameter OPTIME=15 in the user's ACID. When the OPTIME threshold is reached, CICS takes action accordingly as specified in the terminals' TYPETERM SIGNOFF parameter.

- *(ZCIC0042: CAT II) The IAO will ensure that all CICS users have a 15 minute time-out limit specified.*

(3) The IAO will maintain documentation regarding any deviations from this requirement.

8.2.3.5 CICS Terminal Controls

Specify SIGNOFF(YES) or SIGNOFF(LOGOFF) on the CICS TYPETERM resource definition for all terminals. Do not specify the SIGNOFF(NO) option for any terminal.

8.2.3.6 Transaction Controls

Use OTRAN transaction protection for the administration of transaction-level checking. OTRAN protection allows the use of a transaction to be permitted either globally, or within a specific facility. The LCF process does not allow ownership to be specified. Therefore, auditing cannot be done. OTRAN does allow ownership specification. LCF transaction security can be overridden in the CICS transaction definition (PCT or RDO). OTRAN cannot be overridden. With DEFPROT specified, all unidentified transactions are protected, requiring all new transactions to be identified to the TOP SECRET database before they can be used. If DEFPROT is ON, it affects all transaction-based facilities (e.g., IMS, CICS).

The following lists of transactions have specific and unique access authorization requirements:

(1) Transactions in *Table B-1* are only for CICS internal use. Access validation to these transactions is be performed using the CICS region ACID, not the CICS end-user ACID.

Define these transactions with the following specifications:

(a) TOP SECRET rule(s) restrict access only to CICS region ACIDs.

(b) CICS transaction resource definitions use RESSEC (NO) and CMDSEC (NO).

(2) Transactions in *Table B-2* have an explicitly defined resource rule restricting them as noted in the table.

(3) The transactions in *Table B-3* may be exempt from security checking, and CICS permits any terminal user to initiate these transactions. They should be accessible to all CICS users. Define these transactions with the following specifications:

(a) Exempt from security checking by placing them in the TOP SECRET BYPASS TRANIDS list.

(b) CICS transaction resource definitions may use RESSEC (NO) and CMDSEC (NO).

(4) Other transactions may exist that execute within CICS and do not run under the authority of an individual user (e.g., background transactions). If so, these transactions are fully documented and may be exempt from access validation. Define them in the TOP SECRET BYPASS TRANIDS list.

(5) The TOP SECRET environmental utility transaction TSEU provides the capability to examine CICS security-related information. Restrict access to TSEU transaction only to Security personnel.

The use of the BYPASS list should be kept to a minimum. Only transactions that do not present a security exposure (e.g., sign-on/sign-off, menus, etc.) are included. Transactions for applications and COTS software are placed in unique profiles. Where required, multiple profiles are created to provide for more granular control and separation of capabilities. For example, for a COTS product that provides administrative, technical support, and user transactions, each of these functional areas would be provided with a separate profile to allow the assignment of access based on functional requirements.

(1) Non-suspend status to prevent the region from being disabled if the default userid is inadvertently suspended.

(2) A non-expiring password to prevent the region from being disabled if the default userid's password is subjected to a denial-of-service attack.

9. DATABASE MANAGEMENT SYSTEMS

9.1 General Considerations

Database management systems (DBMSs) provide the facilities to design, create, update, access, and manage database files. Information is stored in multiple files with various users accessing the data for many reasons. A single person (an Administrator) typically manages these files for all the database users.

Most database management systems require users to identify themselves by supplying a logonid and password before accessing the database system. This method provides a good defense against unauthorized access to the system.

Securing the use of database options, resources, and processes is crucial. All database functions (such as commands, transactions, and interactive options) should be reviewed for potential security exposures and to prevent unauthorized use. For example, only the database administrator should be allowed access to all the internal facilities used to manage and administer the database management system.

The informational data in the database should be protected against unauthorized access. Operating system-level data set controls for the database data sets are essential, but these controls are not enough. Users should not have complete access to all the data in a DBMS just because they have access to the OS data sets. Consideration should be given to securing the internal data structures, such as tables or files, within the OS data sets. This level of protection is usually handled by the internal security within the database product.

Use the following recommendations when securing access to database management systems:

(1) Control user access to the software product's data sets, and restrict access only to authorized personnel.

(2) All database systems in use at the DOD sites will interface with the system ACP to perform I&A validation. Any DBMS incapable of using the ACP to accomplish I&A will be phased out.

- *(ZDBM0010: CAT II) The IAO will ensure that Database systems interface with the system ACP to perform I&A (Identification and Authentication).*

(3) Review database user access, and restrict it to various options or processes within the database management system. Depending on the particular database product, this includes, but is not limited to, areas such as regions, transactions, options, and commands.

(4) Determine access to data structures within the database, and only grant it to eligible database users.

9.2 IDMS

IDMS (Integrated Database Management System) is a Database Management System (DBMS) from Computer Associates (CA) for IBM mainframe and compatible environments. IDMS can be secured through internal security provisions, through an external ACP, or through a combination of the two. At this time, only I&A is required to be handled by means of an external ACP. It should be noted, however, that every attempt should be made to externally secure every resource possible. (In future versions of this document, securing IDMS resources externally will be the standard.)

9.2.1 General Considerations

IDMS security starts with load module RHDCSRTT, also known as the SRTT (Security Resource Type Table). This module comes with IDMS and initially contains default values. The values the module contains are changed through modification and assembly of the #SECRTT macro. Entries are made in the SRTT that specify what resources are to be secured and how they are to be secured. The SRTT is loaded at IDMS system start-up, and can be reloaded dynamically by issuing a DCMT VARY NUCLEUS command for module RHDCSRTT. The scope of the SRTT extends over one or more CA-IDMS systems, depending on the security scheme. Generally, the following is defined in the SRTT:

- Each resource type to be secured
- The system that enforces security on the resource (internal IDMS or external ACP)
- For resources to be secured externally, information that the external security system needs to service a security check request on the resource

Resource rules are written for the ACP to arbitrate access to the IDMS regions (central versions [CVs]) based on the resource classes and names specified in the SRTT.

- *(ZIDM0010: CAT II) The IAO will ensure that IDMS is using external security and that the resource to be protected is configured properly to the IDMS-CV.*

9.2.1.1 Data Set Access

Control all IDMS system data sets so that only authorized users can access these data sets and only with the appropriate levels of permission.

- *(ZIDM0020: CAT II) The IAO will ensure that IDMS data set access authorization restricts UPDATE and/or ALLOCATE access to systems programming personnel and justification for any additional access is provided.*

9.2.1.2 Execution Mode

IDMS can be run as either a batch job or an STC. In either case, a unique userid will be associated with each IDMS region or CV. No default userids will be used. Each CV's userid will only have access to those resources required by IDMS to perform its function.

- *(ZIDM0030: CAT II) The IAO will ensure that IDMS regions (central versions) are defined with a unique userid and is properly defined to the ACP.*

9.2.1.3 IDMS Resource

To assign Signon processing to an external ACP, entries are added to the SRTT for the sign-on resource type SGON. A new SRTT is generated by use of the #SECRTT macro. The first #SECRTT macro initializes SRTT values for all IDMS resources. The value of the TYPE parameter on the first macro must be INITIAL. *Do not change this macro.*

Code the second #SECRTT macro coded as follows to specify the resource class:

```
#SECRTT TYPE=ENTRY,RESTYPE=SGON,EXTCLS='resource class',                X
      SECBY=EXTERNAL,EXTNAME=(RESNAME)
```

By design, the value of EXTCLS can be user specified.

The STIG recommended resource class is SGO for ACF2, #IDMSGON for RACF, and IDMSSGON for TOP SECRET. This field, also referred to as a resource type**,** is used when coding ACP security rules.

- *(ZIDM0010: CAT II) The IAO will ensure that the IDMS resource class is properly defined and protected in the ACP.*

IDMS also requires that the last entry made in the #SECRTT macro must specify TYPE=FINAL. *Do not change this macro.*

Please refer to the *CA-IDMS Security Administration Guide* for further details on coding the #SECRTT macro.

In addition to the resource class, the value for what is generally referred to as resource name must be specified. The resource name uniquely identifies each IDMS CV, and is the value specified for SYSTEM ID on the SYSTEM statement specified when the IDMS CV is generated. This SYSTEM ID should match the userid assigned to the CV. The SYSTEM statement is coded as follows:

```
MOD SYSTEM 120 SYSTEM ID IS resource name
```

For example, if the resource name is IDMSD:

MOD SYSTEM 120 SYSTEM ID IS IDMSD

Each CV will have a unique name within the LPAR so that access granted for a specific CV does not automatically give access to other CVs.

- *(ZIDM0014: CAT II) The IAO will ensure that each IDMS CV is uniquely defined to the ACP IDMS resource class.*

9.2.1.4 APPLIDs

Accessing IDMS from VTAM or a session manager (e.g., CL/SUPERSESSION) requires an APPLID. Each CV has a separate and unique APPLID, within the applicable Session Manager. Users should only have access to those CVs/APPLIDs required to perform their jobs.

9.2.2 ACF2

9.2.2.1 Data Set Access

Control all IDMS system data sets so that only authorized users can access these data sets and only with the appropriate levels of permission.

9.2.2.2 Execution Mode

If the IDMS CV is run as an STC, code the userid as follows:

MUSASS, NO-SMC, JOBFROM, MUSUPDT, STC

If the IDMS CV is run as a batch job, code the userid as follows:

MUSASS, NO-SMC, JOBFROM, MUSUPDT, RESTRICT,
PGM(*xxxxxxxx*), SUBAUTH

9.2.2.3 IDMS Resource

Following is an example of the ACF2 rule set that needs to be coded to allow a user access to an IDMS **CV**:

$KEY(*resource name*) TYPE(SGO)
UID(*user*) ALLOW

9.2.2.4 APPLIDs

Accessing IDMS from VTAM or a session manager (e.g., CL/SUPERSESSION) requires an APPLID. Each CV has a separate and unique APPLID. Users should only have access to those CVs/APPLIDs required to perform their jobs.

9.2.3 RACF

9.2.3.1 Data Set Access

Control all IDMS system data sets so that only authorized users can access these data sets and only with the appropriate levels of permission.

9.2.3.2 Execution Mode

A unique userid is associated with each IDMS region or CV. All IDMS CV userids are defined as PROTECTED userids. For example:

AU IDMSPROD NAME('IDMS PROD CV') NOPASSWORD
OWNER(*admin*) DFLTGRP(*idms-cv-group*)

Propagation control must be implemented for each region/CV to ensure that the CV's userid is not propagated to batch jobs submitted by that region. This is done by defining in the PROPCNTL class profiles whose names match those of each region (CV). (Note that, as specified in *Section 9.4.1.3, IDMS Resource*, each CV's userid matches the resource name associated with the region.) The following is an example of the steps necessary to ensure that propagation control is activated for the regions. Do the following for each region/CV userid:

- Define a profile to the PROPCNTL class:

  RDEFINE PROPCNTL *resource name*

  For example, if the *resource name* (IDMS region's userid) is IDMSD, then the command would be as follows:

  RDEFINE PROPCNTL IDMSD

- Ensure that the PROPCNTL class is active:

  SETROPTS CLASSACT(PROPCNTL)

- Ensure that SETROPTS RACLIST processing is active for the PROPCNTL class:

  SETROPTS RACLIST(PROPCNTL)

- *(ZIDMR032: CAT II) The IAO will ensure that each IDMS CV userids are defined to the PROPCNTL resource class.*

All IDMS CVs that run as STCs has a matching profile defined to the STARTED resource class as shown in the following example:

```
RDEFINE STARTED IDMS*.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCIDMS) TRUSTED(NO))
```

9.4.3.3 IDMS Resource

Add a new class to the RACF Class Descriptor Table and the RACF Router Table for *classname* #IDMSGON. Following are examples of the two macros required to achieve this:

```
ICHERCDE CLASS=#IDMSGON,
                DFTUACC=NONE,
                FIRST=ALPHA,
                ID=nnn,
                MAXLNTH=8,
                OPER=NO,
                OTHER=ANY,
                POSIT=nnn

ICHRFRTB CLASS=#IDMSGON,
                ACTION=RACF
```

NOTE: Local configuration determines the value of nnn.

Following is an example of the RACF rule that needs to be coded to allow a user access to an IDMS CV:

```
RDEF #IDMSGON resource name UACC(NONE) OWNER(*******)

PE resource name CLASS(#IDMSGON) ID(user) ACCESS(READ)
```

9.2.3.4 APPLIDs

Accessing IDMS from VTAM or a session manager (e.g., CL/SUPERSESSION) requires an **APPLID**. Each **CV** has a separate and unique **APPLID**. Users only have access to those **CVs**/**APPLIDs** required to perform their jobs.

9.2.4 TOP SECRET

9.2.4.1 Data Set Access

Control all IDMS system data sets so that only authorized users can access these data sets and only with the appropriate levels of permission.

9.2.4.2 Execution Mode

Associate each IDMS **CV** with a unique ACID using the following examples:

(1) If the IDMS CV is executed as a batch job:

TSS CREATE(*resource name*) NAME(*'xxxxx xxxxx'*)
TYPE(USER) DEPT(*xxxx*) FAC(BATCH)
MASTFAC(*resource name*) PASS(*password*,0)
SOURCE(INTRDR)

(2) If the IDMS CV is executed as an STC:

TSS CREATE(*resource name*) TYPE(USER)
NAME (*'xxxxxx xxxxxx'*) DEPT(*xxxx*) FAC(STC)
MASTFAC(*resource name*) PASS(*password*,0)
SOURCE(INTRDR)

(3) Additionally, if executed as an STC, add the ACID above to the STC record using the following example:

TSS ADD(STC) PROCNAME(*proc name*) ACID(*resource name*)

(4) Propagation control must be implemented for each region/CV to ensure that the CV's ACID is not propagated to batch jobs submitted by that region. This is accomplished by defining each IDMS CV ACID to the PROPCNTL resource class.

The following command example shows an IDMS CV ACID being owned to the PROPCNTL resource class:

TSS ADD(*deptacid*) PROPCNTL(*idms-cv-acid)*

- *(ZIDMT032: CAT II) The IAO will ensure that each IDMS CV userids are defined to the PROPCNTL resource class.*

9.2.4.3 IDMS Resource

(1) Add resource class IDMSSGON to the Resource Description Table (RDT) using the following example:

TSS ADD(RDT) RESCLASS(IDMSSGON) RESCODE(*xx*)

(2) Add the resource names to resource class IDMSSGON, and permit users access to them as in the following example:

```
TSS ADD(dept-acid) IDMSSGON(resource name)
TSS PERMIT(user-acid) IDMSSGON(resource name)
```

(3) Define each IDMS CV in the TOP SECRET Facilities Matrix Table using the following example:

```
*   IDMSD    IDMS CV
FAC(USERxx=NAME=IDMSD,PGM=IDM,ID=xx,KEY=n,TYPE=IDMS)
FAC(IDMSD=ACTIVE,SHRPRF,NOASUBM,NOABEND,MULTIUSER,
      NOXDEF)
FAC(IDMSD=LUMSG,STMSG,SIGN(M),NOINSTDATA,NORNDPW,
      AUTHINIT)
FAC(IDMSD=NOPROMPT,NOAUDIT,NORES|RES,WARNPW,NOTSOC)
FAC(IDMSD=NOTRACE,MODE=FAIL,LOG(SMF,INIT,MSG,SEC9))
FAC(IDMSD=UIDACID=8,LOCKTIME=000)
```

- *(ZIDMT040: CAT II) The IAO will ensure that IDMS Top Secret facilities are properly defined.*

9.2.4.4 TSS Command Task Installation

Follow these steps to install the TSS command task:

(1) Copy the load module TSSIDMS from the TSS load library into the IDMS program load library.

(2) Define the program TSSIDMS in the IDMS system generation as follows:

```
PROGRAM TSSIDMS LANGUAGE IS ASSEMBLER
```

(3) Define the task TSS in the IDMS system as follows:

```
TASK TSS INVOKES PROGRAM TSSIDMS
```

9.2.4.5 Application Interface Installation

Follow these steps to install the application interface:

(1) Copy the load module TSSMAI from the TOP SECRET load library into the IDMS program library.

(2) Define the program TSSMAI in the IDMS system generation as follows:

PROGRAM TSSMAI LANGUAGE IS ASSEMBLER

9.2.4.6 APPLIDs

Accessing IDMS from VTAM or a session manager (e.g., CL/SUPERSESSION) requires an APPLID. Each CV has a separate and unique APPLID. Users only have access to those CVs/APPLIDs required to perform their jobs.

This page is intentionally left blank.

10. DASD MANAGEMENT SOFTWARE

10.1 General Considerations

DASD management software products perform storage management functions. They provide many effective services for users in an OS/390 installation. For example, these products determine data placement, move data between device types, control DASD space usage, and manage and automate data backup. Based on installation policy, they automatically assign specific data definition attributes to data sets when they are created. DASD management software products also help users to define performance goals and data availability requirements.

DASD management software products may have unlimited access to DASD resources and carry with them many powerful management features and capabilities. Therefore they are properly protected and only accessed by authorized users. Improper protection of these products can cause serious problems, such as destruction of production data, improper access of sensitive information, system data integrity exposures, etc.

Use the following recommendations when implementing security controls for DASD management software products:

(1) The services of an ACP are used primarily for security control. However, sometimes it may not be possible to provide a secure environment using only ACP controls. In this case, the use of product internal security may be warranted and is to be investigated for possible use. Product internal security facilities are not allowed to compromise existing ACP security controls under any circumstances.

(2) Access to all data sets relative to software products (e.g., executable code and cataloged procedures, definition/configuration data, and exit routines) are controlled and restricted only to authorized personnel. General users are not allowed to access these data sets.

(3) Access to all commands, to batch and on-line utilities, and to production and maintenance jobs relative to software products are protected and restricted only to authorized personnel.

(4) Access to all DASD volumes and to users' data sets managed by software products are secured and restricted only to authorized personnel.

(5) Review product interfaces for potential security exposures. Document any potential security exposures. Notify DISA FSO and the vendor.

(6) Collect SMF data for auditing purposes.

The following sections provide detailed information concerning the protection of DASD management software products.

10.2 DFSMS

Vendor: IBM Corporation

DFSMS (Data Facility Storage Management Subsystem) is IBM's OS/390 product implementation of system-managed storage. DFSMS/MVS is a fully integrated storage management tool that allows an organization to manage all of its storage resources and data automatically by system resources (hardware and software), eliminating manual storage management.

DFSMS/MVS consists of the following functional components:

- **DFSMSdfp** (Data Facility Product) provides the storage, program, data, and device management functions of MVS/ESA. The Storage Management Subsystem (SMS) component of DFSMSdfp is fundamental in providing these functions. DFSMSdfp provides the foundation for distributed data access, using the Distributed File Manager to support remote access of MVS/ESA data and storage resources from workstations, personal computers, or other authorized systems in an SNA LU 6.2 network. Use the DFSMS/MVS Network File System server to enable an MVS/ESA system to act as a file server to workstations, personal computers, and other authorized systems in a TCP/IP network.

- **DFSMSdss** (Data Set Services) provides data movement, copy, dump, and restore, converting data sets and volumes to and from SMS management and space management functions for MVS/ESA.

- **DFSMShsm** (Hierarchical Storage Manager) provides the backup, recovery, migration, recall, disaster recovery (using ABARS), space management, and availability management functions in the SMS environment.

- **DFSMSrmm** (Removable Media Manager) provides the management functions for removable media including tape cartridges, reels, and optical volumes.

The latest release of DFSMS from IBM has moved virtually all of the system storage I/O and management into this product, along with additional functionality. This is a major change in the OS/390 environment. Because of these extensive changes, it is important to note that the steps outlined here reflect the minimum allowable security for implementing this product.

Use the following recommendations and techniques to control access to DFSMS:

(1) Validate authorization to access DFSMS via the ACP and its standard resources.

(2) Control DFSMS via the Facility, Storage, Management, and Program resource classes. Control these resource classes via the ACP.

(3) Only grant users access to those DFSMS resources necessary to perform their normal job functions.

10.2.1 SMS Classes and Groups

SMS classes and groups are lists of traits and characteristics associated with or assigned to data sets, objects, and volumes. Automatic Class Selection (ACS) routines assign classes to data, based on its requirements and attributes, and selects the target storage group. An SMS configuration can contain the following types of classes and groups:

- Data Class

  Defines attributes about the data set that would normally be associated with the SPACE, DCB, or AMP parameters in standard JCL.

- Storage Class

  Defines the data set as being SMS-managed. The storage class assignment affects which SMS-controlled volume is selected to hold that data set.

- Management Class

  Defines space and availability management attributes of the data set. This includes how often to perform backups and how many backup versions are kept. A management class can only be associated with an SMS-controlled data set.

- Storage Group

  Defines a list of volumes and manages them as if they were one large, single volume. SMS applies the properties assigned to a storage group to all the volumes within the storage group.

Of these, the resident ACP controls the Storage (STORCLAS) and Management (MGMTCLAS) classes.

10.2.2 DFSMS/MVS Functions and Commands

This section discusses the controls used to protect DFSMS/MVS functions and commands. The single term “functions” may be used throughout this section to imply both functions and commands. As with all general sections in the OS/390 STIG, the discussion may use RACF-oriented language. Each topic discussed is addressed in an ACP-specific section demonstrating how to meet DOD requirements using ACP command examples.

The ability to perform functions associated with DFSMS/MVS will be controlled using SAF. STGADMIN resources defined to the FACILITY resource class used to control access to these functions. Although a number of STGADMIN resources are used specifically to protect the Storage Management Subsystem, resource checking is still performed in environments where system-managed storage is not in use. Some DFSMS/MVS functions are allowed by default and require a STGADMIN resource to be defined to prevent its use. A generic resource will be defined to the FACILITY resource class with no user access by default. This will ensure access to sensitive functions is protected from unauthorized personnel.

STGADMIN resources protect a wide range of DFSMS/MVS functions from the DFSMSdfp, DFSMSdss, DFSMShsm, and DFSMSrmm components. Some sites may have specialized systems programming groups responsible for these different functions or aspects of storage management. The requirements in the STIG regarding access authorization to STGADMIN resources may refer to a single group, that is "systems programming personnel responsible for storage management." Depending on your site's organizational structure and the function being protected, this single group reference may apply to different specialized groups within the systems programming department. Each site should maintain a document, such as an SOP, that outlines the structure of the system-level support area including the roles and responsibilities of each department and group within this area. In the absence of such a document, the IAO will be responsible for ensuring appropriate documentation (such as a DD Form 2875) is maintained justifying the access to sensitive STGADMIN functions.

The ACP resources used to control all DFSMS/MVS functions begin with the high-level qualifier STGADMIN. To distinguish these functions and ensure authorization is restricted to the appropriate personnel, access to STGADMIN resources will be controlled using the first two high-level resource name qualifiers at a minimum. The exception will be DFSMSdss Administrator resources that will be controlled using the first three high-level resource name qualifiers at a minimum.

- *(ZSMS0010: CAT II) The IAO will ensure that no access is given to the high-level STGADMIN resource.*

10.2.2.1 DFSMSdfp Resource Protection

DFSMSdfp is the core component of DFSMS/MVS. It performs the essential data, storage, program, and device management functions of the operating system. DFSMSdfp includes Access Method Services (AMS), OPEN/CLOSE/EOV routines, catalog management, DADSM (DASD space control) utilities, IDCAMS, SMS, NFS, ISMF, and other functions. Many of the functions offered with these services and utilities are intended for storage administration only and must be restricted to appropriate personnel.

The DFSMSdfp resources in this section are grouped together by functional support, such as SMS configuration or catalog maintenance. Please note that all DFSMSdfp resources are protected using the FACILITY resource class.

There is one unique DFSMSdfp resource that does not fit well into a group. This resource is named STGADMIN.DPDSRN.*olddsname*, where *olddsname* is up to 23 characters of the

existing data set name. It controls the ability to scratch or rename a data set that is allocated to another address space in the system or sysplex. To preserve data integrity, this functionality should not be allowed. However there are times when you may need to scratch or rename a data set that has the same name as a data set used by another address space, for example, when building a new system. Access to STGADMIN.DPDSRN.*olddsname* resources will be restricted to systems programming personnel on an as needed basis only. Permanent access to these resources will not be permitted and will not be granted on a production system. All STGADMIN.DPDSRN.*olddsname* resources will be defined to the ACP as fully qualified and not generic, all access will be logged. Appropriate documentation justifying access requirements to STGADMIN.DPDSRN.*olddsname* resources will be maintained by the IAO.

- *(ZSMS0010: CAT II) The IAO will ensure that STGADMIN.DPDSRN.olddsname is restricted to system programmers on an as needed basis and all access will be logged.*

NOTE: The STGADMIN.DPDSRN.olddsname resource does not affect the processing of a data set allocated to a user's current address space. It does not allow a user to rename or scratch a data set that is open in their current address space.

10.2.2.1.1 DASD Cache Configuration

DFSMSdfp can be used to manage storage control unit characteristics. The following table lists the SAF resource information relative to the protection of DFSMSdfp functions specific to DASD cache configuration support:

Table B-5. DFSMSdfp SAF RESOURCES (10.2.2.1.1)

DFSMSdfp SAF RESOURCES		
DASD CACHE CONTROLLER CONFIGURATION SUPPORT		
RESOURCE NAME	DESCRIPTION	ACCESS
STGADMIN.IDC.BINDDATA	Use AMS BINDDATA command to support paging and caching subsystems	READ
STGADMIN.IDC.LISTDATA	Use AMS LISTDATA command to obtain caching subsystem information	READ
STGADMIN.IDC.LISTDATA.ACCESSCODE	Use AMS LISTDATA command with the ACCESSCODE parameter to support remote maintenance of cache units	READ
STGADMIN.IDC.SETCACHE STGADMIN.IDC.SETCACHE.DISCARDPINNED STGADMIN.IDC.SETCACHE.PENDINGOFF STGADMIN.IDC.SETCACHE.REINITIALIZE STGADMIN.IDC.SETCACHE.SUBSYSTEM	Use AMS SETCACHE command with various parameters to support caching subsystem configuration	READ

All DFSMSdfp DASD cache controller SAF resources identified in the above table will be defined to the FACILITY resource class with no user access by default. Access to these resource will be restricted to systems programming personnel responsible for storage management only.

- *(ZSMS0010: CAT II) The IAO will ensure that all access to the resources in the above table will be restricted to systems programming personnel responsible for storage management.*

10.2.2.1.2 SMS Configuration

DFSMSdfp can be used to manage SMS configuration characteristics. The following table lists the SAF resource information relative to the protection of DFSMSdfp functions specific to SMS configuration support:

Table B-6. DFSMSdpf SAF RESOURCES (10.2.2.1.2)

DFSMSdfp SAF RESOURCES		
SMS CONFIGURATION SUPPORT		
RESOURCE NAME	DESCRIPTION	ACCESS
STGADMIN.IDC.DCOLLECT	Collect data set and volume statistics and information, and SMS configuration data	READ
STGADMIN.IGD.ACTIVATE.CONFIGURATION	Activate an SMS configuration from the Interactive Storage Management Facility (ISMF) application	READ
STGADMIN.IGG.ALTER.SMS	Alter the storage class and management class of an SMS-managed data set	READ
STGADMIN.IGG.ALTER.UNCONVRT	Alter an SMS-managed VSAM data set to an unmanaged VSAM data set	READ
STGADMIN.IGG.LIBRARY	Define, delete, or alter library and volume entries in a tape library	READ
STGADMIN.IGWSHCDS.REPAIR	Use AMS SHCDS command to manage SMSVSAM recovery	READ

All DFSMSdfp SMS configuration SAF resources identified in the above table will be defined to the FACILITY resource class with no user access by default. Access to these resource will be restricted to systems programming personnel responsible for storage management only.

- *(ZSMS0010: CAT II) The IAO will ensure that all access to the resources in the above table will be restricted to systems programming personnel responsible for storage management.*

The STGADMIN.IGD.ACTIVATE.CONFIGURATION resource protects the ability to activate an SMS configuration. If a user issues the ACTIVATE command from the Control Data Set Application Selection panel of ISMF, and either the FACILITY resource class is inactive or the named resource does not exist, the operator is queried to decide whether the ACTIVATE action should be allowed. The user will remain on the panel without the ability to provide additional input until action is taken from the operator console. If the user has authority to activate an SMS configuration from ISMF, activation proceeds without confirmation from the operator console, and the user continues with normal operations. All access to the STGADMIN.IGD.ACTIVATE.CONFIGURATION resource will be logged using the ACP.

- *(ZSMS0010: CAT II) The IAO will ensure that STGADMIN.IGD.ACTIVATE.CONFIGURATION is restricted to system programmers on an as needed basis and all access will be logged.*

10.2.2.1.3 Integrated Catalog Facility (ICF) Catalog Maintenance

DFSMSdfp can be used to manage ICF catalog characteristics. An ICF catalog consists of two separate kinds of data sets, a Basic Catalog Structure (BCS) and a VSAM Volume Data Set (VVDS). The following table lists the SAF resource information relative to the protection of DFSMSdfp functions specific to Integrated Catalog Facility (ICF) catalog maintenance:

Table B-7. DFSMSdfp SAF RESOURCES (10.2.2.1.3)

DFSMSdfp SAF RESOURCES		
ICF CATALOG MAINTENANCE		
RESOURCE NAME	DESCRIPTION	ACCESS
STGADMIN.IDC.DIAGNOSE.CATALOG	Use AMS DIAGNOSE command to analyze the contents of a catalog	READ
STGADMIN.IDC.DIAGNOSE.VVDS	Use AMS DIAGNOSE command to compare the VVDS against the BCS	READ
STGADMIN.IGG.ALTBCS	Alter BCS catalog attributes	READ
STGADMIN.IGG.DEFDEL.UALIAS	Define and delete an alias to a user catalog	READ
STGADMIN.IGG.DEFNVSAM.NOBCS	Define a non-VSAM data set with no BCS entry	READ
STGADMIN.IGG.DEFNVSAM.NONVR	Define a non-VSAM data set with no VVDS entry	READ
STGADMIN.IGG.DELGDG.FORCE	FORCE DELETE a generation data group	READ
STGADMIN.IGG.DELETE.NOSCRATCH	Delete a BCS data set entry without deleting the actual data set	READ
STGADMIN.IGG.DELNVR.NOBCSCHK	Delete a VVDS data set entry without checking the BCS entry	READ
STGADMIN.IGG.DIRCAT	Direct a catalog request bypassing the normal catalog search	READ
STGADMIN.IGG.DLVVRNVR.NOCAT	Delete a VVDS data set entry without an associated catalog	READ

All DFSMSdfp ICF catalog maintenance SAF resources identified in the above table will be defined to the FACILITY resource class with no user access by default. Access to these resource will be restricted to systems programming personnel responsible for storage management only.

- *(ZSMS0010: CAT II) The IAO will ensure that all access to the resources in the above table will be restricted to systems programming personnel responsible for storage management.*

System Master Catalog Management of User Catalog Aliases

Section 3.1.5.1, Data Set Controls, restricts *alter* and *update* data set access to the System Master Catalog to systems programming personnel. In the past, security personnel required these levels of access to the System Master Catalog to DEFINE and DELETE user catalog aliases as part of maintaining user accounts on the system. The *alter* access is excessive given the sensitive nature of the System Master Catalog. To allow security personnel to adequately maintain user catalog aliases, the FACILITY resource class can be used instead of assigning *alter* and *update* data set access to the System Master Catalog.

The STGADMIN.IGG.DEFDEL.UALIAS resource in the FACILITY resource class controls the ability to DEFINE and DELETE an alias related to a user catalog without the need for data set access to system catalogs. To allow a user to DEFINE and DELETE an alias in the System Master Catalog, permit the user *read* access to the STGADMIN.IGG.DEFDEL.UALIAS resource. A user will still be able to perform these functions if they have *alter* data set access to the System Master Catalog even if they do not have *read* access to STGADMIN.IGG.DEFDEL.UALIAS.

The STGADMIN.IGG.DEFDEL.UALIAS resource will be defined to the FACILITY resource class with no user access by default. Access to this resource will be restricted to systems programming personnel and security personnel. All access to this resource will be logged using the ACP.

- *(ZSMS0010: CAT II) The IAO will ensure that STGADMIN.IGG.DEFDEL.UALIAS is restricted to system programmers on an as needed basis and all access will be logged.*

10.2.2.2 DFSMSdss Resource Protection

DFSMSdss is a DASD data and space management tool. DFSMSdss utilities can be used to copy and move data sets between volumes, dump and restore data sets and volumes, convert data sets and volumes to and from SMS management, compress partitioned data sets, and many other DASD management functions.

DFSMSdss resources can be grouped into two categories. One group of resources respects existing ACP controls, such as data set and volume resource rules, before allowing the DFSMSdss function. Because additional ACP controls may be in effect, access authorization to some DFSMSdss functions outside the systems programming group responsible for storage management will be permitted. These resources protect Non-Administrator functions.

The other group of resources provides the authority required to perform system storage administration tasks. The authority associated with these functions allows a user to obtain a privileged status and effectively bypass all ACP data set and volume controls. Access authorization to these resources will be restricted to systems programming personnel responsible for storage management.

The following table lists the SAF resource information relative to the protection of DFSMSdss Non-Administrator functions:

Table B-8. DFSMSdss SAF RESOURCES (10.2.2.2 a)

DFSMSdss SAF RESOURCES			
Non-Administrator Functions			
RESOURCE NAME	DESCRIPTION	ACCESS	USERS
STGADMIN.ADR.COPY.BYPASSACS	Use DFSMSdss COPY command with user-specified storage and management classes	READ	Sysprogs
STGADMIN.ADR.COPY.CNCURRNT	Use DFSMSdss COPY command with quick data set serialization	READ	Sysprogs End-users
STGADMIN.ADR.COPY.INCAT	Use DFSMSdss COPY command altering the catalog search sequence	READ	Sysprogs
STGADMIN.ADR.COPY.PROCESS.SYS	Use DFSMSdss COPY command on SYS1 data sets	READ	Sysprogs
STGADMIN.ADR.COPY.TOLERATE.ENQF	Use DFSMSdss COPY command while data set is in use	READ	Sysprogs End-users
STGADMIN.ADR.CONVERTV	Use DFSMSdss CONVERTV command to convert existing volumes to and from SMS	READ	Sysprogs
STGADMIN.ADR.DEFRAG	Use DFSMSdss DEFRAG command to relocate data extents on a DASD volume	READ	Sysprogs
STGADMIN.ADR.DUMP.CNCURRNT	Use DFSMSdss DUMP command with quick data set serialization	READ	Sysprogs End-users
STGADMIN.ADR.DUMP.INCAT	Use DFSMSdss DUMP command altering the catalog search sequence	READ	Sysprogs

DFSMSdss SAF RESOURCES			
Non-Administrator Functions			
RESOURCE NAME	DESCRIPTION	ACCESS	USERS
STGADMIN.ADR.DUMP.PROCESS.SYS	Use DFSMSdss DUMP command on SYS1 data sets	READ	Sysprogs
STGADMIN.ADR.DUMP.TOLERATE.ENQF	Use DFSMSdss DUMP command while data set is in use	READ	Sysprogs End-users
STGADMIN.ADR.PATCH	Use DFSMSdss SET PATCH command to modify default operations	READ	Sysprogs
STGADMIN.ADR.RELEASE.PROCESS.SYS	Use DFSMSdss RELEASE command to free unused DASD space for SYS1 data sets	READ	Sysprogs
STGADMIN.ADR.RELEASE.INCAT	Use DFSMSdss RELEASE command to free unused DASD space for data sets altering the catalog search sequence	READ	Sysprogs
STGADMIN.ADR.RESTORE.BYPASSACS	Use DFSMSdss RESTORE command with user-specified storage and management classes	READ	Sysprogs
STGADMIN.ADR.RESTORE.DELCATE	Use DFSMSdss RESTORE during a disaster recovery when existing catalog entries may no longer be valid. Allows DFSMSdss to perform a DELETE NOSCRATCH operation.		Sysprogs
STGADMIN.ADR.RESTORE.IMPORT	Use DFSMSdss RESTORE indicating the data sets being restored are from another system and are considered new	READ	Sysprogs

DFSMSdss SAF RESOURCES			
Non-Administrator Functions			
RESOURCE NAME	DESCRIPTION	ACCESS	USERS
STGADMIN.ADR.RESTORE.TOLERATE.ENQF	Use DFSMSdss RESTORE command while data set is in use	READ	Sysprogs End-users

All DFSMSdss Non-Administrator functions identified in the above table will be defined to the FACILITY resource class with no user access by default. Access to these resource will be restricted to systems programming personnel responsible for storage management and authorized end-users as indicated in the table. Fully qualified resource names for all access authorizations permitted to end-users will be defined by the IAO.

- *(ZSMS0010: CAT II) The IAO will ensure that all access to the resources in the above table will be restricted to systems programming personnel and end-users.*

The following table lists the SAF resource information relative to the protection of DFSMSdss Administrator functions:

Table B-9. DFSMSdss SAF RESOURCES (10.2.2.2 b)

DFSMSdss SAF RESOURCES		
ADMINISTRATOR FUNCTIONS		
RESOURCE NAME	DESCRIPTION	ACCESS
STGADMIN.ADR.STGADMIN.BUILDSA	Use DFSMSdss BUILDSA command to build the Stand-Alone Services IPL-able core image	READ
STGADMIN.ADR.STGADMIN.COMPRESS	Use DFSMSdss COMPRESS command to remove unused space in partitioned data sets	READ
STGADMIN.ADR.STGADMIN.COPY	Use DFSMSdss COPY command to perform data set, volume, and track movement	READ
STGADMIN.ADR.STGADMIN.COPY.DELETE	Use DFSMSdss COPY command and delete the data sets after completion	READ
STGADMIN.ADR.STGADMIN.COPY.RENAME	Use DFSMSdss COPY command using new names for the data sets	READ

DFSMSdss SAF RESOURCES		
ADMINISTRATOR FUNCTIONS		
RESOURCE NAME	DESCRIPTION	ACCESS
STGADMIN.ADR.STGADMIN.DEFRAG	Use DFSMSdss DEFRAG command to relocate data set extents on a DASD volume to reduce or eliminate free-space fragmentation	READ
STGADMIN.ADR.STGADMIN.DUMP	Use DFSMSdss DUMP command to dump data sets, volumes, and tracks to a sequential data set	READ
STGADMIN.ADR.STGADMIN.DUMP.DELETE	Use DFSMSdss DUMP command and delete the data sets after completion	READ
STGADMIN.ADR.STGADMIN.PRINT	Use DFSMSdss PRINT command to print data sets, tracks, and VTOCs	READ
STGADMIN.ADR.STGADMIN.RELEASE	Use DFSMSdss RELEASE command to free unused DASD space for data sets	READ
STGADMIN.ADR.STGADMIN.RESTORE	Use DFSMSdss RESTORE command to restore data sets, volumes, and tracks	READ
STGADMIN.ADR.STGADMIN.RESTORE. RENAME	Use DFSMSdss RESTORE command using new names for the data sets	READ

All DFSMSdss Administrator functions identified in the above table will be defined to the FACILITY resource class with no user access by default. Access to these resource will be restricted to systems programming personnel responsible for storage management. DFSMSdss SAF resources for Administrator functions will be defined using the first three high-level resource name qualifiers at a minimum. All access to these resources will be logged using the ACP.

- *(ZSMS0010: CAT II) The IAO will ensure that all access to at least the first three high-level qualifiers of the resources in the above table will be restricted to systems programming personnel responsible for storage management and will be logged.*

10.2.2.3 DFSMShsm Resource Protection

This section was not completed at the time this document was prepared. Guidance for this product will be added in a future update to this document.

10.2.2.4 DFSMSrmm Resource Protection

DFSMSrmm is a product that manages removable media. There are no current plans to develop guidance for DFSMSrmm in this document.

10.2.3 PROGRAM Resource Class

Use the PROGRAM resource class to prevent unauthorized users from running selected Interactive Storage Management Facility (ISMF) programs. Details on this protection can be found in the associated IBM documentation.

The PROGRAM resource class is used to protect programs used to modify or change SMS. Restrict these programs only to personnel who provide DASD management, system security, and systems programming. These programs all begin with DGT and reside in SYS1.DGTLLIB and SYS1.DFQLLIB data sets. The default user access to these programs will be specified as NONE.

- *(ZSMS0012: CAT II) The IAO will ensure that the DGT* program resource is defined to the ACP with no user access by default and only authorized user are given access.*

10.2.4 SMS Data Set Controls

Use the following recommendations to control access to DFSMS data sets:

(1) Restrict *update* and *alter* access to the following control data sets only to systems programming personnel who are responsible for DASD management:

   (a) Source Control Data Set (SCDS) contains an SMS configuration, which defines a storage management policy.

   (b) Active Control Data Set (ACDS) contains a copy of the most recently activated configuration. All systems in an SMS complex use this configuration to manage storage.

   (c) Communications Data Set (COMMDS) contains the name of the ACDS containing the currently active storage management policy, the current utilization statistics for each system-managed volume, and other system information.

(2) The ACDS data set will reside on a different volume than the COMMDS data set.

- *(ZSMS0022: CAT II) The IAO will ensure that SMS control data set(s) are placed on separate volumes.*

(3) Allocate backup copies of the ADCS and COMMDS data sets on a different shared volume from the primary ADCS and COMMDS data sets.

(4) The ACS Routine Source Data Sets contain clist-like routines that define actions to be taken when a new data set is allocated. The SMS-managed classes are selected by the Automatic Class Selection (ACS) routines:

Partitioned data sets whose members are source ACS routines
Sequential data sets that contain one source ACS routine

(5) The ACS Routine Test Library contains partitioned data set(s) whose members are ACS test cases.

- *(ZSMS0020: CAT II) The IAO will ensure that DFSMS control data sets restrict Update or Allocate access to system programmers responsible for dasd management. Justification is required for any additional access.*

10.2.5 Additional Controls

10.2.5.1 Resource Ownership

The use of SMS management classes and storage classes can be controlled using the ACP. The product default is to use the resource owner value, which is based on the high-level qualifier of the data set name, to control access to management and storage classes. As an alternative, the user allocating the data set can be used to control access to these classes. This option is controlled with the USE_RESOWNER parameter. Refer to *Section 10.2.5.2, System Parmlib Members*, for additional information.

- *(ZSMS0014: CAT II) The IAO will ensure that if USE_RESOWNER(YES) is in effect, a resource owner (RESOWNER) in the DFP segment of all ACP data set profiles is defined.*

10.2.5.2 System Parmlib Members

The IEASYS*xx*, IGDSMS*xx*, and IEFSSN*xx* members of SYS1.PARMLIB direct the initialization and activation of SMS.

(1) In member IEASYS*xx*, the SMS=*xx* parameter indicates the member name of the IGDSMS*xx* within SYS1.PARMLIB that is used for initialization. For example, if SMS=00 in IEASYS*xx*, the IGDSMS00 member of SYS1.PARMLIB is used during initialization.

(2) Member IDGSMS*xx* provides initialization parameters to SMS.

Table B-10. SMS INITIALIZATION PARAMETERS (in IGDSMS*xx*) (10.2.5.2 a)

SMS INITIALIZATION PARAMETERS (in IGDSMSxx)	
PARAMETER	DESCRIPTION
The following parameters are required for SMS initialization:	
SMS	Identifies the member as a repository of SMS initialization control information.
ACDS(dsname)	Identifies the name of the data set containing the active configuration. If the dsname is omitted, the operator is prompted for a value.
COMMDS(dsname)	Identifies the name of the communications data set. If the dsname is omitted, the operator is prompted for a value.
The following parameters are optional for SMS initialization. The underlined values indicate the product default values. Additional STIG requirements may apply depending on the parameter values in effect:	
USE_RESOWNER({YES|NO})	Indicates whether construct authorization checking is done using the RESOWNER value, which is based on the high-level qualifier of the data set name, or using the data set allocator userid. If YES is specified, the RESOWNER value in the DFP segment of the ACP data set profiles is used. If NO is specified, the RESOWNER value in the DFP segment of the ACP data set profiles is not used. The userid allocating the data set is used instead. Refer to *Section 10.2.5.1, Resource Ownership*, for additional information.
ACSDEFAULTS({YES|NO})	Indicates whether SMS initializes the following ACS routine variables from an additional call to the ACP: &APPLIC &DEF_DATACLAS &DEF_MGMTCLAS &DEF_STORCLAS If NO is specified, these variables have no values associated with them. The ACSDEFAULTS parameter is not applicable when USE_RESOWNER(NO) is specified.
OVRD_EXPDT({YES|NO})	Allows for the override of an expiration date when an unexpired SMS-managed DASD data set is deleted.

The parameter settings for member IGDSMSxx are at the discretion of the site. Parameter default values may change with product maintenance and newer releases of software. Therefore all optional parameter settings in *Table B-9, SMS INITIALIZATION PARAMETERS (in IGDSMSxx)* are explicitly coded to ensure desired operations.

- *(ZSMS0032: CAT II) The systems programmer will ensure that the parameters in the above table are defined in the IDGSMSxx members in parmlib.*
-

(3) Member IEFSSN*xx* activates the SMS subsystem to MVS.

IEFSSN*xx* is used to define SMS to MVS. The following is the keyword syntax for defining IEFSSN*xx*:

```
SUBSYS SUBNAME(SMS)
[INITRTN(IGDSSIIN) [INITPARM('ID=yy,PROMPT={NO     }']]
                                                  YES    ]]
                                                  [DISPLAY]]
```

Member IEFSSN*xx* supports the following parameters:

Table B-11. SUBSYSTEM INITIALIZATION PARAMETERS (in IEFSSN*xx*) (10.2.5.2 b)

SUBSYSTEM INITIALIZATION PARAMETERS (in IEFSSNxx)	
PARAMETERS	DESCRIPTION
Required Parameters:	
SUBSYS SUBNAME(SMS)	Identifies and defines the Storage Management Subsystem to MVS.
Optional Parameters:	
IGDSSIIN	Identifies the subsystem initialization routine IGDSSIIN for SMS.
ID={*xx*|<u>00</u>}	Specifies the SYS1.PARMLIB IGDSMS*xx* member to be used for initialization in two special cases: (1) When the value specified in the SMS parameter of IEASYSyy does not correspond to any IGDSMS*xx* and the default IGDSMS00 does not exist. (2) When initialization of software controlling PDSEs fails.
PROMPT={DISPLAY|YES|<u>NO</u>}	Indicates how much control the operator has during the rest of SMS initialization.

(4) Use the following STIG required SMS subsystem definition:

```
SUBSYS SUBNAME(SMS) INITRTN(IGDSSIIN)
```

- *(ZSMS0030: CAT II) The systems programmer will ensure that SMS IGDSSIIN parameters are defined in the IEFSSNxx member in parmlib.*

10.2.6 ACF2

Use the following STIG recommended ACF2 resource types:

FAC	FACILITY Resource Class
PGM	PROGRAM Resource Class
MGM	MGMTCLAS Resource Class
STR	STORCLAS Resource Class

10.2.6.1 SMS Classes

(1) Use the default CLASMAP definitions for MGMTCLAS and STORCLAS.

(2) Define resource rules for the MGMTCLAS resource class. The following is an example resource rule, replacing *management class* with a one to eight-character management class and *uid* with the user's UID string:

```
SET RESOURCE(MGM)
COMPILE * STORE
$KEY(management class) TYPE(MGM)
UID(uid) ALLOW
```

(3) Define resource rules for the STORCLAS resource class. The following is an example resource rule, replacing *storage class* with a one to eight-character storage class and *uid* with the user's UID string:

```
SET RESOURCE(STR)
COMPILE * STORE
$KEY(storage class) TYPE(STR)
UID(uid) ALLOW
```

- *(ZSMSA008: CAT II) The IAO will ensure that the MGMTCLAS and STORCLAS resource classes are defined to the GSO CLASSMAP record.*

(4) Ensure that the MGM and STR resource types of *r-rmgm* and *r-rstr* are defined within the GSO INFODIR. To find out if these resource types are defined in INFODIR, issue the SHOW ACF2 command. If the resource type is not defined, issue the following ACF2 commands:

```
ACF
SET CONTROL(GSO)
CHANGE INFODIR TYPE(R-RMGM R-RSTR) ADD
```

- *(ZSMSA004: CAT II) The IAO will ensure that r-rmgm, r-rstr, r-rfac and r-rpgm resource types are defined within the GSO INFODIR.*

  Issue the following Operator command to refresh the in-storage resource directory:

  F ACF2,REFRESH(INFODIR)

10.2.6.2 DFSMS/MVS Resource Controls

This section illustrates the rules required to implement the controls for DFSMS/MVS resources discussed throughout *Section 10.2.2, DFSMS/MVS Functions and Commands* in an ACF2 environment.

ACF2 processes SAF calls to the FACILITY resource class by default using the STIG recommended resource type FAC. No additional SAFDEF or CLASMAP definitions are required.

- *(ZSMSA006: CAT II) The IAO will ensure that Facility and Program resource classes are defined to the ACF2 GSO SAFDEF record.*

The following rule may be used to establish default protection for all DFSMS/MVS resources:

```
$KEY(STGADMIN) TYPE(FAC)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO ALL DFSMS -
    RESOURCES)
```

10.2.6.2.1 DFSMSdfp Resource Controls

The following rules may be used to control access to the DFSMSdfp resources discussed in *Section 10.2.2.1, DFSMSdfp Resource Protection*:

```
$KEY(STGADMIN) TYPE(FAC)
DPDSRN.olddsname UID(sysprog-group) SERVICE(READ) LOG -
    DATA(DFSMSDFP BYPASS DATA SET INTEGRITY CHECKING)
IDC.- UID(sysprog-group, storage-mgmt-group) SERVICE(READ) ALLOW -
    DATA(DFSMSDFP VARIOUS ACCESS METHOD SERVICES)
IGD.ACTIVATE.CONFIGURATION -
    UID(sysprog-group, storage-mgmt-group) SERVICE(READ) LOG -
        DATA(DFSMSDFP ACTIVATE SMS CONFIGURATION)
IGG.- UID(sysprog-group, storage-mgmt-group) SERVICE(READ) ALLOW -
    DATA(DFSMSDFP VARIOUS CATALOG MANAGEMENT -
        FUNCTIONS)
IGG.DEFDEL.UALIAS UID(sysprog-group, storage-mgmt-group, -
    security-group) SERVICE(READ) LOG DATA(DFSMSDFP DEFINE -
        AND DELETE USER ALIASES IN THE MASTER CATALOG)
```

```
IGWSHCDS.REPAIR UID(sysprog-group, storage-mgmt-group) -
    SERVICE(READ) ALLOW DATA(DFSMSDFP AMS SHCDS -
        COMMAND)
```

10.2.6.2.2 DFSMSdss Resource Controls

The following rules may be used to control access to the DFSMSdss resources discussed in *Section 10.2.2.2, DFSMSdss Resource Protection*:

```
$KEY(STGADMIN) TYPE(FAC)
ADR.- UID(sysprog-group, storage-mgmt-group) SERVICE(READ) ALLOW -
    DATA(DFSMSDSS NON ADMINISTRATOR FUNCTIONS)
ADR.COPY.CNCURRNT UID(end-user-group) SERVICE(READ) ALLOW -
    DATA(DFSMSDSS COPY COMMAND USING QUICK -
        SERIALIZATION)
ADR.COPY.TOLERATE.ENQF UID(end-user-group) SERVICE(READ) -
    ALLOW DATA(DFSMSDSS COPY COMMAND WHILE DATA SET IS -
        IN USE)
ADR.DUMP.CNCURRNT UID(end-user-group) SERVICE(READ) -
    ALLOW DATA(DFSMSDSS DUMP COMMAND USING QUICK -
        SERIALIZATION)
ADR.DUMP.TOLERATE.ENQF UID(end-user-group) SERVICE(READ) -
    ALLOW DATA(DFSMSDSS DUMP COMMAND WHILE DATA SET -
        IS IN USE)
ADR.RESTORE.TOLERATE.ENQF UID(end-user-group) -
    SERVICE(READ)   ALLOW DATA(DFSMSDSS RESTORE COMMAND -
        WHILE DATA SET IS IN USE)
ADR.STGADMIN.- UID(sysprog-group, storage-mgmt-group) -
    SERVICE(READ) LOG DATA(DFSMSDSS ADMINISTRATOR -
        FUNCTIONS)
```

10.2.6.3 PROGRAM Resource Class

(1) Ensure that an SAFDEF record is defined with the following information:

```
SAFDEF.PGM ID(PROGMCHK) MODE(GLOBAL)
RACROUTE(REQUEST=AUTH CLASS=PROGRAM REQSTOR=
    PROGMCHK SUBSYS=CONTENTS)
```

- *(ZSMSA006: CAT II) The IAO will ensure that Facility and Program resource classes are defined to the ACF2 GSO SAFDEF record.*

(2) Define resource rules for the PROGRAM resource class. The following is an example resource rule that may be entered:

```
SET RESOURCE(PGM)
COMPILE * STORE
$KEY(DGT*****) TYPE(PGM)
UID(SYS) ALLOW
UID(*) PREVENT
```

(3) Ensure that the PGM resource type of *r-rpgm* is defined within the GSO INFODIR. To find out if this resource type is defined in INFODIR, issue the SHOW ACF2 command. If the resource type is not defined, issue the following ACF2 commands:

```
ACF
SET CONTROL(GSO)
CHANGE INFODIR TYPE(R-RPGM) ADD
```

- *(ZSMSA004: CAT II) The IAO will ensure that r-rmgm, r-rstr, r-rfac and r-rpgm resource types are defined within the GSO INFODIR.*

  Issue the following Operator command to refresh the in-storage resource directory:

  ```
  F ACF2,REFRESH(INFODIR)
  ```

10.2.6.4 SMS Data Set Controls

The data sets described in *Section 10.2.4, SMS Data Set Controls,* are protected from unauthorized access to prevent the possible compromise of the SMS environment.

The following ACF2 commands can be used to protect these data sets, replacing *hlq* with the data set high-level qualifier, and *name* with the remaining portion of the data set name or mask (i.e., SMS.-.-) and replacing *uid* with the UID string:

(1) Grant access to storage administrators:

```
SET RULE
$KEY(hlq)
name UID(uid) READ(A) WRITE(L) EXEC(A)
```

(2) Grant access to personnel who perform file maintenance on the SMS data sets:

```
SET RULE
$KEY(hlq)
name UID(uid) READ(A) WRITE(L) ALLOC(L) EXEC(A)
```

(3) Grant access to all other personnel with a need to review or access the information within these SMS data sets, as required:

SET RULE
$KEY(*hlq*)
name UID(*uid*) READ(A) EXEC(A)

10.2.6.5 Additional Controls

10.2.6.5.1 Resource Ownership

For all data set profiles under SMS control, a resource owner is defined within the DFP segment using the following command as an example. Replace *hlq* with the data set high-level qualifier, *name* with the remaining portion of the data set name or mask, *dfp name* with the name of the DFP segment name, and *resowner* with the owner of this data set resource:

SET PROFILE(DATASET) DIVISION(PROFILE)
COMPILE
$KEY(*hlq*)
name DFP(*dfp name*)
SET PROFILE(DATASET) DIVISION(DFP)
INSERT *dfp name* RESOWNER(*resowner*)

A resource owner is assigned by including a $RESOWNER control statement in the corresponding rule set. The $RESOWNER control statement specifies the userid acting as the resource owner of the data set:

SET RULE
$KEY(SYS1)
$RESOWNER(SYSTEMS)
PARMLIB UID(SYS) READ(A) WRITE(L) ALLOC(L) EXEC(A)

10.2.6.5.2 System Parmlib Members

Standard controls are maintained over the system **parmlib**, as defined in *Section 2, OS/390 Integrity*. No additional ACP controls are required at this time.

10.2.7 RACF

Use the following default RACF resource classes:

FACILITY - FACILITY Resource Class
PROGRAM - PROGRAM Resource Class
STORCLAS - STORCLAS Resource Class
MGMTCLAS - MGMTCLAS Resource Class

10.2.7.1 SMS Classes and Groups

(1) Activate RACF general resource classes MGMTCLAS and STORCLAS, and place these resources in the RACLIST:

```
SETROPTS CLASSACT(MGMTCLAS STORCLAS) RACLIST
    (MGMTCLAS STORCLAS)
```

(2) Define the profile, where *class* is MGMTCLAS or STORCLAS, and *value* is the one to eight-character entry for the management class or storage class that is to be protected:

```
RDEFINE class value UACC(NONE)
```

(3) Selectively allow access to users requiring access to SMS. Use the following as a sample, replacing *user-id* with the userid of the user or a RACF Group:

```
PERMIT value CLASS(class) ID(user-id) ACCESS(READ)
```

(4) Refresh the RACLIST to effect the changes made to these resources:

```
SETROPTS RACLIST(MGMTCLAS STORCLAS) REFRESH
```

- *(ZSMSR008: CAT II) The IAO will ensure that MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resource classes are active and refreshed.*

10.2.7.2 DFSMS/MVS Resource Controls

This section illustrates the commands required to implement the controls for DFSMS/MVS resources discussed throughout *Section 10.2.2, DFSMS/MVS Functions and Commands* in a RACF environment.

The FACILITY resource class is used by several other products to control resource access and may already be configured properly. Ensure the FACILITY resource class is enabled for generic processing and is active.

The following commands may be used to activate generic processing for the FACILITY resource class:

```
SETROPTS GENERIC(FACILITY)
SETROPTS GENCMD(FACILITY)
```

After all the necessary resource profiles are defined, activate the FACILITY resource class to enable SAF protection. The following command may be used to activate the FACILITY resource class:

```
SETROPTS CLASSACT(FACILITY)
```

- *(ZSMSR008: CAT II) The IAO will ensure that MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resource classes are active and refreshed.*

The following command may be used to establish default protection for all DFSMS/MVS resources:

```
RDEFINE FACILITY STGADMIN.** UACC(NONE) OWNER(admin) -
   DATA('DEFAULT ACCESS TO ALL DFSMS RESOURCES')
```

10.2.7.2.1 DFSMSdfp Resource Controls

The following commands may be used to control access to the DFSMSdfp resources discussed in *Section 10.2.2.1, DFSMSdfp Resource Protection*:

```
RDEFINE FACILITY STGADMIN.DPDSRN.olddsname UACC(NONE) -
   OWNER(admin) DATA('DFSMSDFP BYPASS DATA SET INTEGRITY -
      CHECKING') AUDIT(ALL)
RDEFINE FACILITY STGADMIN.IDC.** UACC(NONE) -
   OWNER(admin) DATA('DFSMSDFP VARIOUS ACCESS METHOD -
      SERVICES')
RDEFINE FACILITY STGADMIN.IGD.ACTIVATE.CONFIGURATION -
   UACC(NONE) OWNER(admin) DATA('DFSMSDFP ACTIVATE SMS -
      CONFIGURATION') AUDIT(ALL)
RDEFINE FACILITY STGADMIN.IGG.** UACC(NONE) -
   OWNER(admin) DATA('DFSMSDFP VARIOUS CATALOG -
      MANAGEMENT FUNCTIONS')
RDEFINE FACILITY STGADMIN.IGG.DEFDEL.UALIAS UACC(NONE) -
   OWNER(admin) DATA('DFSMSDFP DEFINE AND DELETE USER -
      ALIASES IN THE MASTER CATALOG') AUDIT(ALL)
RDEFINE FACILITY STGADMIN.IGWSHCDS.REPAIR UACC(NONE) -
   OWNER(admin) DATA('DFSMSDFP AMS SHCDS COMMAND')
```

PERMIT STGADMIN.DPDSRN.*olddsname* CLASS(FACILITY) -
ID(*sysprog-group*) ACCESS(READ)
PERMIT STGADMIN.IDC.** CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group*) ACCESS(READ)
PERMIT STGADMIN.IGD.ACTIVATE.CONFIGURATION -
CLASS(FACILITY) ID(*sysprog-group storage-mgmt-group*) -
ACCESS(READ)
PERMIT STGADMIN.IGG.** CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group*) ACCESS(READ)
PERMIT STGADMIN.IGG.DEFDEL.UALIAS CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group security-group*) ACCESS(READ)
PERMIT STGADMIN.IGWSHCDS.REPAIR CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group*) ACCESS(READ)

10.2.7.2.2 DFSMSdss Resource Controls

The following commands may be used to control access to the DFSMSdss resources discussed in *Section 10.2.2.2, DFSMSdss Resource Protection*:

RDEFINE FACILITY STGADMIN.ADR.** UACC(NONE) -
OWNER(*admin*) DATA('DFSMSDSS NON ADMINISTRATOR -
FUNCTIONS')
RDEFINE FACILITY STGADMIN.ADR.COPY.CNCURRNT -
UACC(NONE) OWNER(*admin*) DATA('DFSMSDSS COPY -
COMMAND USING QUICK SERIALIZATION')
RDEFINE FACILITY STGADMIN.ADR.COPY.TOLERATE.ENQF -
UACC(NONE) OWNER(*admin*) DATA('DFSMSDSS COPY -
COMMAND WHILE DATA SET IS IN USE')
RDEFINE FACILITY STGADMIN.ADR.DUMP.CNCURRNT -
UACC(NONE) OWNER(*admin*) DATA('DFSMSDSS DUMP -
COMMAND USING QUICK SERIALIZATION')
RDEFINE FACILITY STGADMIN.ADR.DUMP.TOLERATE.ENQF -
UACC(NONE) OWNER(*admin*) DATA('DFSMSDSS DUMP -
COMMAND WHILE DATA SET IS IN USE')
RDEFINE FACILITY STGADMIN.ADR.RESTORE.TOLERATE.ENQF -
UACC(NONE) OWNER(*admin*) DATA('DFSMSDSS RESTORE -
COMMAND WHILE DATA SET IS IN USE')
RDEFINE FACILITY STGADMIN.ADR.STGADMIN.** UACC(NONE) -
OWNER(*admin*) DATA('DFSMSDSS ADMINISTRATOR -
FUNCTIONS') AUDIT(ALL)

PERMIT STGADMIN.ADR.** CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group*) ACCESS(READ)
PERMIT STGADMIN.ADR.COPY.CNCURRNT CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group end-user-group*) ACCESS(READ)
PERMIT STGADMIN.ADR.COPY.TOLERATE.ENQF CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group end-user-group*) ACCESS(READ)
PERMIT STGADMIN.ADR.DUMP.CNCURRNT CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group end-user-group*) ACCESS(READ)
PERMIT STGADMIN.ADR.DUMP.TOLERATE.ENQF -
CLASS(FACILITY) ID(*sysprog-group storage-mgmt-group* -
end-user-group) ACCESS(READ)
PERMIT STGADMIN.ADR.RESTORE.TOLERATE.ENQF -
CLASS(FACILITY) ID(*sysprog-group storage-mgmt-group* -
end-user-group) ACCESS(READ)
PERMIT STGADMIN.ADR.STGADMIN.** CLASS(FACILITY) -
ID(*sysprog-group storage-mgmt-group*) ACCESS(READ)

10.2.7.3 PROGRAM Resource Class

After all the necessary resource profiles are defined, activate the PROGRAM resource class to enable SAF protection. The following command may be used to activate the PROGRAM resource class:

SETROPTS CLASSACT(PROGRAM)

- *(ZSMSR008: CAT II) The IAO will ensure that MGMTCLAS, STORCLAS, PROGRAM, and FACILITY resource classes are active and refreshed.*

Define a PROGRAM profile to protect SMS programs. Protect the SMS programs and grant access to users as required, replacing *user-id* with the userid of the user or a RACF Group:

RDEFINE PROGRAM DGT* UACC(NONE)
ADDMEM('SYS1.DGTLLIB'//NOPADCHK)

PERMIT DGT* CLASS(PROGRAM) ID(*user-id*) ACCESS(READ)
(In the above command, replace DGT with the appropriate program name.)*

10.2.7.4 SMS Data Set Controls

Protect the data sets described in *Section 10.2.4, SMS Data Set Controls,* from unauthorized access to prevent the possible compromise of the SMS environment.

(1) Assign default protection for these data sets, replacing *data name* with the fully qualified data set name or a generic prefix (e.g., SYS1.SMS.**):

ADDSD '*data name*' UACC(NONE)

NOTE:: The above commands are only issued if the data set has not already been defined in a RACF data set profile.

(2) Permit access to those personnel who manage the SMS environment, replacing *user-id* with the userid of the user or a RACF Group:

PERMIT '*data name*' ID(*user-id*) ACCESS(UPDATE)

(3) Permit access to those personnel who perform maintenance on these data sets:

PERMIT '*data name*' ID(*user-id*) ACCESS(ALTER)

NOTE:: Issue the SECURITY command from the command line of the ISMF Data Set Application to protect these data sets.

10.2.7.5 Additional Controls

10.2.7.5.1 Resource Ownership

For all data set profiles under SMS control, define a resource owner within the DFP segment using the following command as an example. Replace *data-set* with the data set name or a generic prefix, *user-id* with the userid of the user or a RACF Group of the resource owner, and *access* with the default access for the data set:

ADDSD *data-set* DFP(RESOWNER(*user-id*)) UACC(*access*)
or
ALTDSD *data-set* DFP(RESOWNER(*user-id*))

10.2.7.5.2 System Parmlib Members

Standard controls are maintained over the system parmlib, as defined in *Section 2, OS/390 Integrity*. No additional ACP controls are required at this time.

10.2.8 TOP SECRET

Use the following default TSS resource classes:

IBMFAC - FACILITY Resource Class *(Not to be confused with the TSS resource.)*
PROGRAM - PROGRAM Resource Class
STORCLAS - STORCLAS Resource Class
MGMTCLAS - MGMTCLAS Resource Class

10.2.8.1 SMS Classes and Groups

(1) Assign the MGMTCLAS and STORCLAS resources for SMS to those personnel who administer access to them, replacing *user-id* with a user, department, or division and *class name* with the one to eight-character management or storage class:

TSS ADD(*user-id*) MGMTCLAS(*class name*)
TSS ADD(*user-id*) STORCLAS(*class name*)

(2) Selectively allow access to users requiring access to SMS, replacing *user-id* with the userid of the user, or a Group profile:

TSS PERMIT(*user-id*) MGMTCLAS(*class name*) ACCESS(READ)
TSS PERMIT(*user-id*) STORCLAS(*class name*) ACCESS(READ)

10.2.8.2 DFSMS/MVS Resource Controls

This section illustrates the commands required to implement the controls for DFSMS/MVS resources discussed throughout *Section 10.2.2, DFSMS/MVS Functions and Commands* in a TOP SECRET environment.

The FACILITY resource class used by IBM is identified by the IBMFAC resource class when using TOP SECRET. The IBMFAC resource class is predefined in the TOP SECRET RDT. No additional configuration of the IBMFAC entry in the RDT is required.

The following command may be used to establish default protection for all DFSMS/MVS resources:

TSS ADDTO(*dept-acid*) IBMFAC(STGADMIN.)

10.2.8.2.1 DFSMSdfp Resource Controls

The following commands may be used to control access to the DFSMSdfp resources discussed in *Section 10.2.2.1, DFSMSdfp Resource Protection*:

TSS PERMIT(*sysprog-group*) IBMFAC(STGADMIN.DPDSRN.*olddsname*)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.IDC.) ACCESS(READ)
TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.IGD.ACTIVATE.CONFIGURATION)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.IGG.) ACCESS(READ)
TSS PERMIT(*sysprog-group, storage-mgmt-group, security-group*)
IBMFAC(STGADMIN.IGG.DEFDEL.UALIAS)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.IGWSHCDS.REPAIR) ACCESS(READ)

10.2.8.2.2 DFSMSdss Resource Controls

The following commands may be used to control access to the DFSMSdss resources discussed in *Section 10.2.2.2, DFSMSdss Resource Protection*:

TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.ADR.) ACCESS(READ)
TSS PERMIT(*end-user-group*)
IBMFAC(STGADMIN.ADR.COPY.CNCURRNT) ACCESS(READ)
TSS PERMIT(*end-user-group*)
IBMFAC(STGADMIN.ADR.COPY.TOLERATE.ENQF)
ACCESS(READ)
TSS PERMIT(*end-user-group*)
IBMFAC(STGADMIN.ADR.DUMP.CNCURRNT) ACCESS(READ)
TSS PERMIT(*end-user-group*)
IBMFAC(STGADMIN.ADR.DUMP.TOLERATE.ENQF)
ACCESS(READ)
TSS PERMIT(*end-user-group*)
IBMFAC(STGADMIN.ADR.RESTORE.TOLERATE.ENQF)
ACCESS(READ)
TSS PERMIT(*sysprog-group, storage-mgmt-group*)
IBMFAC(STGADMIN.ADR.STGADMIN.) ACCESS(READ)
AUDIT(ALL)

10.2.8.3 PROGRAM Resource Class

(1) Assign ownership of the PROGRAM resource class for the ISMF programs to those personnel who administer access to them, replacing *user-id* with a user, department, or division:

TSS ADD(*user-id*) PROGRAM(DGT)

(2) Selectively grant access to the SMS programs, replacing *user-id* with the userid of the user or a Group profile or the ALL profile, and *program* with a program name or prefix:

TSS PERMIT(*user-id*) PROGRAM(*program*)

10.2.8.4 SMS Data Set Controls

The data sets described in *Section 10.2.4, SMS Data Set Controls*, are protected from unauthorized access to prevent the possible compromise of the SMS environment.

(1) Assign ownership of the data sets, replacing *user-id* with a user, department, or division that administer access to the SMS control data sets, and *data name* with the prefix of the SMS control data sets:

TSS ADD(*user-id*) DSN(*data name*)

(2) Permit access to those personnel who manage the SMS environment, replacing *user-id* with the userid of the user or a Group profile:

TSS PERMIT(*user-id*) DSN(*data name*) ACC(UPDATE) ACTION(AUDIT)

(3) Permit access to those personnel that perform maintenance on these data sets:

TSS PERMIT(*user-id*) DSN(*data name*) ACC(ALL) ACTION(AUDIT)

10.2.8.5 Additional Controls

10.2.8.5.1 Resource Ownership

For all data set profiles under SMS control, define a resource owner within the DFP segment using the following command as an example. Replace *user-id* with a user, department, or division, *data name* with the prefix of the SMS controlled data sets, and *resource-id* with a userid or control-type user:

TSS ADD(*user-id*) DSN(*data name*) RESOWNER(*resource-id*)

10.2.8.5.2 System Parmlib Members

Standard controls are maintained over the system parmlib, as defined in *Section 2, OS/390 Integrity*. No additional ACP controls are required at this time.

11. TAPE MANAGEMENT SOFTWARE

11.1 General Considerations

Tape management software products provide the facilities to control and manage the tape storage environment. They typically offer features such as real-time processing, tape data set retention, on-line inquiry and update, tape library maintenance, and scratch pool management.

Consideration should be given to securing the data sets that comprise the tape management system. Data sets containing the software product and information regarding the tape storage environment should be protected from unauthorized access and are restricted only to authorized personnel.

If an interactive application is available to access the tape management system, thought must be given to securing this facility. Access to on-line applications are prohibited from general use; access is granted only to authorized personnel. Some commands and features within the application provide the ability to modify the tape storage environment. These items are strictly controlled and restricted to individual(s) responsible for tape storage control, such as the tape librarian.

All security and product interfaces are carefully evaluated for possible system and data integrity problems and for potential security exposures. These include interfaces delivered with the tape management software, and interfaces offered by other software packages that may interact with the tape management system. These interfaces may offer their own internal security, provide the potential to circumvent ACP security controls, or expose weaknesses in protection.

Depending on the product, access authority can be controlled in one of the following three methods:

- Exclusive use of ACP controls
- A combination of ACP controls and Internal Product Security Controls
- Internal product security only

The IAO administers access authority assignments for users.

Use ACP controls whenever possible. However, it may not be possible to provide a totally secure environment using only ACP controls. In this case, the use of internal security may be warranted and investigated for possible use. If it is determined that an enhanced level of protection is gained that the ACP does not provide, the internal security may be activated. It is important to remember that base-level ACP controls are not to be compromised.

Use the following recommendations when securing access to tape management software:

(1) Control access to the software product's data sets, and restrict access only to authorized personnel.

(2) Strictly enforce access to the on-line applications, and restrict access only to authorized personnel.

(3) Rigidly control the use of commands, options, and functions within the products, and restrict it to those functions necessary for users to accomplish their assigned responsibilities.

(4) Review all interfaces for possible system and data integrity problems, and for potential security exposures. Document any potential security exposures. Notify DISA FSO and the vendor.

(5) The ACP controls access authority. Evaluate internal security for possible use, providing it does not replace or compromise existing ACP security controls.

11.2 CA-1

Vendor: Computer Associates

NOTE:: All the information in this section pertains to CA-1, Version 5.0 and above.

CA-1 is a comprehensive tape management system providing features such as real-time processing, tape data set retention, on-line inquiry and update, tape library maintenance, and scratch pool management. When active, CA-1 becomes an extension of the operating system, utilizing system-resident programs, and directly interfacing with the data management environment.

To establish this level of functionality, CA-1 takes advantage of several OS/390 facilities and performs dynamic modifications to the OS/390 operating system, including the following items:

(1) CA-1 X and Y SVCs are dynamically installed during initialization. Refer to *Section 2.1.2.4, Supervisor Calls (SVCs)*, for security guidelines.

(2) CA-1 module TMSSMF83 dynamically front-ends SMF exit IEFU83. Refer to *Section 2.1.2.6, OS/390 and Other Product Exits*, for security guidelines.

(3) CA-1 modules dynamically replace IBM label editor routines. Refer to *Section 2.1.2, Software Integrity*, for general security guidelines.

(4) The subsystem entry, TMS, is dynamically established during initialization rather than explicitly defined in SYS1.PARMLIB member IEFSSN*xx*. Refer to *Section 2.1.2, Software Integrity*, for general security guidelines.

NOTE:: By product design, the dynamic functions mentioned above are not performed by CA-1 modules. They are established by the CAIRIM component of the Computer Associates CA-90s product on behalf of CA-1.

(5) Several CA-1 modules require LPA residency. Refer to *Section 2.1.2.8, Link Pack Area*, for security guidelines.

(6) The CA-1 load library is specified in the system Linklist, and APF authorization is required. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* and *Section 2.1.2.9, Linklist*, for security guidelines.

Implement CA-1 security management by using a combination of ACP and internal product security controls.

11.2.1 Internal Security

Use the following recommendations with CA-1 internal product security:

(1) Use the CA-1 system password when deactivating, batch activating, and reinitializing CA-1. When executing TMSINIT after an operating system IPL, the IEFTMS0 WTOR message is displayed on the system console. The proper response is the CA-1 system password.

Starting with CA-1, Version 5.1, use an additional security check using the ACP. Refer to *Section 11.2.2, External Security*, for further information about TMSINIT security.

NOTE: The CA-1 default system password is common with all CA-1 systems. The default system password will be changed to a unique password**.**

- *(ZCA10020: CAT II) The systems programmer/IAO will ensure that the CA-1 default system password is changed.*

(2) Use CA-1 internal passwords to access the CA-1 ISPF application or the TIQ command processor. The CA-1 system password allows complete access to all on-line functions. Additional passwords with different degrees of functionality are defined by default, and are common to all CA-1 systems (as is the system password).

Use ACP controls to validate the authority to use the CA-1 internal passwords. Refer to *Section 11.2.2, External Security*, for further information about password security.

(3) Use the CA-1 system password when executing the TMSUDSNB utility to perform updates to TMC and Audit Control records and to TMC DSNB records.

Use ACP controls to supplement access authorization validation to these data sets. Refer to *Section 11.2.2, External Security*, for further information about the Y SVC and BATCH security interfaces.

(4) Do not implement CA-1 internal security for data set password protection.

11.2.2 External Security

CA-1 ACP security interfaces are controlled by options coded in CAI.PPOPTION, member TMOOPT*xx*. The specific required option settings are dependent on the ACP in use on the system. The STIG required settings are detailed in the CA-1 ACP-specific sections.

The ACP security interface options are as follows:

- CATSEC Option

  This option's purpose is to handle tape cataloging and un-cataloging as an external security call even if the external security system is not active.

  This option only applies to CA-1, Version 5.3 and above.

- OCEOV Option

  This option controls OPEN/CLOSE/EOV processing. Access authorization validation is performed for all tape data sets opened for *read*, *update*, or *data set creation*.

- PMASK Option

  This option is used by foreign Countries that do not support the special character masking specified by CA. Our recommendation is not to use this or to change the default specified by CA.

  This option only applies to CA-1, Version 5.3 and above.

- DSNB Option

  This option controls data set access authority for secondary data set(s) on a tape and works with the OCEOV option. When a secondary data set is opened, an access authorization check is performed on the primary, or first, data set on the tape along with the standard OCEOV call for the secondary data set.

  The access authority is the same as used with the OCEOV call for the secondary data set (e.g., *read*, *update*, or *data set creation*).

NOTE: This option may conflict with software products that conserve volume usage by stacking data sets on tapes. If this is the case, DSNB processing must be turned OFF in the TMOOPT00 options member.

- YSVC Option

  This option controls access to the Y SVC programs, which perform all direct access to the TMC and Audit data sets. It applies only to batch jobs and on-line users, and does not affect real-time tape processing.

  Two different resource names are checked to validate a user's access to the TMC and Audit data sets. YSVCUNCD is used for *unconditional* access and YSVCCOND is used for *conditional* access. Each can be checked for *read* and *update* authorities. For example, a user may have *read* access to YSVCUNCD and *update* access to YSVCCOND. This allows the user to read any record in the TMC and Audit data sets, and allows the user *conditional update* access to these same records. The resource class is CATAPE for both resources.

  Unconditional access authority allows a user to perform the desired function without further security processing. *Conditional* access authority allows a user to perform the desired function if the user also has the same level of access to the data set name in the TMC record being accessed.

- BATCH Option

  This option controls direct access to the Volume and DSNB records within the TMC. It applies only to batch jobs and on-line users, and does not affect real-time tape processing. It works along with Y SVC processing when *conditional* access has been granted. This check is bypassed for users granted Y SVC *unconditional* access.

- PSWD Option

  This option controls the use of CA-1 internal passwords for on-line access. The resource class is set to CATAPE, and the entity name is the actual CA-1 password itself.

- CMD Option

  This option controls the use of CA-1 commands under the CA-1 ISPF and TSO on-line applications. This is accomplished by setting the resource class to CACMD and the entity name to L0, followed by the first six characters of the command name.

The following commands can be secured with this interface:

ADD
CLEAN
CHECKIN
CHECKOUT
DELETE
ERASE
EXTEND
EXPIRE
RETAIN
SCRATCH

- FUNC Option

  This option controls the use of special real-time functions such as foreign tape processing (EXPDT=98000) and label processing (NL, NSL, BLP). The resource class is set to CATAPE. Based on the volume serial number, the entity name is the type of tape label followed by RES (defined to CA-1) or NORES (unknown to CA-1). Possible entity names are as follows:

  NLRES
  NLNORES
  NSLRES
  NSLNORES
  BLPRES
  BLPNORES

  The same applies to foreign tape processing. The entity name, FORNORES, is used for foreign tapes. The entity name, FORRES, is used when specifying EXPDT=98000 for tapes defined to the CA-1 system.

- SCRTCH Option

  When active, this option passes control to the user security exit, TMSUXnS, when TMSCLEAN flags a tape as scratch or deletes a DSNB record.

- UNDEF Option

  This option instructs CA-1 how to react if it encounters an undefined resource or if the ACP is not active. If this option is set to ALLOW, an ACP return code of 04 is changed to 00 and CA-1 processing continues as normal. If set to FAIL, an ACP return code of 04 is changed to 08, and CA-1 issues an error message and abends the task requiring CA-1 processing.

- CREATE Option

  This option controls the level of access authority needed to create a data set on tape. Each ACP has a unique value for *data set creation* (e.g., ACF2 is ALLOCATE, RACF is ALTER, and TOP SECRET is CREATE). Specifying these ACP-specific values for the CREATE option instructs tape data set creation to be processed in a manner similar to that of DASD data sets, including volume serial number access authorization checking. Setting this option to UPDATE allows tape data set creations to be handled with the access authority level of *update*, bypassing volume serial number checking.

- SECWTO Option

  This option controls execution access to the TMSINIT program following the initial CA-1 startup at IPL time. Additional WTOR messages are displayed at the system console requesting the issuer's ACP logonid and password to verify the authority to reinitialize, stop, or batch activate CA-1. The resource class set is CATAPE with possible entity names of REINIT, BATCH, and DEACT.

  This option only applies to CA-1, Version 5.2 and above. With CA-1, Version 5.1, these WTOR messages are always issued, unless modified by the TMSUXnS exit.

- UX0AUPD Option

  This option will eliminate a need to change the TMSUX2A exit. If yes is specified. Yes would allow you to alter fields in the TMC and would require that the TMSUX2A exit would need to be changed, which would require that it would need to be reviewed by FSO.

  This option only applies to CA-1, Version 5.3 and above.

- *(ZCA10010: CAT II) The systems programmer/IAO will ensure that the CA-1 external security options are specified in accordance with the above STIG requirements.*

11.2.3 Resource Controls

SMP/E is used to perform the installation and maintenance of CA-1. During SMP/E processing, CA-1 elements are installed in many data sets. Some may be shared with other CA software products.

A typical installation requires many CA-1 modules to reside in the operating system LPA and a Linklist data set with APF authorization. Refer to *Section 2.1.2.1, Authorized Program Facility (APF), Section 2.1.2.8, Link Pack Area*, and *Section 2.1.2.9, Linklist*, for security information regarding these areas.

11.2.3.1 Data Set Controls

Control access to CA-1 data sets, and restrict access only to authorized personnel. Use the following recommendations to control access to CA-1 data sets:

(1) Restrict users who need to access tape data set information (e.g., block size, counts) and information about creating jobs (e.g., *jobname*, *stepname*, or *ddname*) to the following:

Read authority to the TMC and Audit data sets
Program execute only authority to the CA-1 Linklist library

However, due to the unique file structure of the TMC and Audit data sets, CA-1 uses the YSVC programs to handle all direct I/O activity. Because standard OPEN/CLOSE macros are not used, typical data set security checks are not performed. Even if a user does not have *read* authority to these data sets, the YSVC programs can enable that user to read and update records within these files.

Therefore, control *read* access authority to the TMC and Audit data sets by the YSVCUNCD and YSVCCOND resource names. Typical users should be restricted to *conditional read* access. For further information about TMC and Audit data set access control, refer to *Section 11.2.2, External Security* (specifically, *YSVC Option* and *BATCH Option*).

If these users execute under an ISPF environment, grant additional access authority:

Read authority to the CA-1 ISPF application (i.e., panel, message, skeleton, and table data sets)

Program execute only authority to the CA-1 ISPF application load library

- *(ZCA10030: CAT II) The IAO will ensure that update and allocate access to CA-1 product data sets are limited to system programmers only, unless a letter justifying access is filed with the IAO.*

(2) Restrict tape librarians, CA-1 batch production jobs, and CA-1 started tasks to the following access authority:

Unconditional read and update authorities to the TMC, Audit, Retention, and Vault Pattern Description data sets

NOTE: Read and update authority to the TMC and Audit data sets are controlled by the YSVCUNCD and YSVCCOND resource names, and by standard ACP data set controls, because some CA-1 utilities use conventional OPEN/CLOSE methods.

Read authority to the CA-1 options data set

Read authority to the CA-1 ISPF application (i.e., panel, message, skeleton, and table data sets)

Program execute only authority to the CA-1 Linklist library and the ISPF application load library

CA-1 offers over 50 different batch utilities to help with the administration and support of the product. Some of these utilities allocate unique data set names within the JCL. They are non-SMP/E data sets with no pre-defined rules regarding CA-1 naming conventions. Review all CA-1 production JCL for unique data set names to ensure the appropriate access authority is granted to the job ID.

- *(ZCA10030: CAT II) The IAO will ensure that update and allocate access to CA-1 product data sets are limited to system programmers only, unless a letter justifying access is filed with the IAO.*

- *(ZCA10035: CAT II) The IAO will ensure that update and allocate access to CA-1 TMC and AUDIT data sets are limited to system programmers and update access is limited to tape librarians, unless a letter justifying access is filed with the IAO. All allocate access will be logged.*

(3) Systems programmers responsible for supporting CA-1 require complete access to all CA-1 product installation data sets, except for the TMC and Audit data sets.

Limit access to the TMC and Audit data sets to the authorities necessary to perform their assigned duties. In addition, grant *data set creation* authority to the TMC and Audit data sets only on an as-needed basis. The IAO maintains documentation for this modification and its requirements. Log all *data set creation* access to these data sets using ACP facilities.

- *(ZCA10030: CAT II) The IAO will ensure that update and allocate access to CA-1 product data sets are limited to system programmers only, unless a letter justifying access is filed with the IAO.*

- *(ZCA10035: CAT II) The IAO will ensure that update and allocate access to CA-1 TMC and AUDIT data sets are limited to system programmers and update access is limited to tape librarians, unless a letter justifying access is filed with the IAO. All allocate access will be logged.*

11.2.3.2 Sensitive Utility Controls

Control access to CA-1 sensitive utilities, and restrict access only to authorized personnel. The following table provides a list of CA-1 programs containing sensitive utilities and personnel to whom their use should be restricted. Refer to *Section 3.1.5.3, Sensitive Utility Controls*, for further information.

Table B-12. SENSITIVE UTILITY CONTROLS - CA-1 (11.2.3.2)

SENSITIVE UTILITY CONTROLS - CA-1	
PROGRAM NAME	LEGITIMATE USER
L0nnINIT (nn = CA-1 Release, e.g., 51, 52)	CA-1 and CAIRIM started task IDs, and systems personnel responsible for supporting CA-1
TMSCOPY	CA-1 batch job ID, and systems personnel responsible for supporting CA-1
TMSFORMT	Systems personnel responsible for supporting CA-1
TMSLBLPR	CA-1 started task ID, CA-1 batch job ID, and systems personnel responsible for supporting CA-1
TMSMULV	Systems personnel responsible for supporting CA-1
TMSREMOV	Systems personnel responsible for supporting CA-1
TMSTPNIT	Tape librarian
TMSUDSNB	Systems personnel responsible for supporting CA-1

11.2.3.3 On-line Application Controls

CA-1 offers two on-line applications for use when accessing TMC records. Users granted access to the TMC require access to these CA-1 on-line applications. The level of access to TMC data while under these applications is dependent on the CA-1 internal password entered by the user during application invocation. Access to CA-1 internal passwords is controlled and restricted only to authorized personnel.

A typical user granted *read* access to the TMC should be restricted to a password that is only capable of displaying data, not of modifying it. Conversely, the tape librarians should be granted the access necessary for them to administer and maintain the CA-1 system, allowing them to modify data fields within the TMC. Restrict user access to the appropriate CA-1 on-line application password to the one necessary for that user to accomplish the assigned responsibilities.

Refer to the item, *PSWD Option*, in *Section 11.2.2, External Security*, and to *Section 11.2.1, Internal Security,* for more information about application passwords. For information regarding ACP controls for CA-1 internal passwords, refer to the ACP-specific sections.

Additional protection is used to control access to specific commands while under the CA-1 on-line applications. These powerful commands are used to administer and maintain the tape inventory in the TMC and are strictly controlled. Restrict use of these commands only to the tape librarians, with one exception. The EXTEND and RETAIN commands may be granted to those users needing the functionality of extending the retention dates of tape data sets.

Refer to the item, *CMD Option*, in *Section 11.2.2, External Security*, for more information about application on-line commands. For information regarding ACP controls for CA-1 commands, refer to the ACP-specific sections.

11.2.3.4 Special Tape Handling Privileges

CA-1 provides the capability to control special tape handling functions (i.e., non-label and non-standard label tapes and foreign tapes) by invoking the Function Call security interface. Refer to the item, *FUNC Option*, in *Section 11.2.2, External Security* for more information on tape handling privileges. For information regarding ACP controls for tape handling privileges, refer to the ACP-specific sections.

Use the following recommendations for access to special tape handling functions:

(1) Access to CA-1 special tape handling privileges is controlled and restricted to authorized system-level support personnel only (e.g., systems programming, operations, tape management).

(2) Access authorization to the BLPRES privilege is tightly controlled and restricted to a limited number of authorized personnel. Access is granted at the user level and not at the group level. All access to the BLPRES resource is logged by the ACP.

(3) Access authorization to the FORRES privilege (i.e., foreign tape processing of in-house tapes) is prohibited as a rule. Unlike BLPRES where data set authorization checking is performed, FORRES processing allows complete access to any tape data set. Access to FORRES may be granted on an as needed basis. All access to the FORRES resource is logged by the ACP.

(4) Legitimate requirements may exist for users outside the system-level support realm to have access to special tape handling privileges for non-resident tapes. An example would be personnel responsible for the execution of an application that collects data from many diverse sources, and where:

    (a) The tapes do not have supported labels.

    (b) The volume of tapes being processed exceeds the capacity of the tape library staff to process (copy) in an effective and timely manner.

    (c) Staff expansion is not an option.

In such a case, access authorization to the NLNORES, NSLNORES, BLPNORES or FORNORES resources outside the system-level support realm may be permitted to a limited number of users. For these authorized users, the following recommendations are in effect:

- Access will be granted to specific individuals and not at the group level.
- All resource access will be logged by the ACP.
- Justification documentation with IAO approval is required and must be filed with the IAO.

- *(ZCA10040: CAT II) The systems programmer/IAO will ensure that CA-1 resources are protected in accordance with STIG requirements.*

11.2.3.5 TMSINIT Execution

CA-1 provides the capability to control TMSINIT program execution after the initial activation of CA-1 following an IPL. Refer to the item, *SECWTO Option*, in *Section 11.2.2, External Security*, for more information. For information regarding ACP controls, refer to the ACP-specific sections.

Access to TMSINIT execution (i.e., deactivation, batch activation, and re-initialization) is tightly controlled and restricted only to authorized personnel. General user access is strictly prohibited.

11.2.3.6 Resource Access Authorization Guidelines

The following table entries are guidelines regarding access authorizations to CA-1 resources:

Table B-13. RESOURCE ACCESS AUTHORIZATION GUIDELINES - CA-1 (11.2.3.6)

RESOURCE ACCESS AUTHORIZATION GUIDELINES - CA-1			
RESOURCE NAME	LEGITIMATE USER	ACCESS LEVEL	LOG
L0ADD	Tape librarian	READ	N
L0CLEAN	Tape librarian	READ	N
L0CHECKI	Tape librarian	READ	N
L0CHECKO	Tape librarian	READ	N
L0DELETE	Tape librarian	READ	N
L0ERASE	Tape librarian	READ	N
L0EXTEND	Tape librarian and users requiring the functionality of extending retention dates for tape data sets	READ	N

RESOURCE ACCESS AUTHORIZATION GUIDELINES - CA-1			
RESOURCE NAME	LEGITIMATE USER	ACCESS LEVEL	LOG
L0EXPIRE	Tape librarian	READ	N
L0RETAIN	Tape librarian and users requiring the functionality of extending retention dates for tape data sets	READ	N
L0SCRATC	Tape librarian	READ	N
NLRES	Tape librarian and technical support personnel	READ, UPDATE	N
NLNORES	Tape librarian and technical support personnel	READ, UPDATE	Y
NSLRES	Tape librarian and technical support personnel	READ, UPDATE	N
NSLNORES	Tape librarian and technical support personnel	READ, UPDATE	Y
BLPRES	Tape librarian and technical support personnel[1]	READ, UPDATE	Y
BLPNORES	Tape librarian and technical support personnel[2]	READ, UPDATE	Y
FORRES	Tape librarian	READ, UPDATE	Y
FORNORES	Tape librarian and technical support personnel	READ, UPDATE	Y
YSVCCOND	Users requiring tape data set processing	READ, UPDATE	N
YSVCUNCD	Tape librarian	READ, UPDATE	N
YSVCUNCD	Technical support personnel	READ	N
password	Users requiring access to CA-1 on-line applications for tape data set processing ***NOTE:*** Multiple passwords exist providing different levels of CA-1 functionality ranging from general user to tape librarian.	READ	N
REINIT	Operations staff and systems personnel responsible for supporting CA-1	READ	N
BATCH	Operations staff and systems personnel responsible for supporting CA-1	READ	N
DEACT	Operations staff and systems personnel responsible for supporting CA-1	READ	N

[1] Refer to *Section 3.1.4.3, Tape Label Bypass Privileges*, for further guidance on BLP privileges.
[2] Refer to *Section 3.1.4.3, Tape Label Bypass Privileges*, for further guidance on BLP privileges.

- *(ZCA10040: CAT II) The systems programmer/IAO will ensure that CA-1 resources are protected in accordance with STIG requirements.*

11.2.4 On-line Interfaces

CA-1 provides on-line applications that offer users the ability to perform interactive inquiry against, and update to, the TMC data set. These applications can be invoked while executing under several different software products by invoking the interfaces supplied by CA-1. If installed, these interfaces should be secured from unauthorized access from within these software products. For example, the ISPF and TSO interfaces should be secured by restricting them to the **clist**, which invokes the CA-1 application.

11.2.5 User Exits

CA-1 supplies several user exits that provide the ability to tailor CA-1 processing to the specific needs of each site's environment. Install and maintain all CA-1 user exits utilizing SMP/E. Two of these exits, TMSUXnA and TMSUXnS, provide the capabilities to bypass or modify ACP security controls in place.

Apply the following recommendations to the TMSUXnA and TMSUXnS exits:

(1) Fully document the usage and function of these exits.

(2) DISA FSO will perform a review and integrity analysis of the exit code.

(3) DISA FSO will approve the use of these exits. Use of these exits without approval is prohibited.

(4) The IAO will maintain all associated documentation.

Refer to *Section 2.1.2.6, OS/390 and Other Product Exits*, for security guidelines on exits.

- *(ZCA10050: CAT II) The IAO will ensure that CA-1 security exits in use are reviewed and approved by DISA Field Security Operations.*

11.2.6 ACF2

CA-1 external security utilizing ACF2 is accomplished in the manner described in this section.

The following CA-1 security options are in effect for all sites. Refer to *Section 11.2.2, External Security*, for a description of each option.

Table B-14. CA-1 SECURITY OPTIONS - ACF2 (11.2.6)

CA-1 SECURITY OPTIONS - ACF2	
OPTION	STANDARD VALUE
BATCH	YES
CATSEC	NO[3]
CMD	YES
CREATE	UPDATE[4]
DSNB	YES
FUNC	YES[5]
OCEOV	NO[6]
PMASK	Do not specify or change[3]
PSWD	YES
SCRTCH	NO
SECWTO	YES[7]
UNDEF	FAIL
UX0AUPD	NO[3] [8]
YSVC	YES

[3] Applies to CA-1, Version 5.3 and above.
[4] The vendor recommends setting the CREATE option to UPDATE to avoid volume serial number authorization verification. Otherwise, in an environment where volume access rules are not utilized, user access will be denied when creating a tape data set. Refer to *Section 11.2.2, External Security*, for more information about the CREATE parameter.
[5] The FUNC option provides supplementary security for BLP access. The tape label bypass privilege must still be specified in the ACF2 user LID record to allow access to BLP processing.
[6] The CA-1 security option, OCEOV, is set to NO because ACF2 obtains control of data set OPEN/CLOSE processing before the CA-1 intercept. The vendor recommends that the first security call be used and that this CA-1 control option be turned OFF. Therefore, TAPEDSN must be specified in the OPTS option in the ACF2 GSO record.
[7] Applies to CA-1, Version 5.2 and above.
[8] The UX0AUPD will specify YES only if you alter the fields in the TMC and the TMSUXxA is changed.

- *(ZCA10010: CAT II) The systems programmer/IAO will ensure that the CA-1 external security options are specified in accordance with the above STIG requirements.*
-

11.2.6.1 Defining Resource Types

Define two CA-1 resource types — CAT (for CATAPE resources) and CAC (for CACMD resources). The following ACF2 commands add these types to the resident directory:

```
SET CONTROL(GSO)
CHANGE INFODIR TYPES(D-CAT,D-CAC) ADD
```

Then issue the REFRESH command for INFODIR:

```
F ACF2,REFRESH(INFODIR)
```

11.2.6.2 Defining Access Rules

Protect CA-1 data sets using ACP data set resource controls. Refer to *Section 11.2.3, Resource Controls*, for information on CA-1 data set access authority assignments. For additional information on data set resource controls, refer to *Sections 3.1.5.1* and *3.2.5.1*, both entitled *Data Set Controls*.

Unique CA-1 resources are protected. Restrict access to those resources necessary for users to accomplish their assigned responsibilities. The following table lists the resource types and names that must be defined, along with a short description of each. Refer to *Section 11.2.2, External Security*, for more information about these resource names.

Table B-15. DEFINING RULES - ACF2 (11.2.6.2)

DEFINING RULES - ACF2		
RESOURCE TYPE	RESOURCE NAME	DESCRIPTION
CAC	L0ADD	On-line command ADD
CAC	L0CHECKI	On-line command CHECKIN
CAC	L0CHECKO	On-line command CHECKOUT
CAC	L0CLEAN	On-line command CLEAN
CAC	L0DELETE	On-line command DELETE
CAC	L0ERASE	On-line command ERASE
CAC	L0EXPIRE	On-line command EXPIRE
CAC	L0EXTEND	On-line command EXTEND
CAC	L0RETAIN	On-line command RETAIN
CAC	L0SCRATC	On-line command SCRATCH

DEFINING RULES - ACF2		
RESOURCE TYPE	RESOURCE NAME	DESCRIPTION
CAT	BLPNORES	Bypass label processing for a tape undefined to CA-1
CAT	BLPRES	Bypass label processing for a tape defined to CA-1
CAT	FORNORES	Foreign tape undefined to CA-1
CAT	FORRES	Foreign tape defined to CA-1
CAT	NLNORES	Non-label tape undefined to CA-1
CAT	NLRES	Non-label tape defined to CA-1
CAT	NSLNORES	Non-standard label tape undefined to CA-1
CAT	NSLRES	Non-standard label tape defined to CA-1
CAT	YSVCCOND	Y SVC conditional access
CAT	YSVCUNCD	Y SVC unconditional access
CAT	*password*	CA-1 internal password used to access CA-1 on-line applications ***NOTE:*** A rule is written for each available password, including default passwords.
CAT	REINIT	TMSINIT re-initialization
CAT	BATCH	TMSINIT batch status
CAT	DEACT	TMSINIT deactivation

11.2.6.3 Resource Rule Examples

Following are some resource rule examples:

(1) Allow a user access to the CA-1 on-line application command **DELETE**:

```
$KEY(L0DELETE) TYPE(CAC)
UID(xxxxxxxx) ALLOW
```

(2) Allow all users *conditional read* access to the TMC and Audit data sets:

```
$KEY(YSVCCOND) TYPE(CAT)
UID(*) SERVICE(READ) ALLOW
```

(3) Allow users (e.g., the tape librarian) complete *read* and *update* access to all records in the TMC and Audit data sets regardless of their data set access:

$KEY(YSVCUNCD) TYPE(CAT)
UID(*xxxxxxxx*) SERVICE(READ,UPDATE) ALLOW

(4) Allow a user *read* access to tapes not controlled by CA-1 using BLP processing:

$KEY(BLPNORES) TYPE(CAT)
UID(*xxxxxxxx*) SERVICE(READ) ALLOW

(5) Allow a user access to the CA-1 on-line application password SYSPROG:

$KEY(SYSPROG) TYPE(CAT)
UID(*xxxxxxxx*) ALLOW

(6) Allow a user access to deactivate and reinitialize CA-1:

$KEY(DEACT) TYPE(CAT)
UID(*xxxxxxxx*) ALLOW

$KEY(REINIT) TYPE(CAT)
UID(*xxxxxxxx*) ALLOW

11.2.6.4 Defining the CA-1 STC

The logonid assigned to the started task that initializes CA-1 has *read* and *update* authority to the YSVCUNCD *or* YSVCCOND resource name.

11.2.7 RACF

CA-1 external security utilizing RACF is be accomplished in the manner described in this section.

The following CA-1 security options are in effect for all sites. Refer to *Section 11.2.2, External Security*, for a description of each option.

Table B-16. CA-1 SECURITY OPTIONS - RACF (11.2.7)

CA-1 SECURITY OPTIONS - RACF	
OPTION	STANDARD VALUE
BATCH	YES
CATSEC	NO[9]
CMD	YES
CREATE	UPDATE[10]
DSNB	YES
FUNC	YES[11]
OCEOV	NO[12]
PMASK	Do not specify or change
PSWD	YES
SCRTCH	NO
SECWTO	YES[13]
UNDEF	FAIL
UX0AUPD	NO[9] [14]
YSVC	YES

[9] Applies to CA-1, Version 5.3 and above.
[10] The vendor recommends setting the CREATE option to UPDATE to avoid volume serial number authorization verification. Otherwise, in an environment where volume access rules are not utilized, user access will be denied when creating a tape data set. Refer to Section 11.2.2, External Security, for more information about the CREATE parameter.
[11] The FUNC option provides supplementary security for BLP access. Users who require the tape label bypass privilege must still be granted authority to profile ICHBLP in class FACILITY.
[12] The vendor recommends that OCEOV be set to NO and the RACF SETROPTS option TAPEDSN be active. Be advised that if OCEOV is disabled and RACF TAPEDSN is not active, tape data set protection will not be in effect.
[13] Applies to CA-1, Version 5.3 and above.
[14] The UX0AUPD will specify YES only if you alter the fields in the TMC and the TMSUXxA is changed.

- *(ZCA10010: CAT II) The systems programmer/IAO will ensure that the CA-1 external security options are specified in accordance with the above STIG requirements.*

11.2.7.1 Assembling the Class Descriptor Table

Use the following recommendations to assemble the Class Descriptor Table:

(1) The Class Descriptor Table, ICHRRCDE, is used to describe resource classes to RACF. Two new CA-1 classes, CA@MD and CA@APE, must be added to this table with the following entries:

```
ICHERCDE CLASS=CA@MD,          CA-1 COMMAND CHECKING
    ID=128,
    FIRST=ALPHA,
    OTHER=ANY,
    POSIT=25,
    DFTUACC=NONE

ICHERCDE CLASS=CA@APE,         CA-1 RESOURCE CHECKING
    ID=129,
    FIRST=ALPHA,
    OTHER=ANY,
    POSIT=26,
    DFTUACC=NONE
```

NOTE 1: An IPL of the operating system is required for these changes to take effect.

NOTE 2: The values specified for ID and POSIT are site-specific, and may be changed if necessary. Refer to the IBM RACF Macros and Interfaces manual for more information.

(2) Assemble and link-edit ICHRRCDE into SYS1.LINKLIB. Install and maintain this table using IBM's SMP/E.

11.2.7.2 Assembling the RACF Router Table

Use the following recommendations to assemble the RACF Router Table:

(1) The RACF Router table, ICHRFR01, associates OS/390 Router invocations with RACF functions. The following two entries are required by CA-1 and must be added to this table:

```
ICHRFRTB CLASS=CA@MD,          CA-1 COMMAND PROCESSING
    ACTION=RACF

ICHRFRTB CLASS=CA@APE,         CA-1 RESOURCE PROCESSING
    ACTION=RACF
```

NOTE: An IPL of the operating system is required for these changes to take effect.

(2) Assemble and link-edit ICHRFR01 into SYS1.LINKLIB. Install and maintain this table using IBM's SMP/E.

11.2.7.3 Defining CA-1 Resources to RACF

The RACF RDEFINE command may be used to define all CA-1 resources belonging to the new classes specified in the Class Descriptor Table. The following table lists the TSO RACF commands that can be used to define these resources. A short description of each resource is included. Refer to *Section 11.2.2, External Security*, for more information about CA-1 resources.

Table B-17. DEFINING CA-1 RESOURCES TO RACF (11.2.7.3)

DEFINING CA-1 RESOURCES TO RACF	
RACF COMMAND	DESCRIPTION
RDEFINE CA@MD (L0CLEAN) UACC(NONE)	On-line command CLEAN
RDEFINE CA@MD (L0EXTEND) UACC(NONE)	On-line command EXTEND
RDEFINE CA@MD (L0EXPIRE) UACC(NONE)	On-line command EXPIRE
RDEFINE CA@MD (L0RETAIN) UACC(NONE)	On-line command RETAIN
RDEFINE CA@MD (L0DELETE) UACC(NONE)	On-line command DELETE
RDEFINE CA@MD (L0ADD) UACC(NONE)	On-line command ADD
RDEFINE CA@MD (L0CHECKI) UACC(NONE)	On-line command CHECKIN
RDEFINE CA@MD (L0CHECKO) UACC(NONE)	On-line command CHECKOUT
RDEFINE CA@MD (L0ERASE) UACC(NONE)	On-line command ERASE
RDEFINE CA@MD (L0SCRATC) UACC(NONE)	On-line command SCRATCH
RDEFINE CA@APE (YSVCCOND) UACC(NONE)	Y SVC conditional
RDEFINE CA@APE (YSVCUNCD) UACC(NONE)	Y SVC unconditional
RDEFINE CA@APE (NLRES) UACC(NONE)	Non-label tape defined to CA-1
RDEFINE CA@APE (NLNORES) UACC(NONE)	Non-label tape undefined to CA-1
RDEFINE CA@APE (NSLRES) UACC(NONE)	Non-standard label tape defined to CA-1
RDEFINE CA@APE (NSLNORES) UACC(NONE)	Non-standard label tape undefined to CA-1
RDEFINE CA@APE (BLPRES) UACC(NONE)	Bypass label processing for a tape defined to CA-1

DEFINING CA-1 RESOURCES TO RACF	
RACF COMMAND	DESCRIPTION
RDEFINE CA@APE (BLPNORES) UACC(NONE)	Bypass label processing for a tape undefined to CA-1
RDEFINE CA@APE (FORRES) UACC(NONE)	Foreign tape defined to CA-1
RDEFINE CA@APE (FORNORES) UACC(NONE)	Foreign tape undefined to CA-1
RDEFINE CA@APE (*password*) UACC(NONE)	CA-1 internal password used to access CA-1 on-line applications ***NOTE:*** A rule is written for each available password, including default passwords.
RDEFINE CA@APE (REINIT) UACC(NONE)	TMSINIT re-initialization
RDEFINE CA@APE (BATCH) UACC(NONE)	TMSINIT batch status
RDEFINE CA@APE (DEACT) UACC(NONE)	TMSINIT deactivation

11.2.7.4 Assigning Resource Access Authority

Protect CA-1 data sets using ACP data set resource controls. Refer to *Section 11.2.3, Resource Controls*, for information about CA-1 data set access authority assignments. For additional information on data set resource controls, refer to *Sections 3.1.5.1* and *3.3.5.1*, both entitled *Data Set Controls*.

Protect the unique CA-1 resources defined with the RDEFINE command from unauthorized access. Restrict access to those resources necessary for users to accomplish their assigned responsibilities. The RACF PERMIT command can be used to perform this task. The following are examples of assigning resource access authority:

(1) Permit a user access to the CA-1 on-line application command DELETE:

PERMIT L0DELETE CLASS(CA@MD) ACCESS(READ) ID(*user1*)

(2) Permit users (e.g., the tape librarian) complete *read* and *update* access to all records in the TMC and Audit data sets, regardless of their data set access:

PERMIT YSVCUNCD CLASS(CA@APE) ACCESS(UPDATE) ID(*user1*)

(3) Permit a user *read* access to tapes not controlled by CA-1 using BLP processing:

PERMIT BLPNORES CLASS(CA@APE) ACCESS(READ) ID(*user1*)

(4) Permit a user access to the CA-1 on-line application password SYSPROG:

PERMIT SYSPROG CLASS(CA@APE) ACCESS(READ) ID(*user1*)

(5) Permit a user access to deactivate and reinitialize CA-1:

PERMIT DEACT CLASS(CA@APE) ACCESS(READ) ID(*user1*)
PERMIT REINIT CLASS(CA@APE) ACCESS(READ) ID(*user1*)

11.2.7.5 Activating the CA-1 Classes

The RACF SETROPTS command is used to activate CA-1 security classes that were added to the Class Descriptor Table. The following example can be used to activate these classes:

SETROPTS CLASSACT(CA@CMD,CA@APE)

The vendor recommends that TAPEVOL not be activated.

11.2.7.6 Defining the CA-1 STC

The started task that initializes CA-1 has a matching profile defined to the STARTED resource class. The userid associated with the CA-1 initialization STC is defined as a PROTECTED userid. The CA-1 STC userid has both *read* and *update* authority to the YSVCUNCD *or* YSVCCOND resource name.

11.2.8 TOP SECRET

CA-1 external security utilizing TOP SECRET is accomplished in the manner described in this section.

The following CA-1 security options are in effect for all sites. Refer to *Section 11.2.2, External Security*, for a description of each option.

Table B-18. CA-1 SECURITY OPTIONS - TOP SECRET (11.2.8)

CA-1 SECURITY OPTIONS - TOP SECRET	
OPTION	STANDARD VALUE
BATCH	YES
CATSEC	YES[15]
CMD	YES
CREATE	UPDATE[16]
DSNB	YES
FUNC	YES[17]
OCEOV	YES[18]
PMASK	Do not specify or change
PSWD	YES
SCRTCH	NO
SECWTO	YES[19]
UNDEF	FAIL
UX0AUPD	NO[15 20]
YSVC	YES

[15] Applies to CA-1, Version 5.3 and above.
[16] The vendor recommends setting the CREATE option to UPDATE to avoid volume serial number authorization verification. Otherwise, in an environment where volume access rules are not utilized, user access will be denied when creating a tape data set. Refer to *Section 11.2.2, External Security*, for more information about the CREATE parameter.
[17] The FUNC option provides supplementary security for BLP access. The tape label bypass privilege must still be specified in the TOP SECRET user ACID record to allow access to BLP processing.
[18] The data set OPEN/CLOSE security call will be handled by the CA-1 interface. To avoid duplication of security checking, the control option TAPE should be turned OFF in the TOP SECRET Control Options record.
[19] Applies to CA-1, Version 5.2 and above.
[20] The UX0AUPD will specify YES only if you alter the fields in the TMC and the TMSUXxA is changed.

- *(ZCA10010: CAT II) The systems programmer/IAO will ensure that the CA-1 external security options are specified in accordance with the above STIG requirements.*

11.2.8.1 Assigning Entity Ownership

The following table provides a list of commands that can be used to assign ownership of CA-1 entities within TOP SECRET. A short description of each entity is included. The IAO is assigned ownership of all CA-1 entities. Refer to *Section 11.2.2, External Security*, for more information about these entities.

Table B-19. ASSIGNING ENTITY OWNERSHIP - TOP SECRET (11.2.8.1)

ASSIGNING ENTITY OWNERSHIP - TOP SECRET	
TOP SECRET COMMAND	DESCRIPTION
TSS ADD(*dept-acid*) CACMD(L0CLEAN)	On-line command CLEAN
TSS ADD(*dept-acid*) CACMD(L0EXTEND)	On-line command EXTEND
TSS ADD(*dept-acid*) CACMD(L0EXPIRE)	On-line command EXPIRE
TSS ADD(*dept-acid*) CACMD(L0RETAIN)	On-line command RETAIN
TSS ADD(*dept-acid*) CACMD(L0DELETE)	On-line command DELETE
TSS ADD(*dept-acid*) CACMD(L0ADD)	On-line command ADD
TSS ADD(*dept-acid*) CACMD(L0CHECKI)	On-line command CHECKIN
TSS ADD(*dept-acid*) CACMD(L0CHECKO)	On-line command CHECKOUT
TSS ADD(*dept-acid*) CACMD(L0ERASE)	On-line command ERASE
TSS ADD(*dept-acid*) CACMD(L0SCRATC)	On-line command SCRATCH
TSS ADD(*dept-acid*) CATAPE(YSVCCOND)	Y SVC conditional access
TSS ADD(*dept-acid*) CATAPE(YSVCUNCD)	Y SVC unconditional access
TSS ADD(*dept-acid*) CATAPE(NLRES)	Non-label tape defined to CA-1
TSS ADD(*dept-acid*) CATAPE(NLNORES)	Non-label tape undefined to CA-1
TSS ADD(*dept-acid*) CATAPE(NSLRES)	Non-standard label tape defined to CA-1
TSS ADD(*dept-acid*) CATAPE(NSLNORES)	Non-standard label tape undefined to CA-1
TSS ADD(*dept-acid*) CATAPE(BLPRES)	Bypass label processing for a tape defined to CA-1
TSS ADD(*dept-acid*) CATAPE(BLPNORES)	Bypass label processing for a tape undefined to CA-1
TSS ADD(*dept-acid*) CATAPE(FORRES)	Foreign tape defined to CA-1
TSS ADD(*dept-acid*) CATAPE(FORNORES)	Foreign tape undefined to CA-1

ASSIGNING ENTITY OWNERSHIP - TOP SECRET	
TOP SECRET COMMAND	DESCRIPTION
TSS ADD(*dept-acid*) CATAPE(*password*)	CA-1 internal password used to access CA-1 on-line applications ***NOTE:*** A rule is written for each available password.
TSS ADD(*dept-acid*) CATAPE(REINIT)	TMSINIT re-initialization
TSS ADD(*dept-acid*) CATAPE(BATCH)	TMSINIT batch status
TSS ADD(*dept-acid*) CATAPE(DEACT)	TMSINIT deactivation

11.2.8.2 Permitting Entity Access

Protect CA-1 data sets using ACP data set resource controls. Refer to *Section 11.2.3, Resource Controls*, for information about CA-1 data set access authority assignments. For additional information on data set resource controls, refer to *Sections 3.1.5.1* and *3.4.5.1*, both entitled *Data Set Controls*.

Once ownership is assigned, user access must be permitted. Restrict access to those entities necessary for users to accomplish their assigned responsibilities. The following are examples of the use of the TOP SECRET PERMIT command:

(1) Permit a user access to the CA-1 on-line application command DELETE:

TSS PERMIT(*user01*) CACMD(L0DELETE)

(2) Permit users (e.g., the tape librarian) complete *read* and *update* access to all records in the TMC and Audit data sets, regardless of their data set access:

TSS PERMIT(*user01*) CATAPE(YSVCUNCD) ACCESS(READ,UPDATE)

(3) Permit a user *read* access to tapes that are not controlled by CA-1 using BLP processing:

TSS PERMIT(*user01*) CATAPE(BLPNORES) ACCESS(READ)

(4) Permit a user access to the CA-1 on-line application password SYSPROG:

TSS PERMIT(*user01*) CATAPE(SYSPROG)

(5) Permit a user access to deactivate and reinitialize CA-1:

TSS PERMIT(*user01*) CATAPE(DEACT)
TSS PERMIT(*user01*) CATAPE(REINIT)

11.2.8.3 Defining the CA-1 STC and Facility

Define the started task, ACID, and Facility for CA-1, and grant the appropriate accesses to personnel requiring CA-1 user privileges.

(1) Create the ACID for the CA-1 started task:

TSS CREATE(*CA1*) NAME(*CA1 STC Name*) TYPE(USER) DEPT(*dept-name*)
PASS(*password*,0) FAC(STC) SOURCE(INTRDR)

(2) Define the started task that initializes CA-1 to the STC table. For example:

TSS ADD(STC) PROCNAME(*CA1 STC Name*) ACID(*CA1 ACID*)

This *CA-1 ACID* has both *read* and *update* authority to the YSVCUNCD or YSVCCOND resource name.

(3) Define a Facility for CA-1 with the following attributes:

FACILITY DISPLAY FOR *CA1 Facility Name*

INITPGM=TMS ID=C1 TYPE=099
ATTRIBUTES=SHRPRF,NOASUBM,NOABEND,MUAS,NOXDEF,NOLUMSG
ATTRIBUTES=NOSTMSG,SIGN(M),INSTDATA,NORNDPW,AUTHINIT
ATTRIBUTES=NOPROMPT,NOAUDIT,RES,NOWARNPW,NOWSOC,
LCFCMD
ATTRIBUTES=MSGLC,NOTRACE,NOEODINIT,IJU,NODORMPW,NONPWR
ATTRIBUTES=NOIMSXTND
MODE=FAIL DOWN=GLOBAL LOGGING=INIT,SMF,MSG,SEC9
UIDACID=8 LOCKTIME=000 DEFACID=*NONE* KEY=8

(4) Add the *CA1 Facility Name* as the Master Facility to the *CA1 ACID* as in the following example:

TSS ADD(*CA1 ACID*) MASTFAC(*CA1 Facility Name*)

(5) Data center personnel authorized to execute TMSINIT as an STC are required to access the CA-1 Facility. This can be accomplished as follows:

TSS ADD(*User ACID*) FACILITY(*CA1 Facility Name*)

NOTE: Access to the CA-1 Facility is to be controlled and restricted only to authorized personnel.

12. SYSTEM MONITORING SOFTWARE

12.1 General Considerations

System monitoring software products provide systems programming personnel the ability to monitor, control, interrogate, modify, and analyze operating system components, subsystems, and executing tasks.

Consideration should be given to securing the data sets that contain the system monitoring software products. Access to these data sets is not permitted to general users, and should only be granted to authorized personnel.

Interactive execution of the system monitoring software products may be invoked from a TMP or a VTAM session. Only authorized personnel should have these products listed as options on a display menu or panel. Access to these on-line applications is prohibited from general users and should only be granted to authorized users.

Most system monitoring software products can perform I&A checking before product invocation. For these products, I&A validation is mandatory. The I&A checking is performed by the Access Control Product. This requirement provides protection against unauthorized access to the product.

System monitoring software products are very powerful and require proper control. They have many commands that pose potential integrity risks if not adequately protected. These products provide sensitive capabilities including the abilities to view and change system main storage (core), update the APF list, update the Linklist, and modify the resident LPA with temporary changes.

Sample exits, which interface with the ACPs, are provided with the system monitoring software products. Use these exits to restrict access to the product and to its internal commands. Protect all commands providing the capability to alter integrity (refer to *Section 2, OS/390 Integrity*) or to display sensitive data. Only grant authority for these critical commands to authorized users.

The IAO is responsible for the administration of access to these products.

Use ACP controls whenever possible. Review all ACP resource interfaces for potential security exposures and for possible implementation. However, it may not be possible to provide a secure environment using only ACP controls. In this case, the use of internal security may be warranted and should be investigated for possible use. If it is determined that an enhanced level of protection is gained that the ACP does not provide, the internal security may be activated. It is important to remember that base-level ACP controls are never compromised.

Use the following recommendations when securing access to system monitoring software:

(1) Control access to the software product's data sets, and restrict access only to authorized personnel.

(2) Strictly enforce access to the on-line applications, and restrict access only to authorized personnel.

(3) All system monitoring software products in use at DOD sites, which are capable of performing I&A checking, are required to do so during the logon process.

(4) Rigidly enforce the use of commands, options, and features within the products. Restrict use to that which is necessary for a user to accomplish that user's assigned responsibilities.

(5) Review product interfaces for potential security exposures. Document any potential security exposures. Notify DISA FSO and the vendor of such exposures.

(6) Evaluate system monitoring software product internal security for possible use, providing it does not replace or compromise existing ACP security controls.

- *(ZOMG0010: CAT II) The IAO will ensure that OMEGAMON product libraries are protected in accordance with STIG requirements.*

12.2 OMEGAMON Performance Monitors

12.2.1 General Considerations and Overview

OMEGAMON software products are provided by the Candle Corporation. These products are used to monitor the performance of the mainframe platforms at sites.

OMEGAMON originally was a single stand-alone performance monitor for MVS. It has evolved to become a suite of products providing comprehensive monitoring for the entire enterprise. The individual components of the suite use a common set of services, including exits to interface with the resident ACP and resources to control access to product commands. They have the flexibility to monitor the system in a variety of configurations. This results in several important considerations:

(1) The OMEGACENTER Network Access Manager (NAM) can either serve as a stand-alone security system, or provide an interface to the ACP (such as ACF2, RACF, and TOP SECRET). The DOD standard is to use the resident ACP for I&A validation. The OMEGACENTER NAM be configured to use the Access Control Product.

(2) The individual product sections that follow often make duplicate references to installing the appropriate ACP interface exit. The ACP exit is only installed once for the entire suite, not once for each component.

(3) Access to internal OMEGAMON commands is done in a tiered fashion. The vendor groups commands into one of four categories. Access is granted based on access to the categories, or levels, of commands. The STIG recommendation is to control access to these levels of commands based on ACP resource protections. Sites may, at their discretion, use the ACP to control each individual command.

(4) Some of the installation instructions (e.g., OMEGAMON II for VTAM) make no mention of defining resource controls for the available internal commands. Access to commands in this case is achieved based on the (common) resource controls defined during the installation of another component (e.g., OMEGAMON II for MVS).

(5) Several OMEGAMON components require that the user be defined to the Network Access Manager (the OMEGAMON internal security system), even when user I&A validation is done by the resident ACP.

(6) By default, the first user to log on to the products is assigned Administrator Authority. This authority is to be reviewed and updated as necessary, to ensure that Administrator Authority is delegated to the appropriate individual(s) (i.e., not necessarily to the first systems programmer to log on to OMEGAMON). In addition, the following products from the OMEGAMON suite will have the system *emergency userids* (refer to *Section 3.1.2.6 , Emergency Userids*, for further information) assigned as Administrators to recover from No Administrator Defined situations:

OMEGAVIEW
OMEGAMON II for VTAM
OMEGAMON II for SMS
OMEGAMON II for MVS
OMEGAMON II for CICS

- *(ZOMG0020: CAT II) The IAO will ensure that Emergency Ids are defined as OMEGAMON administrators.*

(7) OMEGAMON software products can run in any of the following three real-time operating modes:

Dedicated Mode	This mode offers high availability and requires a dedicated system console, with the exception of OMEGAMON II for VTAM that requires a dedicated VTAM terminal.
VTAM Mode	This mode uses VTAM for telecommunications access and requires a VTAM definition for the application program. Users log on to the applications as they would to other VTAM applications (e.g., TSO, CICS, etc.). In VTAM mode the products can be accessed directly from VTAM, or via a Session Manager.
TSO/ISPF Mode	This mode operates within the user's TSO address space. It requires additional VTAM and ISPF definitions.

12.2.1.1 Dedicated Mode

Dedicated mode execution of OMEGAMON software products is by design independent of individual users, as it executes using a dedicated system console and/or dedicated VTAM terminal.

Enforce the following controls for Dedicated Mode execution of OMEGAMON software products:

(1) Ensure that the system consoles and/or terminals dedicated to OMEGAMON software products are in a controlled area accessible only to Operations personnel.

(2) Ensure that access to the consoles and/or terminals dedicated to OMEGAMON software products are further restricted to those Operations personnel authorized to use OMEGAMON.

(3) Control access to internal OMEGAMON software product commands using the standard OMEGAMON internal password system.

12.2.1.2 VTAM Mode

Enforce the following controls for VTAM execution of OMEGAMON software products:

(1) The OMEGAMON products should only appear as Session Manager selection options for those individuals authorized access to OMEGAMON applications.

(2) Use the following values for key OMEGAMON VTAM initialization parameters. These keyword parameters and values are coded in the started task JCL. Not all the available initialization parameters are listed in the table below. Several specified values are the default values. They are listed to reiterate their importance.

Table B-20. OMEGAMON VTAM INITIALIZATION PARAMETERS (12.2.1.2)

OMEGAMON VTAM INITIALIZATION PARAMETERS		
OPTION	*DESCRIPTION*	*STANDARD VALUE*
AUP	Specifies whether the OMEGAMON sessions are in automatic update mode.	NO Product Install default value = NO ***NOTE:*** Local changes are justified in writing with supporting documentation.
DATA	Specifies whether OMEGAMON is to use a logon DATA string.	YES Product Install default value = YES
DC	Specifies whether OMEGAMON compresses the 3270 data stream before it is sent to a terminal.	Site defined Product Install default value = NO This is essentially a performance issue.
PRTCT	Defines to OMEGAMON the password to use to open the VTAM ACB, as specified in the VTAMLST APPL statement.	None is specified. Product Install default value = NONE ***NOTE:*** Local changes are justified in writing with supporting documentation.
PSWD	Defines a common logon password for users to log on in VTAM mode.	None is specified. Product Install default value = NONE
SWAP	Defines whether or not the OMVTAM address space marks itself as non-swappable while at least one VTAM session is active. NO indicates that the address space does not swap.	NO Product Install default value = NO ***NOTE:*** Local changes are justified in writing with supporting documentation.
TIMEOUT	Defines the maximum number of minutes that a VTAM mode session can be idle.	15 Product Install default value = 0
UMAX	Defines the maximum number of concurrent users that may be logged on to OMEGAMON.	Site defined Product Install default value = 10

(4) The actual resource mechanisms for controlling accesses vary based on the requirements of each individual OMEGAMON component and on the resident ACP. They are described within each component's section in the appropriate ACP sub-section.

- *(ZOMG0030: CAT II) The systems programmer/IAO will ensure OMEGAMON VTAM initialization parameters are specified in accordance with STIG requirements.*

12.2.1.3 ISPF and TSO Modes

ISPF and TSO Mode execution of OMEGAMON applications occurs within the user's TSO address space. No additional I&A validation is done by the components, since the user has already established a TSO session. Authorization to access the OMEGAMON applications themselves from ISPF and TSO is controlled via the same resource mechanisms as in VTAM mode, as described in the component sections below.

Enforce the following controls for ISPF execution of OMEGAMON applications:

(1) The clist, message, panel, program, skeleton, and table libraries necessary for ISPF execution of OMEGAMON software products is only available in the TSO environment of those individuals authorized access to OMEGAMON applications.

(2) The OMEGAMON applications only appear as ISPF panel selection options for those individuals authorized access to OMEGAMON applications.

The following additional control should be enforced for TSO execution of OMEGAMON applications:

(3) The clist, message, panel, program, skeleton, and table libraries necessary for TSO execution of OMEGAMON software products should only be available in the TSO environment of those individuals authorized access to OMEGAMON applications.

12.2.2 OMEGACENTER GATEWAY for OS/390

The OMEGACENTER GATEWAY for OS/390 product is an analytical engine interfacing with, and integrating information from, a wide array of sources. It probes enterprise-wide events, and data about them is combined and evaluated based on site policies. It provides a common and integrated way to collect and filter system event information across the enterprise, and provides a methodology allowing responsible parts of the organization to communicate effectively.

12.2.2.1 General Considerations

The following data set requires APF authorization:

SYS2.OMEGAMON.TKOGLOAD

This library requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Access greater than read is restricted only to the systems programming personnel

responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* for additional information.

12.2.2.2 ACF2

Complete the following steps when using ACF2 as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON GATEWAY data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.2.1, General Considerations,* for information regarding security controls for APF-authorized data sets.

(2) Ensure that the logonid OMCGATE is defined as MUSASS NO-SMC STC.

- *(ZOMG0040: CAT II) The systems programmer/IAO will ensure that OMEGAMON started tasks are defined in accordance with STIG requirements.*

12.2.2.3 RACF

Complete the following steps when using RACF as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON GATEWAY data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.2.1, General Considerations,* for information regarding security controls for APF-authorized data sets.

(2) Ensure the following:

(a) The STC userid OMCGATE is defined as a PROTECTED userid.

(b) The userid OMCGATE is connected to a group for the OMEGACENTER started tasks.

(c) The OMCGATE STC has a matching profile defined to the STARTED class with no special attributes. For example:

```
RDEFINE STARTED OMCGATE.* UACC(NONE) OWNER(admin)
STDATA(USER(OMCGATE) GROUP(STCOMEG) TRUSTED(NO))
```

- *(ZOMG0040: CAT II) The systems programmer/IAO will ensure that OMEGAMON started tasks are defined in accordance with STIG requirements.*

12.2.2.4 TOP SECRET

Complete the following steps when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON GATEWAY data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.2.1, General Considerations,* for information regarding security controls for APF-authorized data sets.

(2) Ensure that the STC ACID OMCGATE is defined with a non-expiring password and sourced to the internal reader:

```
TSS CREATE(OMCGATE) NAME('OMEGAMON GATEWAY STC')
    TYPE(USER) DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
    SOURCE(INTRDR)
```

(3) Add the STC OMCGATE to the Started Task Table specifying the associated ACID OMCGATE:

```
TSS ADD(STC) PROCNAME(OMCGATE) ACID(OMCGATE)
```

- *(ZOMG0040: CAT II) The systems programmer/IAO will ensure that OMEGAMON started tasks are defined in accordance with STIG requirements.*

12.2.3 OMEGAVIEW

12.2.3.1 Security Overview

The OMEGAVIEW product is the OMEGACENTER status manager. It displays concise information about, and provides access to, all OMEGAMON performance monitoring products. The status information is maintained through OMEGAVIEW's status data manager component, the SDM. Multi-session VTAM support provides navigation between OMEGAVIEW and other OMEGAMON products.

The OMEGAVIEW System Administrator should restrict OMEGAVIEW user access only to selected systems programmers and Operations personnel, and should also restrict user authority options to the lowest level needed to accomplish the user's tasks.

OMEGAVIEW should have the *emergency userids* (refer to *Section 3.1.2.6, Emergency Userids*, for further information) assigned as Administrators to recover from No Administrator Defined situations.

12.2.3.2 ACF2

Complete the following steps when using ACF2 as the ACP for this OMEGAMON II software monitoring product:

(1) During final product configuration (CICAT), specify ACF2 External Security.

(2) Ensure that member KMVINNAM in SYS3.OMEGAMON.*.RKMVPAR is configured to implement ACF2:

```
DEFAULT DSNAME(SYS3.OMEGAMON.*.RKMVNAM) EXIT=KLVA2NEV
    NORACF NODB
```

(3) Assemble and link the exit for security validation, KLVA2NEV, using KLVA2ASM.

(4) Define the logonid MVPROC as a MUSASS NO-SMC STC.

(5) Allow the started task MVPROC only *read* access to SYS2.OMEGAMON.* and SYS3.OMEGAMON.*.

(6) OMEGAVIEW does not use SAF to restrict access authorization to the OMEGAVIEW APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION defines the APPLID of A*xx*MVP01 or a site defined APPLID to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., system programming, storage management, network, and operations). For example:

```
$KEY(Axx MVP01) TYPE(APL)
- UID(-) PREVENT
UID(sys-prog-group) ALLOW
```

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

12.2.3.3 RACF

Complete the following steps when using RACF as the ACP for this OMEGAMON II software monitoring product:

(1) During final product configuration (CICAT), specify RACF External Security.

(2) Define the STC userid MVPROC as a PROTECTED userid.

(3) Define a matching profile for the MVPROC STC to the STARTED resource class. For example:

```
RDEFINE STARTED MVPROC.* UACC(NONE) OWNER(admin)
    STDATA(USER(MVPROC) GROUP(STCOMEG) TRUSTED(NO))
```

(4) Allow the started task MVPROC only *read* access to SYS2.OMEGAMON.** and SYS3.OMEGAMON.**.

(5) Ensure that member, KMVINNAM, in SYS3.OMEGAMON.**.RKMVPAR, is configured to implement RACF:

```
DEFAULT DSNAME(SYS3.OMEGAMON.**.RKMVNAM) RACF NODB
```

(6) OMEGAVIEW does not use SAF to restrict access authorization to the OMEGAVIEW APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*MVP01 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

```
RDEFINE APPL Axx MVP01 UACC(NONE)
PERMIT Axx MVP01 CLASS(APPL) ID(sys-prog-group) ACCESS(READ)
```

(7) Activate the APPL class as follows:

```
SETROPTS CLASSACT(APPL)
```

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

12.2.3.4 TOP SECRET

Complete the following steps when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product:

(1) During final product configuration (CICAT), specify TOP SECRET External Security.

(2) Create an OMEGAMON profile to contain all OMEGAMON permissions:

```
TSS CREATE(NPBOMEG) NAME( OMEGAMON STC PROFILE')
    TYPE(PROFILE) DEPT(dept-acid)
```

NOTE: This profile may already have been created.

(3) Create the STC ACID MVPROC with a non-expiring password, sourced to the internal reader, and a Master Facility of MVPROC:

```
TSS CREATE(MVPROC) NAME('OMEGAVIEW STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
    MASTFAC(MVPROC) SOURCE(INTRDR)
```

(4) Allow the started task MVPROC only *read* access to SYS2.OMEGAMON.* and SYS3.OMEGAMON.*.

(5) Add the OMEGAMON profile to the STC ACID MVPROC:

```
TSS ADD(MVPROC) PROFILE(npbomeg)
```

(6) Add the STC MVPROC to the Started Task Table specifying the associated ACID MVPROC:

```
TSS ADD(STC) PROCNAME(MVPROC) ACID(MVPROC)
```

(7) Define MVPROC as a Facility to TOP SECRET in the Facility Matrix Table using the following example:

```
FACILITY(USERxx=NAME=MVPROC)
FACILITY(MVPROC=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(MVPROC=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(MVPROC=ID=nn,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
    SIGN(M))
FACILITY(MVPROC=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
    NOAUDIT)
FACILITY(MVPROC=NOTSOC,LOG(INIT,SMF,MSG,SEC9))
```

(where nn is a site unique ID code)

(8) Modify the SYS3.OMEGAMON.*.RKMVPAR(KMVINNAM) security system definition to implement TOP SECRET:

DEFAULT DSNAME(SYS3.OMEGAMON.*.RKMVNAM) RACF NODB

(9) OMEGAVIEW does not use SAF to restrict access authorization to the OMEGAVIEW APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*MVP01 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

TSS PERMIT(*sys-prog-group*) KLS(A*xx*MVP01) ACCESS(READ)

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

12.2.4 OMEGAMON II for VTAM

OMEGAMON II for VTAM is the performance monitor product used to monitor a VTAM network.

12.2.4.1 General Considerations

This section documents general security considerations that apply to OMEGAMON II for VTAM. This product has the capability of interfacing with the installed ACP or using internal security. The STIG requirement is to use the ACP for controlling access.

12.2.4.1.1 APF Authorization

Several OMEGAMON II for VTAM data sets require APF authorization. Many of these libraries are shared with other OMEGACENTER products. These data sets include the following:

SYS2.OMEGAMON.TETLOAD
SYS2.OMEGAMON.TKANMODD (shared)
SYS2.OMEGAMON.TKANMOD1 (shared)
SYS2.OMEGAMON.TLOADLIB (shared) *(See note below.)*
SYS2.OMEGAMON.TLVLOAD (shared)

Each of these libraries requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Restrict access greater than *read* only to the systems programmers responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* for additional information.

NOTE: The library, SYS2.OMEGAMON.TLOADLIB, must also be referenced in the VTAM started task procedure. Therefore, VTAM requires read access to this library.

12.2.4.1.2 User Authorities

User authorities within OMEGAMON II for VTAM are controlled via an internal mechanism. This control is accessed through the OPTIONS pull-down under USER AUTHORITIES. Access to the various functions should be tightly controlled and only given to those personnel who have a justified access. Further information on this control can be found in the *OMEGAMON II for VTAM Users Guide*.

12.2.4.2 ACF2

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using ACF2 as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for VTAM data sets using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.4.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify ACF2 External Security on the KONPCSI4 - OMEGAMON II Configuration Parameters screen. Additionally, the value of YES is supplied for the parameter, Install ACF2 Exit. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKONPARM to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.*.RKONNAM) EXIT=KLVA2NEV
    NORACF NODB
```

(3) Ensure that the logonid KON2VTAM is defined as MUSASS NO-SMC STC.

(4) OMEGAMON II for VTAM does not use SAF to restrict access authorization to the OMEGAMON II for VTAM APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OMP01 to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming, network, and operations). For example:

$KEY(A*xx*OMP01) TYPE(APL)
- UID(-) PREVENT
UID(*sys-prog-group*) ALLOW

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

12.2.4.3 RACF

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using RACF as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for VTAM data sets using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.4.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify RACF External Security on the KONPCSI4 - OMEGAMON II Configuration Parameters screen. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKONPARM to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.RKONNAM) RACF NODB

(3) Define the STC userid KON2VTAM as a PROTECTED userid.

(4) Define a matching profile for the KON2VTAM STC to the STARTED resource class. For example:

RDEFINE STARTED KON2VTAM.* UACC(NONE) OWNER(*admin*)
STDATA(USER(KON2VTAM) GROUP(STCOMEG) TRUSTED(NO))

(5) OMEGAMON II for VTAM does not use SAF to restrict access authorization to the OMEGAMON II for VTAM APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OMP01 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, network, and operations). For example:

RDEFINE APPL A*xx*OMP01 UACC(NONE)
PERMIT A*xx*OMP01 CLASS(APPL) ID(*sys-prog-group*) ACCESS(READ)

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and/or protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

12.2.4.4 TOP SECRET

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for VTAM data sets using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.4.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify TOP SECRET External Security on the KONPCSI4 - OMEGAMON II Configuration Parameters screen. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKONPARM to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.RKONNAM) RACF NODB

(3) Create the STC ACID KON2VTAM with a non-expiring password, sourced to the internal reader, and a Master Facility of KON2VTAM:

TSS CREATE(KON2VTAM) NAME('OMEGAMON VTAM STC')
TYPE(USER)
DEPT(*dept-acid*) PASSWORD(*password*,0) FAC(STC)
MASTFAC(KON2VTAM) SOURCE(INTRDR)

(4) Add the OMEGAMON profile to the STC ACID KON2VTAM:

TSS ADD(KON2VTAM) PROFILE(*npbomeg*)

(5) Add the STC KON2VTAM to the Started Task Table specifying the associated ACID KON2VTAM:

TSS ADD(STC) PROCNAME(KON2VTAM) ACID(KON2VTAM)

(6) Define KON2VTAM as a Facility to TOP SECRET in the Facility Matrix Table using the following example:

```
FACILITY(USERxx=NAME=KON2VTAM)
FACILITY(KON2VTAM=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KON2VTAM=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(KON2VTAM=ID=nn,MULTIUSER,RES,LUMSG,STMSG,
    WARNPW,SIGN(M))
FACILITY(KON2VTAM=NOINSTDATA,NORNDPW,AUTHINIT,
    NOPROMPT,NOAUDIT)
FACILITY(KON2VTAM=NOTSOC,LOG(INIT,SMF,MSG,SEC9))
```

(where nn is a site unique ID code)

(7) OMEGAMON II for VTAM does not use SAF to restrict access authorization to the OMEGAMON II for VTAM APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OMP01 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, network, and operations). For example:

```
TSS PERMIT(sys-prog-group) KLS(AxxOMP01) ACCESS(READ)
```

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

12.2.5 OMEGAMON II for SMS

OMEGAMON II for SMS is the performance monitor product for IBM System Managed Storage.

12.2.5.1 General Considerations

This section documents general security considerations that apply to OMEGAMON II for SMS. This product has the capability of interfacing with the installed ACP or using internal security. The STIG requirement is to use the ACP for controlling access.

12.2.5.1.1 APF Authorization

Several OMEGAMON II for SMS data sets require APF authorization. Many of these libraries are shared with other OMEGACENTER products. These data sets include the following:

SYS2.OMEGAMON.TKDFMODA
SYS2A.OMEGAMON.TCNLOAD (shared)
SYS2.OMEGAMON.TKANMODD (shared)
SYS2.OMEGAMON.TKANMOD1 (shared)
SYS2.OMEGAMON.TLOADLIB (shared)
SYS2.OMEGAMON.TLVLOAD (shared)

Each of these libraries requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Access greater than *read* is restricted only to the systems programming personnel responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* for additional information.

12.2.5.1.2 Function Resource Controls

In the ACP sections below, accesses to SMS resources are granted to the user profile by *function level resource*, where the External Security Function-level resources are as follows:

Table B-21. EXTERNAL SECURITY FUNCTION-LEVEL RESOURCES (12.2.5.1.2)

EXTERNAL SECURITY FUNCTION-LEVEL RESOURCES		
RESOURCE NAME	*DESCRIPTION*	*USER ACCESS*
OMIISMS@COM@LISTUSER	Lists users of a volume	SYS, STG, OPS
OMIISMS@COM@SETCACHE	Issues SETCACHE commands	SYS, STG
OMIISMS@DEFINE@APPL	Defines applications to monitor	SYS, STG
OMIISMS@DEFINE@CACHE	Defines list of cached/DFW devices	SYS, STG
OMIISMS@DEFINE@CHP	Defines on-line channel path list	SYS, STG
OMIISMS@DEFINE@GROUP	Defines user DASD groups to monitor	SYS, STG
OMIISMS@DFDSS@ACTION	Initiates DFDSS volume actions	SYS, STG
OMIISMS@DFDSS@DATASET	Initiates DFDSS data set actions	SYS, STG
OMIISMS@HSM@ACTION	Initiates HSM volume actions	SYS, STG
OMIISMS@HSM@CANCEL	Cancels queued HSM requests	SYS, STG
OMIISMS@HSM@COMMAND	Issues HSM commands	SYS, STG
OMIISMS@HSM@DATASET	Initiates HSM data set actions	SYS, STG
OMIISMS@HSM@HR	Holds/releases HSM functions	SYS, STG
OMIISMS@PRODUCT@ACCESS	Product access control	SYS, STG, OPS

EXTERNAL SECURITY FUNCTION-LEVEL RESOURCES		
RESOURCE NAME	*DESCRIPTION*	*USER ACCESS*
OMIISMS@PRODUCT@ADMIN	Product Administrator Authority	SYS, STG
OMIISMS@SYS@OPERATOR	Issues system operator commands	SYS, STG, OPS

Access to the various resources are limited to the appropriate systems programming, storage administration/DASD management, and Operations personnel. The column labeled ***USER ACCESS*** above is the recommended personnel requiring access to the various resources:

- **SYS** Systems Programming personnel
- **STG** Storage Administration/DASD Management personnel
- **OPS** Operations personnel

12.2.5.2 ACF2

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using ACF2 as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for SMS data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.5.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify ACF2 External Security on the Choose Product Security Method option. Additionally, set Enable User Authority Checking to Y.

(3) During final product configuration, specify External Function Based Security on the Choose Panel Level Security Method option. Specify the resource class name of OSM.

As a result of Steps 2 and 3, set member KLVINNAM of data set SYS3.OMEGAMON.*qualifier*.KDFVPRMA as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDFNAM)
   EXIT=KLVA2NEV CLASSES=OSM NORACF NODB
```

(4) Ensure that the logonid KDFPROC is defined as a MUSASS NO-SMC STC.

(5) Ensure that the resource type of OSM is specified in the INFODIR or RESDIR.

(6) Control user access to OMEGAMON II for SMS through the use of the function resource, OMIISMS@PRODUCT@ACCESS, defined to the OSM resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). Control all other sensitive panel functions through ACF2 resources. Refer to *Section 12.2.5.1.2, Function Resource Controls,* for a list of the resources. For example:

```
$KEY(OMIISMS@PRODUCT@ACCESS) TYPE(OSM)
- UID(-) PREVENT
UID(sys-prog-group) ALLOW
```

(7) OMEGAMON II for SMS does not use SAF to restrict access authorization to the OMEGAMON II for SMS APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OTP01 to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). For example:

```
$KEY(Axx OTP01) TYPE(APL)
- UID(-) PREVENT
UID(sys-prog-group) ALLOW
```

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.5.3 RACF

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using RACF as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for SMS data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for the product. Refer to *Section 12.2.5.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify RACF External Security on the Choose Product Security Method option. Additionally, set Enable User Authority Checking to Y.

(3) During final product configuration, specify External Function Based Security on the Choose Panel Level Security Method option. Specify the resource class name of $$OSCAN.

As a result of Steps 2 and 3, set member KLVINNAM of data set SYS3.OMEGAMON.*qualifier*.KDFVPRMA as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDFNAM)
    CLASSES=$$OSCAN RACF NODB
```

(4) Update the Resource Class Descriptor Table and RACF Router Table for *classname* $$OSCAN.

```
ICHERCDE CLASS=$$OSCAN,
                ID=nnn,
                MAXLNTH=28,
                FIRST=ALPHANUM,
                OTHER=ANY,
                POSIT=nnn,
                DFTUACC=NONE
```

NOTE: Local configuration determines the value of nnn.

```
ICHRFRTB CLASS=$$OSCAN,
                ACTION=RACF
```

(5) Ensure the following:

(a) The STC userid KDFPROC is defined as a PROTECTED userid.

(b) The userid KDFPROC is connected to a group for the OMEGACENTER started tasks.

(c) The KDFPROC STC has a matching profile defined to the STARTED resource class with no special attributes. For example:

```
RDEFINE STARTED KDFPROC.* UACC(NONE) OWNER(admin)
    STDATA(USER(KDFPROC) GROUP(STCOMEG) TRUSTED(NO))
```

(6) Control user access to OMEGAMON II for SMS through the use of the function resource OMIISMS@PRODUCT@ACCESS defined to the $$OSCAN class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). Control all other sensitive panel functions through RACF resources. Define all SMS resources with a UACC(NONE). Refer to *Section 12.2.5.1.2, Function Resource Controls*, for a list of the resources. For example:

RDEFINE $$OSCAN OMIISMS@PRODUCT@ACCESS UACC(NONE)

PERMIT OMIISMS@PRODUCT@ACCESS CLASS($$OSCAN)
ID(*sys-prog-group*) ACCESS(READ)

(7) OMEGAMON II for SMS does not use SAF to restrict access authorization to the OMEGAMON II for SMS APPLID. However sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OTP01 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). For example:

RDEFINE APPL A*xx*OTP01 UACC(NONE)
PERMIT A*xx*OTP01 CLASS(APPL) ID(*sys-prog-group*) ACCESS(READ)

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.5.4 TOP SECRET

This section provides the guidance on what values and controls should be set in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. Complete the following steps when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product:

(1) Protect all OMEGAMON II for SMS data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for the product. Refer to *Section 12.2.5.1.1, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(2) During final product configuration (CICAT), specify TOP SECRET External Security on the Choose Product Security Method option. Additionally, set Enable User Authority Checking to Y.

(3) During final product configuration, specify External Function Based Security on the Choose Panel Level Security Method option. Specify the resource class name of KOSCANDL.

As a result of Steps 2 and 3, set member KLVINNAM of data set SYS3.OMEGAMON.*qualifier*.KDFVPRMA as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDFNAM)
    CLASSES=KOSCANDL RACF NODB
```

(4) Create the STC ACID KDFPROC with a non-expiring password, sourced to the internal reader, and a Master Facility of KDFPROC:

```
TSS CREATE(KDFPROC) NAME('OMEGAMON SMS STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
    MASTFAC(KDFPROC) SOURCE(INTRDR)
```

(5) Add the OMEGAMON profile to the STC ACID KDFPROC:

```
TSS ADD(KDFPROC) PROFILE(npbomeg)
```

(6) Add the STC KDFPROC to the Started Task Table specifying the associated ACID KDFPROC:

```
TSS ADD(STC) PROCNAME(KDFPROC) ACID(KDFPROC)
```

(7) Ensure that the resource type of KOSCANDL is defined to the Resource Definition Table (RDT). An example of the command to do this is shown below:

TSS ADDTO(RDT) RESCLASS(KOSCANDL) RESCODE(*xx*) ATTR(LONG)

(where xx is an unused hex value)

NOTE: A department must be given ownership of the RDT entries.

(8) Ensure that KDFPROC is defined as a Facility to TOP SECRET in the Facility Matrix Table. The following is an example:

FACILITY(USER*xx*=NAME=KDFPROC)
FACILITY(KDFPROC=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KDFPROC=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(KDFPROC=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
SIGN(M))
FACILITY(KDFPROC=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(KDFPROC=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

(where nn is a site unique ID code)

(9) Control user access to OMEGAMON II for SMS through the use of the function resource OMIISMS@PRODUCT@ACCESS defined to the KOSCANDL class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). Control all other sensitive panel functions through TOP SECRET resources. Refer to *Section 12.2.5.1.2, Function Resource Controls,* for a list of the resources. For example:

TSS PERMIT(*sys-prog-group*) KOSCANDL (OMIISMS@PRODUCT@ACCESS)

(10) OMEGAMON II for SMS does not use SAF to restrict access authorization to the OMEGAMON II for SMS APPLID. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID of A*xx*OTP01 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, and operations). For example:

TSS PERMIT(*sys-prog-group*) KLS(A*xx*OTP01) ACCESS(READ)

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

12.2.6 OMEGAMON II for MVS

12.2.6.1 Security Overview

OMEGAMON II for MVS is the performance monitor product for the IBM base operating system and components. This product has the capability of interfacing with the installed ACP or using internal security. The STIG requirement is to use External Security for controlling access.

This section also includes information on security considerations for the Candle Management Server (CMS).

12.2.6.1.1 Command-level Security

OMEGAMON II has many commands that are used to inquire and optionally make changes to system parameters and values. The product allows each command to have a security level assigned to it, ranging from 0 to 3. Users are then assigned a security level within their profile that allows them to issue commands assigned to their level and lower. As an example, a user with Level 2 can execute commands secured at Levels 0, 1, or 2. Level 3 provides the highest degree of protection for sensitive commands. A setting of 0 means that any user can access the command. Access to Level 3 is strictly controlled and only granted to authorized systems personnel.

The following commands are installed with a security level of 3 by default from the vendor, and are to remain as Level 3 commands:

ALI	ALIBnn	APFU	CHAP	CONS	CONU
CSAF	.DSA	FNDU	KILL	LPAM	MCHN
MCTL	MDEF	MLST	MNSW	MSCN	MSWP
MZAP	OCMD	OSPC	PEEK	QLLA	RCMD
SCHN	SLST	SSCN	SWPI	SWPO	SZAP
TADR	TSNM	XMCH	XMLS	XMSC	XMZP

The following commands are not installed as Level 3 commands by the vendor, but are designated as Level 3 commands by this STIG:

ACTN	AMAP	.APF	DATA	DDNS
DSPA	DSPC	DSPO	JOBS	LINE
MNT	MODS	PLOT	.RMF	SEEK
STEP	SUBP	TCBS	WSIZnn	

The ACP determines which security level is associated with a user. Please refer to the following ACP-specific sections for the details on how this is controlled.

NOTE: During the installation of the product, Candle internal security assigns default passwords to the various security levels. This password can be entered in response to a **/PWD** command entered by the user to change the security level. Even though the STIG does not allow users to change their security levels via these passwords, each site is required to change their passwords from the defaults.

12.2.6.1.2 APF Authorization

Several OMEGAMON II for MVS data sets require APF authorization. These data sets include the following:

SYS2.OMEGAMON.TETLOAD
SYS2.OMEGAMON.TKANMOD1
SYS2.OMEGAMON.TKANMODD
SYS2.OMEGAMON.TLOADLIB
SYS2.OMEGAMON.TLVLOAD
SYS2.OMEGAMON.TSDLOAD

Each of these libraries requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Restrict access greater than *read* only to the systems programming personnel responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF*), for additional information.

12.2.6.2 ACF2

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using ACF2 as the ACP for this OMEGAMON II software monitoring product.

12.2.6.2.1 ACF2 Candle Management Server Controls

The following is information related to setting up validation for the Candle Management Server (CMS):

(1) Ensure that member KDSCNFG in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
SET ENV VALIDATE=YES
```

(2) Ensure that member KDSINNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDSNAM)
    EXIT=KLVA2NEV NORACF NODB
```

(3) Define the logonid KDSPROC as a STC.

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

12.2.6.2.2 ACF2 Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for MVS:

(1) During final product configuration (CICAT), specify ACF2 External Security. As a result of this, configure member KM2INNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.NAM)
    EXIT=KLVA2NEV NORACF NODB
```

(2) Ensure that the vendor-provided KLVA2NEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Protect all OMEGAMON II for MVS data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(4) Define the logonid OMIIMVS as a MUSASS NO-SMC STC.

(5) Define the logonid OMIIRCOL as a MUSASS NO-SMC STC MUSUPDT.

(5) Define a logonid for each of the following started tasks. The logonid and STC name are the same. These logonids have no special privileges:

KCNDL
OMIICSA
OMIIEPZM
OMIIETE
OMIIHDI
OMIIHIST
OMIIHMN
OMIIHM2

12.2.6.2.3 ACF2 Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for MVS:

(1) Ensure that the resource type is defined as OMS. This is accomplished in the actual KOMACF2X source module. Line 07600000 should be changed to read as follows:

A#ACFCLS DC CL4'ROMS'

Run job KOMACF2A to assemble and link the exit. This resource type is also defined to the ACF2 INFODIR GSO record.

NOTE: The exit program must be specified with the MODULE=KOMACF2X parameter in the ***NOTE:***KOMSUPDI member of SYS3.OMEGAMON.qualifier.ROMDATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) Define the following resource rules to prevent unauthorized access to OMEGAMON. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

$KEY(INITIAL) TYPE(OMS)
- UID(-) PREVENT

$KEY(INITIAL0) TYPE(OMS)
- UID(-) PREVENT
UID(*sys-level-support-grp-0*) ALLOW

$KEY(INITIAL1) TYPE(OMS)
- UID(-) PREVENT
UID(*sys-level-support-grp-1*) ALLOW

$KEY(INITIAL2) TYPE(OMS)
- UID(-) PREVENT
UID(*sys-level-support-grp-2*) ALLOW

$KEY(INITIAL3) TYPE(OMS)
- UID(-) PREVENT
UID(*sys-prog-grp*) ALLOW

NOTE:: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(3) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(4) Optionally, a site can use ACF2 controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(5) OMEGAMON II for MVS does not use SAF to restrict access authorization to the OMEGAMON II for MVS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*O2P01 and A*xx*ORP01 to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

$KEY(A*xx*O2P01) TYPE(APL)
- UID(-) PREVENT
UID(*sys-prog-group*) ALLOW

$KEY(A*xx*ORP01) TYPE(APL)
- UID(-) PREVENT
UID(*sys-prog-group*) ALLOW

(6) Configure and install the security table, KOMSUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOMACF2X security module. Run job KOMSUPD to install the security table.

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.6.3 RACF

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization, or the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using RACF as the ACP for this OMEGAMON II software monitoring product.

12.2.6.3.1 RACF Candle Management Server Controls

The following is information related to setting up validation for the Candle Management Server (CMS):

(1) Ensure that member KDSCNFG in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
SET ENV VALIDATE=YES
```

(2) Ensure that member KDSINNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDSNAM) RACF NODB
```

(3) Ensure the following:

(a) The STC userid KDSPROC is defined as a PROTECTED userid.

(b) The userid KDSPROC is connected to a group for the OMEGACENTER started tasks.

(c) The KDSPROC STC has a matching profile defined to the STARTED resource class with no special attributes. For example:

```
RDEFINE STARTED KDSPROC.* UACC(NONE) OWNER(admin)
  STDATA(USER(KDSPROC) GROUP(STCOMEG) TRUSTED(NO))
```

12.2.6.3.2 RACF Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for MVS:

(1) During final product configuration (CICAT), specify RACF External Security. As a result of this, configure member KM2INNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.NAM) RACF NODB

(2) Protect all OMEGAMON data sets using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization*, for information regarding security controls for APF-authorized data sets.

(3) Ensure the following:

(a) A userid for each STC identified in (c) below is defined as a PROTECTED userid. The userid and STC name should be the same.

(b) Each userid is connected to a group for the OMEGACENTER started tasks.

(c) Each of the following STCs has a matching profile defined to the STARTED resource class with no special attributes.

KCNDL
OMIICSA
OMIIEPZM
OMIIETE
OMIIHDI
OMIIHIST
OMIIHMN
OMIIHM2
OMIIMVS
OMIIRCOL

For example:

RDEFINE STARTED OMII*.* UACC(NONE) OWNER(*admin*)
STDATA(USER(=MEMBER) GROUP(STCOMEG) TRUSTED(NO))

12.2.6.3.3 RACF Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for MVS:

(1) Ensure that the RACF exit program is installed properly to provide for command-level security. During the installation, the resource class of $$OMCAN is specified. Ensure that line 00890000 reads as follows in source member KOMRACFX:

```
MVC U#CHCLSD,=CL8'$$OMCAN '     ALT. RESOURCE CLASS NAME
```

Run job KOMRACFA to assemble and link the exit.

NOTE: The exit program must be specified with the MODULE=KOMRACFX parameter in the KOMSUPDI member of SYS3.OMEGAMON.qualifier.ROMDATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) A new class is added to the RACF Class Descriptor Table and RACF Router Table for classname $$OMCAN. The following is a sample for the class entry:

```
ICHERCDE CLASS=$$OMCAN,
         ID=nnn,
         MAXLNTH=8,
         FIRST=ALPHANUM,
         OTHER=ANY,
         POSIT=nnn,
         DFTUACC=NONE
```

NOTE: Local configuration determines the value of nnn.

```
ICHRFRTB CLASS=$$OMCAN,
         ACTION=RACF
```

(3) Define the following resource profiles to the $$OMCAN class to prevent unauthorized access to OMEGAMON:

```
RDEFINE $$OMCAN INITIAL UACC(NONE)
RDEFINE $$OMCAN INITIAL0 UACC(NONE)
RDEFINE $$OMCAN INITIAL1 UACC(NONE)
RDEFINE $$OMCAN INITIAL2 UACC(NONE)
RDEFINE $$OMCAN INITIAL3 UACC(NONE)
```

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

```
PERMIT INITIAL0 CLASS($$OMCAN) ID(sys-level-support-grp-0)
    ACCESS(READ)
PERMIT INITIAL1 CLASS($$OMCAN) ID(sys-level-support-grp-1)
    ACCESS(READ)
PERMIT INITIAL2 CLASS($$OMCAN) ID(sys-level-support-grp-2)
    ACCESS(READ)
PERMIT INITIAL3 CLASS($$OMCAN) ID(sys-prog-grp) ACCESS(READ)
```

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(6) Optionally, a site can use RACF controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for MVS does not use SAF to restrict access authorization to the OMEGAMON II for MVS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*O2P01 and A*xx*ORP01 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

RDEFINE APPL A*xx*O2P01 UACC(NONE)
PERMIT A*xx*O2P01 CLASS(APPL) ID(*sys-prog-grp*) ACCESS(READ)

RDEFINE APPL A*xx*ORP01 UACC(NONE)
PERMIT A*xx*ORP01 CLASS(APPL) ID(*sys-prog-grp*) ACCESS(READ)

(8) Permit OMIIMVS and OMIIEPZM to issue OS/390 commands by giving an OPERCMDS profile to OMIIMVS and OMIIEPZM.

(9) Configure and install the security table, KOMSUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOMRACFX security module. Run job KOMSUPD to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.6.4 TOP SECRET

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization or the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product.

12.2.6.4.1 TOP SECRET Candle Management Server Controls

The following is information related to setting up validation for the Candle Management Server (CMS):

(1) Ensure that member KDSCNFG in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
SET ENV VALIDATE=YES
```

(2) Ensure that member KDSINNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR specifies the following:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKDSNAM) RACF NODB
```

(3) Create the STC ACID KDSPROC with a non-expiring password, sourced to the internal reader, and a Master Facility of KDSPROC:

```
TSS CREATE(KDSPROC) NAME('OMEGAMON CMS STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
    MASTFAC(KDSPROC) SOURCE(INTRDR)
```

(4) Add the OMEGAMON profile to the STC ACID KDSPROC:

```
TSS ADD(KDSPROC) PROFILE(npbomeg)
```

(5) Add the STC KDSPROC to the Started Task Table specifying the associated ACID KDSPROC:

```
TSS ADD(STC) PROCNAME(KDSPROC) ACID(KDSPROC)
```

(6) Ensure that KDSPROC is defined as Facility to TOP SECRET in the Facility Matrix Table using the following example:

```
KDSPROC
FACILITY(USERxx=NAME=KDSPROC)
FACILITY(KDSPROC=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KDSPROC=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
```

FACILITY(KDSPROC=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
SIGN(M))
FACILITY(KDSPROC=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(KDSPROC=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

(where nn is a site unique ID code)

Each user that requires access to the OMEGAMON CMS product must be given access to the KDSPROC Facility.

12.2.6.4.2 TOP SECRET Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for MVS:

(1) During final product configuration (CICAT), specify TOP SECRET External Security. As a result of this, configure member KM2INNAM in SYS3.OMEGAMON.*qualifier*.RKANPAR to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.NAM) EXIT=KLVTSNEV
RACF NODB

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) Protect all OMEGAMON data sets using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization*, for information regarding security controls for APF-authorized data sets. This should be done by performing the following:

(a) Create an OMEGAMON profile to contain all OMEGAMON permissions:

TSS CREATE(*NPBOMEG*) NAME(OMEGAMON STC PROFILE')
TYPE(PROFILE) DEPT(*dept-acid*)

(b) Permit the OMEGAMON profile (*NPBOMEG*) *all* access to SYS3.OMEGAMON.* and *update* access to SYS2.OMEGAMON.* data sets:

TSS PERMIT(*NPBOMEG*) DSN(SYS3.OMEGAMON.) ACCESS(ALL)
TSS PERMIT(*NPBOMEG*) DSN(SYS2.OMEGAMON.) ACCESS(UPDATE)

(c) Permit the OMEGAMON profile *read* access to all OMEGAMON *loadlibs*:

TSS PERMIT(*NPBOMEG*) DSN(*omegamon.load.library*) ACCESS(READ)

(3) Create a STC ACID for each of the following started tasks. The ACID should match the name of the stated task. Each ACID is defined with a non-expiring password and sourced to the internal reader.

The OMIIMVS and OMIIRCOL STCs are defined with a MASTFAC. The MASTFAC matches the name of the STC ACID. A MASTFAC is not specified for the other STCs mentioned in this paragraph.

KCNDL
OMIICSA
OMIIEPZM
OMIIETE
OMIIHDI
OMIIHIST
OMIIHMN
OMIIHM2
OMIIMVS
OMIIRCOL

For example:

```
TSS CREATE(OMIIMVS) NAME('OMEGAMON MVS STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
        MASTFAC(OMIIMVS) SOURCE(INTRDR)
```

(4) Add the OMEGAMON profile to each STC ACID created in Step 3 above. For example:

```
TSS ADD(OMIIMVS) PROFILE(npbomeg)
```

(5) Add each STC indicated in *Paragraph (3)* above to the Started Task Table specifying the associated matching ACID. For example:

```
TSS ADD(STC) PROCNAME(OMIIMVS) ACID(OMIIMVS)
```

(6) Ensure that OMIIMVS and OMIIRCOL are defined as Facilities to TOP SECRET in the Facility Matrix Table using the following examples:

OMIIMVS OMIIMVS'S FACILITY CONTROLS SIGNON

FACILITY(USER*xx*=NAME=OMIIMV*S*)
FACILITY(OMIIMVS=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(OMIIMVS=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(OMIIMVS=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
SIGN(M))
FACILITY(OMIIMVS=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(OMIIMVS=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

OMIIRCOL OMIIRCOL'S FACILITY CONTROLS COMMAND AUTHORITY

FACILITY(USER*xx*=NAME=OMIIRCOL)
FACILITY(OMIIRCOL=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(OMIIRCOL=PGM=KOB,NOASUBM,NOABEND,NOXDEF)
FACILITY(OMIIRCOL=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,
WARNPW,SIGN(M))
FACILITY(OMIIRCOL=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(OMIIRCOL=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

(where nn is a site unique ID code)

Each user that requires access to the OMEGAMON II for MVS product must be given access to the appropriate Facilities.

(7) Ensure that the vendor-provided KLVTSNEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

12.2.6.4.3 TOP SECRET Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for MVS:

(1) To implement External Security validation for OMEGAMON command levels, update the Resource Definition Table adding a class name of KOMCANDL:

TSS ADD(RDT) RESCLASS(KOMCANDL) RESCODE(*xx*) ATTR(LONG)
TSS ADD(*dept-acid*) RESOURCE(KOMCANDL)

(where xx is an unused hex value)

NOTE: A department must be given ownership of the RDT entries.

(2) Ensure that the TOP SECRET/RACF exit program is installed properly to provide for command-level security. During the installation, the resource class of KOMCANDL will be specified. Ensure that line 00890000 reads as follows in source member KOMRACFX:

MVC U#CHCLSD,=CL8'KOMCANDL' ALT. RESOURCE CLASS NAME

Run job KOMRACFA to assemble and link the exit.

NOTE: The exit program must be specified with the MODULE=KOMRACFX parameter in the KOMSUPDI member of SYS3.OMEGAMON.qualifier.ROMDATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Assign ownership of the following OMEGAMON resource specifying the appropriate department ACID and KOMCANDL resource class. For example:

TSS ADD(*security-dept-acid*) KOMCANDL(INITIAL)

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

TSS PERMIT(*sys-level-support-grp-0*) KOMCANDL(INITIAL0)
TSS PERMIT(*sys-level-support-grp-1*) KOMCANDL(INITIAL1)
TSS PERMIT(*sys-level-support-grp-2*) KOMCANDL(INITIAL2)
TSS PERMIT(*sys-prog-grp*) KOMCANDL(INITIAL3)

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and are not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(6) Optionally, a site can use TOP SECRET controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for MVS does not use SAF to restrict access authorization to the OMEGAMON II for MVS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*O2P01 and A*xx*ORP01 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, storage management, network, and operations). For example:

TSS PERMIT(*sys-prog-grp*) KLS(A*xx*O2P01) ACCESS(READ)
TSS PERMIT(*sys-prog-grp*) KLS(A*xx*ORP01) ACCESS(READ)

(8) Configure and install the security table, KOMSUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOMRACFX security module. Run job KOMSUPD to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

12.2.7 OMEGAMON II for CICS

12.2.7.1 Security Overview

OMEGAMON II for CICS is a comprehensive performance monitor product for the IBM Customer Information Control System (CICS). Its real-time monitor alerts the user to CICS response time degradation and overall system problems. This product has the capability of interfacing with the installed ACP or using internal security. The DOD standard is to use external security for controlling access.

12.2.7.1.1 Command-level Security

OMEGAMON II has many commands that are used to inquire and optionally make changes to system parameters and values. The product allows each command to have a security level assigned to it, ranging from 0 to 3. Users are then assigned a security level within their profile that allows them to issue commands assigned to their level and lower. As an example, a user with Level 2 can execute commands secured at Levels 0, 1, or 2. Level 3 provides the highest degree of protection for sensitive commands. A setting of 0 means that any user can access the command. Access to Level 3 should be strictly controlled and only granted to authorized systems personnel.

The following authorized commands are installed with a security level of 3 by default from the vendor, and are to remain as Level 3 commands:

AIDK	CICM	CMT	CONS	CONU	CSWP
ICEK	KILL	MCHN	MDEF	MLST	MSCN
MZAP	OCMD	SLST	SSCN	SZAP	TDDL
TSQD	XMCH	XMLS	XMSC	XMZP	

The ACP determines which security level is associated with a user. Please refer to the following ACP-specific sections for the details on how this is controlled.

NOTE: During the installation of the product, Candle internal security assigns default passwords to the various security levels. This password can be entered in response to a **/PWD** command entered by the user to change the security level. Even though the STIG requirement do not allow users to change their security levels via these passwords, each site is required to change their passwords from the defaults.

12.2.7.1.2 APF Authorization

Several OMEGAMON II for CICS data sets require APF authorization. These data sets include the following:

SYS2.OMEGAMON.TETLOAD
SYS2.OMEGAMON.TLOADLIB
SYS2.OMEGAMON.TLVLOAD
SYS2.OMEGAMON.TCNLOAD

Each of these libraries requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Access greater than *read* is restricted to only the systems programming personnel responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* for additional information.

12.2.7.2 ACF2

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using ACF2 as the ACP for this OMEGAMON II software monitoring product.

12.2.7.2.1 ACF2 Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for CICS:

(1) During final product configuration (CICAT), specify ACF2 CUA Interface Security. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKC2PARM to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.NAM) EXIT=KLVA2NEV
NORACF NODB

(2) Ensure that the vendor-provided KLVA2NEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

(3) Protect all OMEGAMON II for CICS data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(4) Define the logonid KC2PROC as a MUSASS NO-SMC STC.

(5) Define the logonid KOCCI ID as a MUSASS NO-SMC STC.

12.2.7.2.2 ACF2 Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for CICS:

(1) Ensure the resource type is defined as OCS. This is accomplished in the actual KOCAACF2 source module. Line 07600000 should be changed to read as follows:

A#ACFCLS DC CL4'ROCS'

Run job KOCJACF2 to assemble and link the exit. This resource type will also be defined to the ACF2 INFODIR GSO record.

NOTE: The ACF2 exit program must be specified with the MODULE=KOCAACF2 parameter in the KOCSECUR member of SYS3.OMEGAMON.qualifier.RKC2DATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) Define the following resource rules to prevent unauthorized access to OMEGAMON. Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

$KEY(INITIAL) TYPE(OCS)
UID(-) PREVENT

$KEY(INITIAL0) TYPE(OCS)
UID(-) PREVENT
UID(*sys-level-support-grp-0*) ALLOW

$KEY(INITIAL1) TYPE(OCS)
UID(-) PREVENT
UID(*sys-level-support-grp-1*) ALLOW

$KEY(INITIAL2) TYPE(OCS)
UID(-) PREVENT
UID(*sys-level-support-grp-2*) ALLOW

$KEY(INITIAL3) TYPE(OCS)
UID(-) PREVENT
UID(*sys-prog-grp*) ALLOW

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(3) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(4) Optionally, a site can use ACF2 controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(5) OMEGAMON II for CICS does not use SAF to restrict access authorization to the OMEGAMON II for CICS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*COP01 and A*xx*COP02 to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

$KEY(A*xx*COP01) TYPE(APL)
UID(-) PREVENT
UID(*sys-prog-grp*) ALLOW

$KEY(A*xx*COP02) TYPE(APL)
UID(-) PREVENT
UID(*sys-prog-grp*) ALLOW

(6) Configure and install the security table, KOCSECUR, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOCAACF2 security module. Run job KOCSECJB to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.7.3 RACF

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using RACF as the ACP for this OMEGAMON II software monitoring product.

12.2.7.3.1 RACF Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for CICS:

(1) During final product configuration (CICAT), specify RACF CUA Interface Security. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKC2PARM to read as follows:

DEFAULT DSNAME(SYS3.OMEGAMON.*qualifier*.NAM) RACF NODB

(2) Protect all OMEGAMON data sets using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(3) Ensure the following:

(a) The STC userids KOCCI and KC2PROC are defined as PROTECTED userids.

(b) The userids KOCCI and KC2PROC are connected to a group for the OMEGACENTER started tasks.

(c) The KOCCI and KC2PROC STCs have matching profiles defined to the STARTED resource class with no special attributes. For example:

RDEFINE STARTED KOCCI.* UACC(NONE) OWNER(*admin*)
STDATA(USER(KOCCI) GROUP(STCOMEG) TRUSTED(NO))

12.2.7.3.2 RACF Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for CICS.

(1) Ensure that the RACF exit program is installed properly to provide for command-level security. During the installation, the resource class of $$OCCAN will be specified. Ensure that line 00920001 reads as follows in source member KOCARACF:

```
MVC U#CHCLSD,=CL8'$$OCCAN '     ALTERNATE RES/CLASS NAME
```

Run job KOCJRACF to assemble and link the exit.

NOTE: The RACF exit program must be specified with the MODULE=KOCARACF parameter in the KOCSECUR member of SYS3.OMEGAMON.qualifier.RKC2DATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) A new class is added to the RACF Class Descriptor Table and the RACF Router Table for classname $$OCCAN. The following is a sample for the class entry:

```
ICHERCDE CLASS=$$OCCAN,
         ID=nnn,
         MAXLNTH=8,
         FIRST=ALPHANUM,
         OTHER=ANY,
         POSIT=nnn,
         DFTUACC=NONE
```

NOTE: Local configuration determines the value of nnn.

```
ICHRFRTB CLASS=$$OCCAN,
         ACTION=RACF
```

(3) Define the following resource profiles to the $$OCCAN class to prevent unauthorized access to OMEGAMON:

```
RDEFINE $$OCCAN INITIAL UACC(NONE)
RDEFINE $$OCCAN INITIAL0 UACC(NONE)
RDEFINE $$OCCAN INITIAL1 UACC(NONE)
RDEFINE $$OCCAN INITIAL2 UACC(NONE)
RDEFINE $$OCCAN INITIAL3 UACC(NONE)
```

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

PERMIT INITIAL0 CLASS($$OCCAN) ID(*sys-level-support-grp-0*)
ACCESS(READ)
PERMIT INITIAL1 CLASS($$OCCAN) ID(*sys-level-support-grp-1*)
ACCESS(READ)
PERMIT INITIAL2 CLASS($$OCCAN) ID(*sys-level-support-grp-2*)
ACCESS(READ)
PERMIT INITIAL3 CLASS($$OCCAN) ID(*sys-prog-grp*) ACCESS(READ)

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(6) Optionally, a site can use RACF controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for CICS does not use SAF to restrict access authorization to the OMEGAMON II for CICS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*COP01 and A*xx*COP02 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

RDEFINE APPL A*xx*COP01 UACC(NONE)
PERMIT A*xx*COP01 CLASS(APPL) ID(*sys-prog-grp*) ACCESS(READ)

RDEFINE APPL A*xx*COP02 UACC(NONE)
PERMIT A*xx*COP02 CLASS(APPL) ID(*sys-prog-grp*) ACCESS(READ)

(8) Configure and install the security table, KOCSECUR, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOCARACF security module. Run job KOCSECJB to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.7.4 TOP SECRET

This section provides the guidance on what values and controls should be in regard to product security. Please refer to the installation instructions from the supporting software organization or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product.

12.2.7.4.1 TOP SECRET Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for CICS:

(1) During final product configuration (CICAT), specify TOP SECRET CUA Interface Security. As a result of this, configure member KLVINNAM in SYS3.OMEGAMON.*qualifier*.RKC2PARM to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.NAM) EXIT=KLVTSNEV
   RACF NODB
```

(2) Protect all OMEGAMON data sets using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets. This should be done by performing the following:

(a) Create an OMEGAMON profile to contain all OMEGAMON permissions:

```
TSS CREATE(NPBOMEG) NAME( OMEGAMON STC PROFILE')
   TYPE(PROFILE) DEPT(dept-acid)
```

(b) Permit the OMEGAMON profile (*NPBOMEG*) *all* access to SYS3.OMEGAMON.* and *update* access to SYS2.OMEGAMON.* data sets:

```
TSS PERMIT(NPBOMEG) DSN(SYS3.OMEGAMON.) ACCESS(ALL)
TSS PERMIT(NPBOMEG) DSN(SYS2.OMEGAMON.) ACCESS(UPDATE)
```

(c) Permit the OMEGAMON profile *read* access to all OMEGAMON *loadlibs*:

TSS PERMIT(*NPBOMEG*) DSN(*omegamon.load.library*) ACCESS(READ)

(3) Create the STC ACIDs KC2PROC and KOCCI with a non-expiring password, sourced to the internal reader, and a Master Facility. The MASTFAC matches the name of the STC ACID. For example:

```
TSS CREATE(KC2PROC) NAME('OMEGAMON CICS STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
        MASTFAC(KC2PROC) SOURCE(INTRDR)
```

(4) Add the OMEGAMON profile to the STC ACIDs KC2PROC and KOCCI. For example:

```
TSS ADD(KC2PROC) PROFILE(npbomeg)
```

(5) Add the STCs KC2PROC and KOCCI to the Started Task Table specifying the associated matching ACID. For example:

```
TSS ADD(STC) PROCNAME(KC2PROC) ACID(KC2PROC)
```

(6) Ensure that KC2PROC and KOCCI are defined as Facilities to TOP SECRET in the Facility Matrix Table using the following examples:

```
KC2PROC   FACILITY CONTROLS SIGNON

FACILITY(USERxx=NAME=KC2PROC)
FACILITY(KC2PROC=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KC2PROC=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(KC2PROC=ID=nn,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
      SIGN(M))
FACILITY(KC2PROC=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
      NOAUDIT)
FACILITY(KC2PROC=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

KOCCI       FACILITY CONTROLS SIGNON

FACILITY(USERxx=NAME=KOCCI)
FACILITY(KOCCI=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(KOCCI=PGM=KOB,NOASUBM,NOABEND,NOXDEF)
FACILITY(KOCCI=ID=nn,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
      SIGN(M))
FACILITY(KOCCI=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
      NOAUDIT)
FACILITY(KOCCI=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

      (where nn is a site unique ID code)
```

Each user that requires access to the OMEGAMON II for CICS product is given access to the appropriate Facilities.

(7) Ensure that the vendor-provided KLVTSNEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

12.2.7.4.2 TOP SECRET Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for CICS:

(1) To implement External Security validation for OMEGAMON command levels, update the Resource Definition Table adding a class name of KOCCANDL:

TSS ADD(RDT) RESCLASS(KOCCANDL) RESCODE(*xx*) ATTR(LONG)
TSS ADD(*dept-acid*) RESOURCE(KOCCANDL)

(where xx is an unused hex value)

NOTE: A department must be given ownership of the RDT entries.

(2) Ensure that the TOP SECRET exit program is installed properly to provide for command-level security. During the installation, the resource class of KOCCANDL will be specified. Ensure that line 00670000 reads as follows in source member KOCATOPS:

MVC U#CHCLSD,=CL8'KOCCANDL' ALTERNATE RES/CLASS NAME

Run job KOCJTOPS to assemble and link the exit.

NOTE: The TOP SECRET exit program must be specified with the MODULE=KOCATOPS parameter in the KOCSECUR member of SYS3.OMEGAMON.qualifier.RKC2DATA.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Assign ownership of the following OMEGAMON resource specifying the appropriate department ACID and KOCCANDL resource class. For example:

TSS ADD(*security-dept-acid*) KOCCANDL(INITIAL)

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

TSS PERMIT(*sys-level-support-grp-0*) KOCCANDL(INITIAL0)
TSS PERMIT(*sys-level-support-grp-1*) KOCCANDL(INITIAL1)
TSS PERMIT(*sys-level-support-grp-2*) KOCCANDL(INITIAL2)

TSS PERMIT(*sys-prog-grp*) KOCCANDL(INITIAL3)

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such it is restricted only to systems programmers.

(6) Optionally, a site can use TOP SECRET controls to protect commands to the individual level rather than the security levels. This is accomplished by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for CICS does not use SAF to restrict access authorization to the OMEGAMON II for CICS APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*COP01 and A*xx*COP02 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming and operations). For example:

TSS PERMIT(*sys-prog-grp*) KLS(A*xx*COP01) ACCESS(READ)
TSS PERMIT(*sys-prog-grp*) KLS(A*xx*COP02) ACCESS(READ)

(8) Configure and install the security table, KOCSECUR, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KOCATOPS security module. Run job KOCSECJB to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

12.2.8 OMEGAMON II for DB2

12.2.8.1 Security Overview

OMEGAMON II for DB2 is a comprehensive performance monitor product for the IBM DB2 database product. Its real-time monitor alerts the user to DB2 response time degradation and overall system problems. This product has the capability of interfacing with the installed ACP or using internal security. The DOD standard is to use external security for controlling access.

12.2.8.1.1 Command-level Security

OMEGAMON II has many commands that are used to inquire and optionally make changes to system parameters and values. The product allows each command to have a security level assigned to it, ranging from 0 to 3. Users are then assigned a security level within their profile that allows them to issue commands assigned to their level and lower. As an example, a user with Level 2 can execute commands secured at Levels 0, 1, or 2. Level 3 provides the highest degree of protection for sensitive commands. A setting of 0 means that any user can access the command. Access to Level 3 should be strictly controlled and only granted to authorized systems personnel.

The following authorized commands are installed with a security level of 3 by default from the vendor, and are to remain as Level 3 commands:

AMAP	CONS	DCMD	DCNS	DDNS	.DSA
JOBS	MCHN	MLST	MODS	MSCN	MZAP
OCMD	OSPC	PEEK	SCHN	SLST	SSCN
SUBP	SZAP	TCBS	TCMD	XMCH	XMLS
XMSC	XMZP				

The ACP determines which security level is associated with a user. Please refer to the following ACP-specific sections for the details on how this is controlled.

NOTE: During the installation of the product, Candle internal security assigns default passwords to the various security levels. This password can be entered in response to a **/PWD** command entered by the user to change the security level. Even though the STIG requirement does not allow users to change their security levels via these passwords, each site is required to change their passwords from the defaults.

12.2.8.1.2 APF Authorization

Several OMEGAMON II for DB2 data sets require APF authorization. These data sets include the following:

SYS2.OMEGAMON.RKANMOD
SYS2.OMEGAMON.RKANMODI
SYS2.OMEGAMON.RKANMODL

Each of these libraries requires explicit protection. *Read* access should be restricted to the OMEGAMON started tasks. Restrict access greater than *read* to only the systems programming personnel responsible for product installation/maintenance. Refer to *Section 2.1.2.1, Authorized Program Facility (APF),* for additional information.

12.2.8.2 ACF2

This section provides the guidance on what values and controls should be in place for product security. Please refer to the installation instructions from the supporting software organization, or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using ACF2 as the ACP for this OMEGAMON II software monitoring product.

12.2.8.2.1 ACF2 Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for DB2:

(1) During final product configuration (CICAT), specify ACF2 CUA Interface Security. As a result of this, configure member KD2INNAM in SYS3.OMEGAMON.*qualifier*.RKD2PAR to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKD2NAM)
    EXIT=KD2A2NEV NORACF NODB
```

(2) Ensure that the vendor-provided KD2A2NEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Protect all OMEGAMON II for DB2 data sets (e.g., SYS2.OMEGAMON, SYS3.OMEGAMON) using ACF2. Limit access to these files to the OMEGAMON started tasks and the systems programming personnel responsible for installation and maintenance of the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(4) Define the logonid D2CUA as a MUSASS NO-SMC STC.

(5) Define the logonid O2CI as a NO-SMC STC.

12.2.8.2.2 ACF2 Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for DB2:

(1) Ensure the resource type is defined as ODS. This is accomplished in the actual KO2ACF2X source module. Line 07600000 should be changed to read as follows:

A#ACFCLS DC CL4'RODS'

Run job KO2ACF2A to assemble and link the exit. This resource type will also be defined to the ACF2 INFODIR GSO record.

NOTE: The ACF2 exit program must be specified with the MODULE=KO2ACF2X parameter in the KO2SUPDI member of SYS3.OMEGAMON.qualifier.RKD2SAM.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(2) Define the following resource rules to prevent unauthorized access to OMEGAMON. Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

$KEY(INITIAL) TYPE(ODS)
UID(-) PREVENT

$KEY(INITIAL0) TYPE(ODS)
UID(-) PREVENT
UID(*sys-level-support-grp-0*) ALLOW

$KEY(INITIAL1) TYPE(ODS)
UID(-) PREVENT
UID(*sys-level-support-grp-1*) ALLOW

$KEY(INITIAL2) TYPE(ODS)
UID(-) PREVENT
UID(*sys-level-support-grp-2*) ALLOW

$KEY(INITIAL3) TYPE(ODS)
UID(-) PREVENT
UID(*sys-prog-grp*) ALLOW

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(3) The INITIAL3 rule controls access to all of the sensitive commands. As such, restrict it to only systems programmers.

(4) Optionally, a site may use ACF2 controls to protect commands to the individual level rather than to the security level. This is done by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(5) OMEGAMON II for DB2 does not use SAF to restrict access authorization to the OMEGAMON II for DB2 APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*D2P01 and A*xx*ODP01 to the APL resource type. Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

```
$KEY(Axx D2P01) TYPE(APL)
UID(-) PREVENT
UID(sys-prog-grp) ALLOW

$KEY(Axx ODP01) TYPE(APL)
UID(-) PREVENT
UID(sys-prog-grp) ALLOW
```

(6) Configure and install the security table, KO2SUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KO2ACF2X security module. Run job KO2SUPD to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.8.3 RACF

This section provides the guidance on what values and controls should be in place for product security. Please refer to the installation instructions from the supporting software organization, or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using RACF as the ACP for this OMEGAMON II software monitoring product.

12.2.8.3.1 RACF Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for DB2:

(1) During final product configuration (CICAT), specify RACF CUA Interface Security. As a result of this, configure member KD2INNAM in SYS3.OMEGAMON.*qualifier*.RKD2PAR to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKD2NAM)
    RACF NODB
```

(2) Protect all OMEGAMON data sets using RACF. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets.

(3) Ensure the following:

(a) The STC userids O2CI and D2CUA are defined as PROTECTED userids.

(b) The userids O2CI and D2CUA are connected to a group for the OMEGACENTER started tasks.

(c) The O2CI and D2CUA STCs have matching profiles defined to the STARTED class with no special attributes. For example:

```
RDEFINE STARTED O2CI.* UACC(NONE) OWNER(admin)
    STDATA(USER(O2CI) GROUP(STCOMEG) TRUSTED(NO))
```

12.2.8.3.2 RACF Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for DB2.

(1) Ensure that the RACF exit program is installed properly to provide for command-level security. During the installation, the resource class of $$ODCAN will be specified. Ensure that line 00920001 reads as follows in source member KO2RACFX:

```
MVC U#CHCLSD,=CL8'$$ODCAN '     ALTERNATE RES/CLASS NAME
```

Run job KO2RACFA to assemble and link the exit.

NOTE: The RACF exit program must be specified with the MODULE=KO2RACFX parameter in the KO2SUPDI member of SYS3.OMEGAMON.qualifier.RKD2SAM.

(2) A new class is added to the RACF Class Descriptor Table and the RACF Router Table for classname $$ODCAN. The following is a sample for the class entry:

```
ICHERCDE CLASS=$$ODCAN,
         ID=nnn,
         MAXLNTH=8,
         FIRST=ALPHANUM,
         OTHER=ANY,
         POSIT=nnn,
         DFTUACC=NONE
```

NOTE: Local configuration determines the value of nnn.

```
ICHRFRTB CLASS=$$ODCAN,
         ACTION=RACF
```

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Define the following resource profiles to the $$ODCAN class to prevent unauthorized access to OMEGAMON:

```
RDEFINE $$ODCAN INITIAL UACC(NONE)
RDEFINE $$ODCAN INITIAL0 UACC(NONE)
RDEFINE $$ODCAN INITIAL1 UACC(NONE)
RDEFINE $$ODCAN INITIAL2 UACC(NONE)
RDEFINE $$ODCAN INITIAL3 UACC(NONE)
```

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

```
PERMIT INITIAL0 CLASS($$ODCAN) ID(sys-level-support-grp-0)
    ACCESS(READ)
PERMIT INITIAL1 CLASS($$ODCAN) ID(sys-level-support-grp-1)
    ACCESS(READ)
PERMIT INITIAL2 CLASS($$ODCAN) ID(sys-level-support-grp-2)
    ACCESS(READ)
PERMIT INITIAL3 CLASS($$ODCAN) ID(sys-prog-grp) ACCESS(READ)
```

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such, restrict it to only systems programmers.

(6) Optionally, a site may use RACF controls to protect commands to the individual level rather than the security levels. This is done by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for DB2 does not use SAF to restrict access authorization to the OMEGAMON II for DB2 APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*D2P01 and A*xx*ODP01 to the APPL resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

```
RDEFINE APPL Axx D2P01 UACC(NONE)
PERMIT Axx D2P01 CLASS(APPL) ID(sys-prog-grp) ACCESS(READ)
RDEFINE APPL Axx ODP01 UACC(NONE)
PERMIT Axx ODP01 CLASS(APPL) ID(sys-prog-grp) ACCESS(READ)
```

(8) Configure and install the security table, KO2SUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KO2RACFX security module. Run job KO2SUPD to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

12.2.8.4 TOP SECRET

This section provides the guidance on what values and controls should be in place for product security. Please refer to the installation instructions from the supporting software organization, or to the vendor documentation on the detailed procedures for implementation. The following sub-sections outline the use of the different controls necessary when using TOP SECRET as the ACP for this OMEGAMON II software monitoring product.

12.2.8.4.1 TOP SECRET Product-level Security Controls

The following is information related to setting up product-level security for OMEGAMON II for DB2:

(1) During final product configuration (CICAT), specify TOP SECRET CUA Interface Security. As a result of this, configure member KD2INNAM in SYS3.OMEGAMON.*qualifier*.RKD2PAR to read as follows:

```
DEFAULT DSNAME(SYS3.OMEGAMON.qualifier.RKD2NAM)
    EXIT=KD2TSNEV RACF NODB
```

(2) Protect all OMEGAMON data sets using TOP SECRET. Limit access to these files to the OMEGAMON started tasks and the systems programmers responsible for the product. Refer to *Section 12.2.6.1.2, APF Authorization,* for information regarding security controls for APF-authorized data sets. This should be done by performing the following:

(a) Create an OMEGAMON profile to contain all OMEGAMON permissions:

```
TSS CREATE(NPBOMEG) NAME( OMEGAMON STC PROFILE')
    TYPE(PROFILE) DEPT(dept-acid)
```

(b) Permit the OMEGAMON profile (*NPBOMEG*) *all* access to SYS3.OMEGAMON.* and *update* access to SYS2.OMEGAMON.* data sets:

```
TSS PERMIT(NPBOMEG) DSN(SYS3.OMEGAMON.) ACCESS(ALL)
TSS PERMIT(NPBOMEG) DSN(SYS2.OMEGAMON.) ACCESS(UPDATE)
```

(c) Permit the OMEGAMON profile *read* access to all OMEGAMON *loadlibs*:

```
TSS PERMIT(NPBOMEG) DSN(omegamon.load.library) ACCESS(READ)
```

(3) Create the STC ACIDs D2CUA and O2CI with a non-expiring password, sourced to the internal reader, and a Master Facility. The MASTFAC matches the name of the STC ACID. For example:

```
TSS CREATE(D2CUA) NAME('OMEGAMON DB2 STC') TYPE(USER)
    DEPT(dept-acid) PASSWORD(password,0) FAC(STC)
        MASTFAC(D2CUA) SOURCE(INTRDR)
```

(4) Add the OMEGAMON profile to the STC ACIDs D2CUA and O2CI. For example:

TSS ADD(D2CUA) PROFILE(*npbomeg*)

(5) Add the STCs D2CUA and O2CI to the Started Task Table specifying the associated matching ACID. For example:

TSS ADD(STC) PROCNAME(D2CUA) ACID(D2CUA*)*

(6) Ensure that D2CUA and O2CI are defined as Facilities to TOP SECRET in the Facility Matrix Table using the following examples:

D2CUA FACILITY CONTROLS SIGNON

FACILITY(USER*xx*=NAME=D2CUA)
FACILITY(D2CUA=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(D2CUA=PGM=VTP,NOASUBM,NOABEND,NOXDEF)
FACILITY(D2CUA=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
SIGN(M))
FACILITY(D2CUA=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(D2CUA=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

O2CIFACILITY CONTROLS SIGNON

FACILITY(USER*xx*=NAME=O2CI)
FACILITY(O2CI=MODE=FAIL,ACTIVE,SHRPRF)
FACILITY(O2CI=PGM=KLV,NOASUBM,NOABEND,NOXDEF)
FACILITY(O2CI=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW,
SIGN(M))
FACILITY(O2CI=NOINSTDATA,NORNDPW,AUTHINIT,NOPROMPT,
NOAUDIT)
FACILITY(O2CI=NOTSOC,LOG(INIT,SMF,MSG,SEC9))

(where nn is a site unique ID code)

Each user that requires access to the OMEGAMON II for DB2 product is given access to the appropriate Facilities.

(7) Ensure that the vendor-provided KD2TSNEV exit program is being used. If modifications to this program are necessary, submit a request to DISA FSO for an integrity review prior to implementation.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

12.2.8.4.2 TOP SECRET Command/Access Security Controls

The following is information relating to setting up command and access controls for OMEGAMON II for DB2:

(1) To implement External Security validation for OMEGAMON command levels, update the Resource Definition Table adding a class name of **KODCANDL**:

TSS ADD(RDT) RESCLASS(KODCANDL) RESCODE(*xx*) ATTR(LONG)
TSS ADD(*dept-acid*) RESOURCE(KODCANDL)

(where xx is an unused hex value)

NOTE: A department must be given ownership of the RDT entries.

(2) Ensure that the TOP SECRET exit program is installed properly to provide for command-level security. During the installation, the resource class of KODCANDL will be specified. Ensure that line 00670000 reads as follows in source member KO2RACFX:

MVC U#CHCLSD,=CL8'KODCANDL' ALTERNATE RES/CLASS NAME

Run job KO2RACFA to assemble and link the exit.

NOTE: The TOP SECRET exit program must be specified with the MODULE=KO2RACFX parameter in the KO2SUPDI member of SYS3.OMEGAMON.qualifier.RKD2SAM.

- *(ZOMG0070: CAT II) The IAO will ensure that OMEGAMON external security exits are installed in accordance with STIG requirements.*

(3) Assign ownership of the following OMEGAMON resource specifying the appropriate department ACID and KODCANDL resource class. For example:

TSS ADD(*security-dept-acid*) KODCANDL(INITIAL)

(4) Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

TSS PERMIT(*sys-level-support-grp-0*) KODCANDL(INITIAL0)
TSS PERMIT(*sys-level-support-grp-1*) KODCANDL(INITIAL1)
TSS PERMIT(*sys-level-support-grp-2*) KODCANDL(INITIAL2)
TSS PERMIT(*sys-prog-grp*) KODCANDL(INITIAL3)

NOTE: The levels of access that are provided for the command structure are progressively restrictive. INITIAL0 access is the least restrictive and is the access authority that is provided to the majority of OMEGAMON II product users. INITIAL3 is the most restrictive and is assigned to the sensitive commands. The INITIAL rule allows a user to enter a password to switch levels. This mechanism is not to be used in the DOD environment and is not granted to any user. The IAO is responsible for the assignment and administration of the access levels.

(5) The INITIAL3 rule controls access to all of the sensitive commands. As such, restrict it to only systems programmers.

(6) Optionally, a site may use TOP SECRET controls to protect commands to the individual level rather than to the security level. This is done by specifying the command as externally validated and writing a rule to allow access to the command. Refer to the vendor documentation for additional information.

(7) OMEGAMON II for DB2 does not use SAF to restrict access authorization to the OMEGAMON II for DB2 APPLIDs. However, sites using CL/SUPERSESSION can control access to VTAM APPLIDs. In accordance with *Section 6.2, CL/SUPERSESSION*, use dynamic application lists to ensure that the ACP arbitrates access to all applications. Sites using CL/SUPERSESSION will define the APPLID(s) of A*xx*D2P01 and A*xx*ODP01 to the KLS resource class. Restrict access to authorized system-level support personnel only (e.g., systems programming, operations, and database administration). For example:

TSS PERMIT(*sys-prog-grp*) KLS(A*xx*D2P01) ACCESS(READ)
TSS PERMIT(*sys-prog-grp*) KLS(A*xx*ODP01) ACCESS(READ)

(8) Configure and install the security table, KO2SUPDI, to specify EXTERNAL=NO for all Level 3 commands, to change the three vendor supplied-level passwords, and to specify the KO2RACFX security module. Run job KO2SUPD to install the security table.

- *(ZOMG0050: CAT II) The systems programmer/IAO will ensure that OMEGAMON APPLIDs are configured and protected in accordance with STIG requirements.*

- *(ZOMG0060: CAT II) The systems programmer/IAO will ensure that OMEGAMON products are configured in accordance with STIG requirements.*

- *(ZOMG0080: CAT II) The systems programmer/IAO will ensure that OMEGAMON resources are protected in accordance with STIG requirements.*

- *(ZOMGT090: CAT II) The systems programmer/IAO will ensure that OMEGAMON facilities are defined in accordance with STIG requirements.*

13. SPOOL ACCESS SOFTWARE

13.1 General Considerations

Spool access software products allow users to display, modify, and control JES activities relative to input, execution, and output queues, and to initiators and output devices. Spool data may be viewed and processed as needed. Some products provide the ability to monitor the system log and to issue system commands.

Consideration is given to securing the data sets that contain the spool access software products. Restrict access to these data sets only to authorized personnel.

Interactive execution of the spool access software products are available under the appropriate TMP. Prohibit access to these on-line applications from general use. Only grant access to authorized personnel.

Spool access software products provide powerful features that are required to be properly controlled. Review of all commands, options, and functions for potential data or system integrity problems, or for possible security exposures. For example, access to JES initiators or printers is not permitted to the general user community, access is only granted to authorized personnel.

Consideration should also be given to limiting the scope of access to data. Since spool access software products monitor all JES activities and access the entire JES spool, the potential exists for users to view restricted information from other tasks.

Depending on the product, control access authority by using one of the following three methods:

- Exclusive use of ACP controls
- A combination of ACP controls and Internal Product Security Controls
- Internal product security only

The IAO administers access authority assignments for users.

Use ACP controls whenever possible. Review all ACP resource interfaces for potential security exposures and for possible implementation. However, it may not be possible to provide a totally secure environment using only ACP controls. In this case, the use of internal security may be warranted and should be investigated for possible use. If it is determined that an enhanced level of protection is gained that the ACP does not provide, the internal security may be activated. It is important to remember that base-level ACP controls are never to be compromised. If the product is not compatible with ACP controls, access authority provided by the product's internal security, is carefully reviewed for possible security risks.

Use the following recommendations when securing spool access software:

(1) Control access to the software product's data sets, and restrict access only to authorized personnel.

(2) Strictly control access to the on-line applications, and restrict access only to authorized personnel.

(3) Rigidly control access to the use of commands, options, and functions within the products. Restrict access to that which is necessary for a user to accomplish that user's assigned responsibilities.

(4) Review product interfaces for potential security exposures. Document any potential security exposures. Notify DISA FSO and the vendor.

(5) Evaluate spool access software product internal security for possible use, providing it does not replace or compromise existing ACP security controls.

13.2 System Display and Search Facility

IBM's System Display and Search Facility (SDSF) is a software product that allows you to monitor, manage, and control OS/390 and z/OS MVS/JES2 systems in a sysplex from a single interface. Through a series of interactive panels, SDSF provides the ability to:

- Control JES2 job processing and spool output
- Control JES2 devices such as printers, initiators, lines, and spool offloaders
- Browse the system log
- Manage system resources such as Workload Management (WLM) resources, JES2 Multi-Access Spool (MAS), and JES2 job classes

13.2.1 General Considerations

The information in this article is based on Version 2, Release 10 of OS/390 unless otherwise noted.

13.2.1.1 SDSF Data Set Protection

The product data sets for SDSF are packaged as follows:

- Distribution data sets hold the master copy of the product elements. There is no typical need for general users to access these data sets. The standard naming convention for these data sets is to use the prefix SYS1.ISF.AISF*.

- Target data sets hold the execution copy of the product elements. General users are likely to need read access to some of these data sets. The standard naming convention for these data sets is to use the prefix SYS1.ISF.SISF*.

- *(ZISF0005: CAT II) The IAO will restrict all update and alter access to SDSF product data sets to systems programming personnel.*

13.2.1.2 ISFPARMS Configuration File

ISFPARMS defines global options, panel formats, and security for SDSF. ISFPARMS can be defined using assembler macros or statements. Statements provide several enhancements compared to assembler macros. Statements are easier to define and are more dynamic when implementing modifications. Several new SDSF functions are not supported with assembler macros.

- *(ZISF0010: CAT II) The systems programmer responsible for supporting SDSF will use the ISFPARMS statement method exclusively to configure SDSF.*

Even when ISFPARMS statements are used exclusively, the ISFPMAC macro must be used to identify the default SDSF server when invoking SDSF. For example:

ISFPMAC SERVER=*server*

The ISFPMAC macro has several other parameters that support the global initialization configuration of SDSF. These parameters will not be coded using the ISFPMAC macro. Instead, the OPTIONS statement will be coded to specify the global initialization parameters.

- *(ZISF0020: CAT II) The systems programmer responsible for supporting SDSF will use the OPTIONS statement to configure the global initialization parameters.*

SDSF reverts from ISFPARMS statement format to ISFPARMS macro format when the SDSF server is unavailable or when ISFPARMS statements are missing. If these situations occur, recovery of normal operations may require access to SDSF using the macro format. For this reason, ISFPARMS macro format may be use to define a recovery group indicating specific individuals responsible for restoring normal system operations.

- *(ZISF0030: CAT II) The systems programmer responsible for supporting SDSF will use the ISFPARMS macro format using the ISFGRP macro to define a specific recovery group used for restoring normal system operations.*

- *(ZISF0040: CAT II) The systems programmer responsible for supporting SDSF will define individual members from the systems programming group to the SDSF recovery group.*

- *(ZISF0050: CAT II) The systems programmer responsible for supporting SDSF will ensure that any IBM default groups defined using the ISFPARMS macro format are removed.*

13.2.1.3 Security Implementation

The SAF interface is an alternative to using ISFPARMS to provide security for SDSF. The use of the SAF interface is consistent with the DOD requirement to control all products within the operating system using the ACP.

- *(ZISF0060: CAT II) The IAO will use SAF security to protect SDSF and its resources.*

SDSF may revert to ISFPARMS security if SAF returns an indeterminate result and cannot make a security decision. In a RACF environment, this can occur when a resource class is inactive or no profiles are defined to a resource class. To ensure SAF security is always in effect, the ACP must be configured to actively support the required SAF resource classes.

- *(ZISF0070: CAT II) The IAO will configure the ACP to actively support the SDSF, WRITER, JESSPOOL, and OPERCMDS resource classes.*

Installation exit routines can be written for the set of exit points provided by SDSF. These routines can supplement the authorizations established with ISFPARMS and the SAF security interface. These programs allow for customized authorization processing and return to SDSF their authorization decisions.

Implementation of any of the installation exit routines is subject to the requirements for exits as specified in *Section 2.1.2, Software Integrity*, and *Section 2.1.2.6, OS/390 and Other Product Exits*. As of the publication of this document, DISA FSO has not approved the use of any SDSF installation exit routines.

- *(ZISF0080: CAT II) The systems programmer responsible for supporting SDSF will ensure that installation exit routines are reviewed, approved, and implemented in accordance with STIG required policy.*

13.2.1.4 ISFPARMS OPTIONS Statement

The ISPPARMS OPTIONS statement specifies the global initialization parameters for SDSF. Three of these parameters have security considerations and are discussed in this section.

ISFPARMS OPTIONS STATEMENT PARAMETERS	
PARAMETER/VALUE	*FUNCTION*
ATHOPEN (YES)	Allows SDSF to bypass ACP protection when opening data sets that are dynamically allocated by SDSF.
INDEX (sys1.haspindx)	Specifies the HASPINDX data set dynamically allocated by SDSF.

Specifying ATHOPEN (YES) makes SDSF a ‘trusted’ STC in regards to data set access and as such it is able to access any data set on the system. This privilege is required primarily to allow SDSF to access JES2 spool data sets when SAF protection is enabled for the JES2 spool. Protection of JES2 spool data is a STIG requirement. Information on securing the JESSPOOL class resources is discussed in Section 5.1.4, Security Controls for JES2 SPOOL Data Sets.

NOTE: Beginning with z/OS V1R2 JES2 environments, SDSF does not allocate the JES2 spool volumes. Therefore the ATHOPEN parameter in ISFPARMS is obsolete with z/OS V1R2 and above.

The HASPINDX data set is used by SDSF when building the SYSLOG panel. This data set contains information related to all SYSLOG jobs and data sets on the spool. Since SDSF dynamically allocates this data set, explicit user access authorization to this data set should not be required. Due to the potentially sensitive data in this data set, access authorization will be restricted.

- *(ZISF0090: CAT II) The IAO will restrict all access to the HASPINDX data set specified on the INDEX parameter to systems programming personnel.*

NOTE: Users may allocate individual HASPINDX data sets in their TSO logon procedures. This requirement pertains to the system-wide HASPINDX data set only. It does not pertain to individual HASPINDX data sets.

13.2.1.5 ISFPARMS GROUP Statement

The ISFPARMS GROUP statement defines user groups and their characteristics. Some of these characteristics include access authorization to SDSF functions and commands. Access to these functions and commands can be controlled alternatively using SAF resources. The use of the SAF interface is consistent with the DOD requirement to control all products within the operating system using the ACP. To ensure SAF security is always in effect, authorizations to SDSF functions and commands should not be defined in ISFPARMS.

- *(ZISF0100: CAT II) The systems programmer responsible for supporting SDSF will not specify any Group Function Parameters supported by SAF-equivalent resources on GROUP statements defined in ISFPARMS. These Group Function Parameters include AUTH, CMDAUTH, CMDLEV, and DSPAUTH.*

13.2.1.6 SDSF Server File Specification

The SDSF server is an address space that SDSF uses to process ISFPARMS statements and provides the ability to view sysplex data on various panels. The input to the SDSF server is the ISFPARMS statements. By default, SDSF uses SYS1.PARMLIB member ISFPRMxx as input to read the ISFPARMS statements. The SDSFPARM DD statement may be used to specify an alternative location for ISFPARMS statements. Explicit JCL specifications ensure expected operations, reduce ambiguity, and are self-documenting.

- *(ZISF0110: CAT II) The systems programmer responsible for supporting SDSF will use SYS1.PARMLIB member ISFPRMxx as input to the ISFPARMS statements for the SDSF server.*

- *(ZISF0120: CAT II) The systems programmer responsible for supporting SDSF will specify SYS1.PARMLIB on the SDSFPARM DD statement in the SDSF procedure.*

13.2.1.7 SDSF Resource Protection

SAF can be used to control the following SDSF resources and functions. Each of these topics are addressed in separate sections. As with all general sections in the OS/390 STIG, the discussion uses RACF-oriented language. Each topic discussed in the general sections are addressed in an ACP-specific section demonstrating how to meet STIG requirements using ACP command examples.

- Membership in SDSF Groups
- SDSF Panels
- SDSF Maintenance Commands
- SDSF Filtering Commands
- SDSF / Command
- Action Characters
- Overtypeable Fields
- MVS and JES2 Commands Generated by SDSF
- Destination Names
- Destination Operator Authority
- Initiators
- Printers and Punches
- Lines
- Nodes
- Offloader
- MAS Members
- Job Classes
- Scheduling Environments
- WLM Resources
- System Requests
- WLM Enclaves
- z/OS UNIX Processes
- Spool Volumes
- Jobs, Output Groups, and SYSIN/SYSOUT Data Sets
- SDSF Server Operations
- MQSeries for OS/390

An operation performed by an SDSF user often requires access authorization to more than one resource class and resource name. In order to perform the task, a user must have proper authority to all of the required resources. For example, to overtype a field in an SDSF panel, a user must have access to the panel, to the overtypeable field, to the MVS or JES2 command that is generated, and to the object (e.g., the job, output group, initiator, or printer) being acted upon. IBM's OS/390 SDSF Customization and Security Guide and z/OS SDSF Operation and Customization Guide provide several tables documenting the relationship between SDSF commands and functions to SAF resources.

In *Section 3.1.5.6, OS/390 System Command Controls*, and *Section 5.1.5, Security Controls for JES2 Commands*, the OS/390 STIG requires the site's installation SOP to document user access to system commands in terms of responsibilities and roles. The system-level groups defined in

the SOP and the functions they perform are used to document and justify the access requirements to specific SDSF SAF resources.

The intention of this section is to document the minimum controls required to protect SDSF resources. It is strongly suggested that IBM's OS/390 SDSF Customization and Security Guide or z/OS SDSF Operation and Customization Guide be reviewed prior to implementation of SAF controls. An implementation of this scale should be tested thoroughly on a test/development platform before defining the security controls in a production environment.

13.2.1.7.1 Membership in SDSF Groups

The ISFPARMS GROUP statement defines user groups and which functions the members of the groups may perform. Membership in these groups can be controlled using SAF resource names. The format of the resource is GROUP.group-name.server. For example, the following GROUP statement defines a group with the name SYSPROG:

```
GROUP NAME(SYSPROG) ACTION(ALL) APPC(ON) …
```

Assuming the name of the SDSF server is SDSF, the SAF resource name used to permit access to this group is GROUP.SYSPROG.SDSF. The number of groups defined in ISFPARMS is site dependent. However, it is suggested that at least three be defined to provide the necessary distinction in functionality. These groups are systems programming, operations, and end-user.

The following table lists the SAF resource information relative to the protection of groups defined by the ISFPARMS GROUP statement:

SDSF ISFPARMS GROUP STATEMENT SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*FUNCTION*
SDSF	GROUP.*group-name.server*	READ	Membership of an SDSF group defined in ISFPARMS

- *(ZISF0130: CAT II) The IAO will define all groups created using the GROUP statements in the ISFPARMS to the ACP with no user access by default.*

- *(ZISF0130: CAT II) The IAO will define a generic resource such as GROUP. to the ACP to provide the default protection.*

- *(ZISF0130: CAT II) The IAO will restrict access to group resources to the appropriate personnel according to their role and function. For example, if a SYSPROG group is defined with the functions suited for systems programmers, access to the GROUP.SYSPROG.server will be restricted to systems programming personnel.*

13.2.1.7.2 SDSF Panels

SDSF panels provide access to JES2 data and operating system resources. While some panels are suitable for end-users to review their JES2 job activities, many panels are dedicated to supporting the operating systems and must be restricted to appropriate personnel.

Panels can be categorized as either end-user displays or operator displays. When using SAF resources to control access to SDSF panels, end-user displays are indicated by DSP as the second node in the resource name, and operator displays are indicated by ODSP as the second node in the resource name.

The following table lists the SAF resource information relative to the protection of SDSF panels:

Table B-22. SDSF PANEL SAF RESOURCES (13.2.1.7.2)

SDSF PANEL SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFCMD.DSP.ACTIVE.*jesx*	READ	Display Active users (DA) panel command
SDSF	ISFCMD.DSP.HELD.*jesx*	READ	Held Output (H) panel command
SDSF	ISFCMD.DSP.INPUT.*jesx*	READ	Input Queue (I) panel command
SDSF	ISFCMD.DSP.OUTPUT.*jesx*	READ	Output Queue (O) panel command
SDSF	ISFCMD.DSP.STATUS.*jesx*	READ	Status (ST) panel command
SDSF	ISFCMD.DSP.SCHENV.*system*	READ	Scheduling Environment (SE) panel command
SDSF	ISFCMD.ODSP.JOBCLASS.*jesx*	READ	Job Class (JC) panel command
SDSF	ISFCMD.ODSP.INITIATOR.*jesx*	READ	Initiator (INIT) panel command
SDSF	ISFCMD.ODSP.LINE.*jesx*	READ	Line (LI) panel command
SDSF	ISFCMD.ODSP.NODE.*jesx*	READ	Node (NO) panel command
SDSF	ISFCMD.ODSP.SO.*jesx*	READ	Spool Offload (SO) panel command
SDSF	ISFCMD.ODSP.MAS.*jesx*	READ	Multi-Access Spool (MAS) panel command
SDSF	ISFCMD.ODSP.SYSLOG.*jesx*	READ	Syslog and Operlog (LOG) panel

SDSF PANEL SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
			command
SDSF	ISFCMD.ODSP.PRINTER.*jesx*	READ	Printer (PR) panel command
SDSF	ISFCMD.ODSP.PUNCH.*jesx*	READ	Punch (PUN) panel command
SDSF	ISFCMD.ODSP.READER.*jesx*	READ	Reader (RDR) panel command
SDSF	ISFCMD.ODSP.RESOURCE.*system*	READ	Resource (RES) panel command
SDSF	ISFCMD.ODSP.SR.*system*	READ	System Request (SR) panel command
SDSF	ISFCMD.ODSP.ULOG.*jesx*	READ	User Log (ULOG) panel command
SDSF	ISFCMD.ODSP.ENCLAVE	READ	Enclave (ENC) panel command
SDSF	ISFCMD.ODSP.PROCESS	READ	Process (PS) panel command
SDSF	ISFCMD.ODSP.SPOOL.*jesx*	READ	Spool (SP) volume panel command

In the table:
- jesx is the name of the JES2 subsystem
- system is the name of the MVS system (sysplex support)

NOTE: The ENC, PS, and SP panel commands only apply to z/OS V1R2 and above.

- *(ZISF0140: CAT II) The IAO will define SDSF panel SAF resources to the ACP with no user access by default.*

- *(ZISF0140: CAT II) The IAO will define generic resources such as ISFCMD.DSP. and ISFCMD.ODSP. to the ACP to provide the default protection.*

- *(ZISF0140: CAT II) The IAO will restrict all access to SDSF operator display resources to operations personnel and systems programming personnel.*

- *(ZISF0140: CAT II) The IAO will restrict all access to SDSF end-user display resources to authorized SDSF users.*

13.2.1.7.3 SDSF Maintenance Commands

Maintenance commands are used to support the SDSF product. The personnel maintaining SDSF for the user community may use these commands to aid in problem resolution. The

following table lists the SAF resource information relative to the protection of SDSF maintenance commands:

Table B-23. SDSF MAINTENANCE COMMAND SAF RESOURCES (13.2.1.7.3)

SDSF MAINTENANCE COMMAND SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFCMD.MAINT.ABEND	READ	Cause SDSF to abend
SDSF	ISFCMD.MAINT.TRACE	READ	Create trace records with SDSF data

- *(ZISF0150: CAT II) The IAO will define SDSF maintenance command SAF resources to the ACP with no user access by default.*

- *(ZISF0150: CAT II) The IAO will define a generic resource such as ISFCMD.MAINT. to the ACP to provide the default protection.*

- *(ZISF0150: CAT II) The IAO will restrict all access to SDSF maintenance command resources to systems programming personnel.*

13.2.1.7.4 SDSF Filtering Commands

Filtering commands are used to control the data displayed on SDSF panels. Some filter commands are used only for supporting the operating system, and others provide the ability to display data on a system-wide level. Filter commands can be used to override the configuration in ISFPARMS.

The following table lists the SAF resource information relative to the protection of SDSF filtering commands:

Table B-24. SDSF FILTERING COMMAND SAF RESOURCES (13.2.1.7.4)

SDSF FILTERING COMMAND SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFCMD.FILTER.ACTION	READ	Display WTOR messages by routing code
SDSF	ISFCMD.FILTER.DEST	READ	Display jobs based on destination
SDSF	ISFCMD.FILTER.FINDLIM	READ	Reset the line limit for the FIND command
SDSF	ISFCMD.FILTER.INPUT	READ	Include SYSIN data sets on display
SDSF	ISFCMD.FILTER.OWNER	READ	Display jobs based on owning IDs
SDSF	ISFCMD.FILTER.PREFIX	READ	Display jobs based on job name
SDSF	ISFCMD.FILTER.RSYS	READ	Display WTOR messages by system name
SDSF	ISFCMD.FILTER.SYSID	READ	Display SYSLOG data based on JES2 system name
SDSF	ISFCMD.FILTER.SYSNAME	READ	Display sysplex data based on system name

- *(ZISF0160: CAT II) The IAO will define SDSF filtering command SAF resources to the ACP with no user access by default.*

- *(ZISF0160: CAT II) The IAO will define a generic resource such as ISFCMD.FILTER. to the ACP to provide the default protection.*

- *(ZISF0160: CAT II) The IAO will restrict all access to SDSF filter command resources to operations personnel and systems programming personnel.*

- *(ZISF0160: CAT II) The IAO will restrict all access to the ISFCMD.FILTER.INPUT resource to systems programming personnel only.*

13.2.1.7.5 SDSF / Command

The SDSF / command can be used to issue MVS or JES2 commands from the SDSF command line. Use of the **/** command must be protected as you would any system console.

While the SDSF control checks the user's authority to use the / command, it does not check the user's authorization to the MVS or JES2 command or the object of the command. MVS and JES2 command authorization to the OPERCMDS resource class is performed by MVS and JES2 only after SDSF checks the authorization to the / command. Refer to *Section 3.1.5.6*, *OS/390 System Command Controls*, and *Section 5.1.5, Security Controls for JES2 Commands*, for information on controlling these resources.

The following table lists the SAF resource information relative to the protection of the SDSF / command:

Table B-25. SDSF/COMMAND SAF RESOURCE (13.2.1.7.5)

SDSF/COMMAND SAF RESOURCE			
RESOURCE CLASS	***RESOURCE NAME***	***REQUIRED ACCESS***	***DESCRIPTION***
SDSF	ISFOPER.SYSTEM	READ	Issue the / command

- *(ZISF0170: CAT II) The IAO will define the SDSF / command SAF resource to the ACP with no user access by default.*

- *(ZISF0170: CAT II) The IAO will restrict all access to the ISFOPER.SYSTEM resource to operations personnel and systems programming personnel.*

13.2.1.7.6 Action Characters

Action characters are short commands, usually one or two characters that are entered in the NP column of SDSF panels. Unlike most SDSF commands, action characters are not SAF-protected as distinct resources. The security controls relative to the use of action characters is with the object of the action and the MVS or JES2 command generated in response to the action character. The objects of action characters are resources such as initiators in the SDSF class, printers and punches in the WRITER class, and jobs, output groups, and SYSIN/SYSOUT data sets in the JESSPOOL class.

For example, if a user enters a C action character on the printer panel to purge output, two SAF calls are generated. The first SAF call checks that the user has update access to the printer defined to the WRITER resource class. The second SAF calls check that the user has update access to the jesx.CANCEL.DEV resource defined to the OPERCMDS resource class. There is no specific SAF call for the C action character. The user requires the proper access authorization to both resources to perform the action. Security requirements regarding the objects of actions are discussed in various sections throughout this chapter. Security requirements regarding the protection of MVS system commands are discussed in *Section 3.1.5.6, OS/390 System Command Controls*. Security requirements regarding the protection of JES2 commands are discussed in *Section 5.1.5, Security Controls for JES2 Commands*. Refer to *Section 13.2.1.7.8, MVS and JES2 Commands Generated by SDSF*, for additional security requirements regarding end-users under SDSF.

13.2.1.7.7 Overtypeable Fields

Most SDSF panels contain data that is modifiable. When the user overtypes the data displayed in a field on the panel, the field value can be changed permanently. Use of an overtypeable field causes an interaction with three resources—(1) the overtypeable field; (2) the object of the overtypeable field, such as an initiator, printer, MAS member, or job, and (3) the MVS or JES2 command generated by overtyping the field.

There are approximately 200 specific SAF resource names available to control access to overtypeable fields. In general, the use of overtypeable fields results in the modification of a system-level resource and functions as a shortcut for issuing system commands. As such, access authorization to most SDSF overtypeable fields should be restricted to the appropriate personnel responsible for supporting the operating system.

Some SDSF overtypeable fields present on end-user displays can be used to manage job status and output. With the additional security controls in effect for SDSF resources and JESSPOOL resource protection enabled, end-users can be allowed access to overtypeable fields that modify jobs ensuring that these fields are only issued on the appropriate JES2 jobs.

The following table lists the SAF resource information relative to the protection of the SDSF overtypeable fields:

Table B-26. SDSF OVERTYPEABLE FIELD SAF RESOURCES (13.2.1.7.7)

SDSF OVERTYPEABLE FIELD SAF RESOURCES				
RESOURCE CLASS	*RESOURCE NAME*	*REQ'D ACCESS*	*DESCRIPTION*	*USER/ GROUP*
SDSF	ISFATTR.OUTPUT.**	UPDATE	Modify output group fields on the Held Output (H) and Output Queue (O) panels	Operations Systems
SDSF	ISFATTR.OUTPUT.BURST	UPDATE	Modify burst indication field on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.CLASS	UPDATE	Modify JES2 output class on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.DEST	UPDATE	Modify JES2 print destination name on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.FCB	UPDATE	Modify output FCB ID on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.FLASH	UPDATE	Modify output flash ID on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.FORMS	UPDATE	Modify output form number on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.PRMODE	UPDATE	Modify printer process mode on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.UCS	UPDATE	Modify output UCS ID on H and O panels	End-user Operations Systems
SDSF	ISFATTR.OUTPUT.WRITER	UPDATE	Modify output external writer name on H and O panels	End-user Operations Systems

SDSF OVERTYPEABLE FIELD SAF RESOURCES				
RESOURCE CLASS	*RESOURCE NAME*	*REQ'D ACCESS*	*DESCRIPTION*	*USER/ GROUP*
SDSF	ISFATTR.OUTDESC.**	UPDATE	Modify output descriptor fields on the Job Data Set (JDS) and Output Descriptor (OD) panels	End-user Operations Systems
SDSF	ISFATTR.LINE.**	UPDATE	Modify Line panel fields	Operations Systems
SDSF	ISFATTR.NODE.**	UPDATE	Modify Node panel fields	Operations Systems
SDSF	ISFATTR.OFFLOAD.**	UPDATE	Modify Spool Offload panel fields	Operations Systems
SDSF	ISFATTR.MODIFY.**	UPDATE	Modify Spool Offload panel fields	Operations Systems
SDSF	ISFATTR.JOB.**	UPDATE	Modify job fields on the Display Active (DA), Input (I), and Status (ST) panels	Operations Systems
SDSF	ISFATTR.JOB.PRTDEST	UPDATE	Modify JES2 print destination name on ST and I panels	End-user Operations Systems
SDSF	ISFATTR.JCLS.**	UPDATE	Modify Job Class panel fields	Operations Systems
SDSF	ISFATTR.MEMBER.**	UPDATE	Modify Multi-Access Spool panel fields	Operations Systems
SDSF	ISFATTR.PROPTS.**	UPDATE	Modify Printer panel fields, lines and transmitter fields on the Lines panel, and Punch panel fields	Operations Systems
SDSF	ISFATTR.SELECT.**	UPDATE	Modify selection criteria fields on the Initiator, Line, Printer, Punch, and Spool Offload panels	Operations Systems
SDSF	ISFATTR.RDR.**	UPDATE	Modify Reader panel fields	Operations Systems

SDSF OVERTYPEABLE FIELD SAF RESOURCES				
RESOURCE CLASS	*RESOURCE NAME*	*REQ'D ACCESS*	*DESCRIPTION*	*USER/ GROUP*
SDSF	ISFATTR.RESOURCE.**	UPDATE	Modify WLM Resource panel fields	Operations Systems

- *(ZISF0180: CAT II) The IAO will define SDSF overtypeable field SAF resources to the ACP with no user access by default.*

- *(ZISF0180: CAT II) The IAO will define a generic resource such as ISFATTR. to the ACP to provide the default protection.*

- *(ZISF0180: CAT II) The IAO will restrict all access to SDSF overtypeable field resources as indicated in the previous table.*

13.2.1.7.8 MVS and JES2 Commands Generated by SDSF

While systems programming personnel and operations personnel are routinely permitted access to system commands and JES2 commands, end-users are restricted to just a handful of display-type commands. If end-users are allowed to manage their own jobs while under SDSF using functions such as action characters and overtypeable fields, they must be given access to additional OPERCMDS resources. With the additional security controls in effect for SDSF resources and JESSPOOL resource protection enabled, end-users can be allowed access to operator commands that modify jobs ensuring that these commands are only issued on the appropriate JES2 jobs. Refer to *Section 3.1.5.6, OS/390 System Command Controls*, and *Section 5.1.5, Security Controls for JES2 Commands*, for information on securing MVS and JES2 system commands respectively.

The following table indicates the system command SAF resources appropriate for all authorized SDSF users and other related security information:

Table B-27. SYSTEM COMMAND SAF RESOURCES FOR ALL SDSF USERS (13.2.1.7.8)

SYSTEM COMMAND SAF RESOURCES FOR ALL SDSF USERS			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
OPERCMDS	JES2.DISPLAY.BAT	READ	Display (D) action character on various panels
OPERCMDS	JES2.DISPLAY.TSU	READ	
OPERCMDS	JES2.DISPLAY.STC	READ	
OPERCMDS	JES2.DISPLAY.DEV	READ	
OPERCMDS	JES2.MSEND.CMD	READ	Various action characters on the I and ST panels
OPERCMDS	JES2.DISPLAY.BATOUT	READ	List (L) output action character on various end-user panels
OPERCMDS	JES2.DISPLAY.TSUOUT	READ	
OPERCMDS	JES2.DISPLAY.STCOUT	READ	
OPERCMDS	MVS.DISPLAY.WLM	READ	Display (D) MAS members on SE panel
OPERCMDS	JES2.MODIFY.BATOUT	UPDATE	Release (A) and Hold (H) action characters on O and H panels Numerous overtypeable fields on O and H panels
OPERCMDS	JES2.MODIFY.TSUOUT	UPDATE	
OPERCMDS	JES2.MODIFY.STCOUT	UPDATE	
OPERCMDS	MVS.CANCEL.ATX*	UPDATE	Cancel (C, CD, P, PP) action characters on DA, I, and ST panels
OPERCMDS	MVS.CANCEL.TSU	UPDATE	
OPERCMDS	JES2.CANCEL.BAT	UPDATE	Various Cancel and Purge action characters on various end-user panels
OPERCMDS	JES2.CANCEL.TSU	UPDATE	
OPERCMDS	JES2.CANCEL.STC	UPDATE	
OPERCMDS	JES2.CANCEL.DEV	UPDATE	
OPERCMDS	JES2.RELEASE.BATOUT	UPDATE	Cancel (C), Release (O), and Purge (P) action characters and H and ST panels
OPERCMDS	JES2.RELEASE.STCOUT	UPDATE	
OPERCMDS	JES2.RELEASE.TSUOUT	UPDATE	
OPERCMDS	JES2.RESTART.DEV	UPDATE	Restart (E) action character on various panels
OPERCMDS	JES2.RESTART.BAT	CONTROL	
OPERCMDS	JES2.MODIFYHOLD.BAT	UPDATE	Hold (H) action character on DA, I, and ST panels
OPERCMDS	JES2.MODIFYHOLD.STC	UPDATE	
OPERCMDS	JES2.MODIFYHOLD.TSU	UPDATE	
OPERCMDS	JES2.ROUTE.JOBOUT	UPDATE	Overtypeable field PRTDEST on I and ST panels

- *(ACP00270: CAT II) The IAO will ensure that OS/390 Sensitive System Commands are defined to the OPERCMDS resource class. Only limited number of authorized people are able to issue these commands. All access is logged.*

- *(ZJES0052: CAT II) The IAO will ensure that access to JES2 system commands listed in the following table are restricted to the appropriate personnel and logged where indicated:*

13.2.1.7.9 Destination Names

Each JES2 job is associated with a destination. SDSF panel data can be limited to display only job information specific to a destination. Destination names that are used on the DEST command and the IDEST parameter of ISFPARMS can be controlled.

Protection of destinations should be used to ensure JES2 job information is restricted to appropriate personnel. The following table lists the SAF resource information relative to the protection of destination names:

Table B-28. SDSF DESTINATION NAME SAF RESOURCES (13.2.1.7.9)

SDSF DESTINATION NAME SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFOPER.ANYDEST.*jesx*	READ	Any destination name
SDSF	ISFAUTH.DEST.*destname*	READ	Specific destination name

In the table:
- jesx is the name of the JES2 subsystem
- destname is destination name of the job

- *(ZISF0190: CAT II) The IAO will define SDSF destination name SAF resources to the ACP with no user access by default.*

- *(ZISF0190: CAT II) The IAO will define generic resources such as ISFOPER.ANYDEST. and ISFAUTH.DEST. to the ACP to provide the default protection.*

The ISFOPER.ANYDEST.jesx resource must be defined before defining any ISFAUTH.DEST.destname resources or unexpected authorization results may occur. Also, user authorization to ISFOPER.ANYDEST.jesx ensures that jobs are displayed for SDSF users who do not have their default destinations set.

The IAO should permit access to the ISFOPER.ANYDEST.jesx resource to all authorized users of SDSF.

When the IDEST parameter is specified for groups defined to ISFPARMS, a corresponding SAF resource rule for that destination (i.e., ISFAUTH.DEST.destname) must be defined and

authorized to the users in that group. If this is not done, no jobs can appear on the SDSF panels for those users.

- *(ZISF0190: CAT II) The IAO will ensure the following items are in effect when permitting access to ISFAUTH.DEST.destname resources to end-users:*

  - *All ISFAUTH.DEST.destname resources defined to the ACP will be fully qualified and not generic.*

  - *The access level to ISFAUTH.DEST.destname resources will be restricted to **read**.*

  - *The IAO will restrict access to the generic resource ISFAUTH.DEST. to operations personnel and systems programming personnel.*

13.2.1.7.10 Destination Operator Authority

Access to jobs, output groups, or SYSIN/SYSOUT data sets is typically controlled by the JESSPOOL resource class. However, authority can be granted to users allowing them to bypass this JESSPOOL protection and permitting them access to jobs, output groups, or SYSIN/SYSOUT data sets by destination only. This is called destination operator authority.

To permit destination operator authority to a user, you must first give the user READ authority to the ISFOPER.DEST.jesx profile in the SDSF resource class. This identifies the user as a destination operator. Second, you must give the user authorization to the resources in the SDSF resource class that protects the destination for jobs, output groups, and data sets.

The following table lists the SAF resource information relative to the protection of destination operator authority:

Table B-29. SDSF DESTINATION OPERATOR AUTHORITY SAF RESOURCES (13.2.1.7.10)

SDSF DESTINATION OPERATOR AUTHORITY SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAMES*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFOPER.DEST.*jesx*	READ	Browse and print Standard SYSIN/ SYSOUT data sets
	ISFAUTH.DEST.*destname*.DATASET .*dsname*	READ	
SDSF	ISFOPER.DEST.*jesx*	READ	Browse and print Standard SYSIN/ SYSOUT data sets
	ISFAUTH.DEST.*destname*.DATASET.JESJCL	READ	
	ISFAUTH.DEST.*destname*.DATASET .JESMSGLG	READ	
	ISFAUTH.DEST.*destname*.DATASET .JESYSMSG	READ	
SDSF	ISFOPER.DEST.*jesx*	READ	Display and list jobs
	ISFAUTH.DEST.*destname*	READ	
	ISFAUTH.DEST.*qualifier.qualifier*	READ	
SDSF	ISFOPER.DEST.*jesx*	READ	All other functions such as cancel, purge, and release jobs
	ISFAUTH.DEST.*destname*	ALTER	
	ISFAUTH.DEST.*qualifier.qualifier*	ALTER	

In the table:
- *jesx* is the name of the JES2 subsystem
- *destname* is destination name of the job
- *dsname* is name of the data set

- *(ZISF0200: CAT II) The IAO will define SDSF destination operator authority SAF resources to the ACP with no user access by default.*

- *(ZISF0200: CAT II) The IAO will define generic resources such as ISFOPER.DEST., ISFAUTH.DEST., ISFAUTH.DEST.qualifier., ISFAUTH.DEST.qualifier.DATASET., and ., ISFAUTH.DEST.qualifier.DATASET.JCL* to the ACP to provide the default protection.*

NOTE: Protection of ISFAUTH.DEST. resources is also discussed in *Section 13.2.1.7.9, Destination Names*.

- *(ZISF0200: CAT II) The IAO will restrict destination operator authority (i.e., ISFOPER.DEST.jesx) to operations personnel and systems programming personnel.*

- *(ZISF0200: CAT II) The IAO will restrict ALTER access to ISFAUTH.DEST.destname and ISFAUTH.DEST.qualifier.qualifier resources to operations personnel and systems programming personnel.*

There are two types of SYSIN/SYSOUT data sets, Standard and System Message. Standard SYSIN/SYSOUT data sets include system-generated messages, job input, and job output. Destination operator authority to Standard SYSIN/SYSOUT data sets is not a typical authorization required by operations personnel and systems programming personnel as it may allow inappropriate access to user and application data.

- *(ZISF0200: CAT II) The IAO will not permit destination operator authority to Standard SYSIN/SYSOUT data sets (i.e., ISFAUTH.DEST.qualifier.DATASET).*

System Message SYSIN/SYSOUT data sets only contain system-generated messages associated with jobs. Access to system-level job information is a typical requirement for operations personnel and system programming personnel to perform their duties.

- *(ZISF0200: CAT II) The IAO will restrict destination operator authority to System Message SYSIN/SYSOUT data sets (i.e., ISFAUTH.DEST.qualifier.DATASET.JCL*) to operations personnel and systems programming personnel.*

13.2.1.7.11 Initiators

JES2 initiators select jobs for execution and help build the environment for the jobs to execute. Operations related to initiators displayed on the INIT panel can be protected.

The following table lists the SAF resource information relative to the protection of JES2 initiators:

Table B-30. SDSF INITIATOR SAF RESOUCES (13.2.1.7.11)

SDSF INITIATOR SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFINIT.I*xx.jesx*	READ	Display information about an initiator
SDSF	ISFINIT.I*xx.jesx*	CONTROL	All other functions such as start, stop, and drain an initiator

In the table:
- xx is the number of the JES2 initiator
- jesx is the name of the JES2 subsystem

- *(ZISF0210: CAT II) The IAO will define SDSF initiator SAF resources to the ACP with no user access by default.*

- *(ZISF0210: CAT II) The IAO will define generic a resource such as ISFINIT. to the ACP to provide the default protection.*

- *(ZISF0210: CAT II) The IAO will restrict all access to SDSF initiator resources to operations personnel and systems programming personnel.*

13.2.1.7.12 Printers and Punches

Printers and punches are output devices defined to JES2. Operations related to printers and punches displayed on the PR and PUN panels respectively can be controlled while under SDSF using the WRITER resource class.

The following table lists the SAF resource information relative to the protection of JES2 printers and punches:

Table B-31. JES2 PRINTER AND PUNCH SAF RESOURCES (13.2.1.7.12)

JES2 PRINTER AND PUNCH SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
WRITER	*jesx*.LOCAL.*device-name*	READ	Display information about a local printer or punch
WRITER	*jesx*.RJE.*device-name*	READ	Display information about a remote printer or punch
WRITER	*jesx*.LOCAL.*device-name*	ALTER	Purge output on a local printer or punch
WRITER	*jesx*.RJE.*device-name*	ALTER	Purge output on a remote printer or punch
WRITER	*jesx*.LOCAL.*device-name*	CONTROL	All other functions such as start and stop a local printer or punch
WRITER	*jesx*.RJE.*device-name*	CONTROL	All other functions such as start and stop a remote printer or punch

In the table:
- jesx is the name of the JES2 subsystem
- device-name is the name of the printer and punch

Section 5 of the OS/390 STIG discusses the security controls required for JES2. Refer to *Section 5.1.3, Security Controls for Output*, for general requirements regarding printer and punch resources. In addition, the following requirement applies for SDSF:

- *(ZJES0032: CAT II) The IAO will restrict ALTER and CONTROL access to JES2 printer and punch resources to operations and systems programming personnel.*

13.2.1.7.13 Lines

A line is a communications link, such as a wire or telephone circuit, for connecting geographically dispersed computer systems. Operations related to NJE and RJE lines displayed on the LI panel can be protected.

The following table lists the SAF resource information relative to the protection of JES2 communication lines:

Table B-32. SDSF LINE SAF RESOURCES (13.2.1.7.13)

SDSF LINE SAF RESOURCES			
RESOURCE CLASS	***RESOURCE NAME***	***REQUIRED ACCESS***	***DESCRIPTION***
SDSF	ISFLINE.*device-name.jesx*	READ	Display information about a line and associated transmitters and receivers
SDSF	ISFLINE.*device-name.jesx*	ALTER	Cancel data being transmitted and received
SDSF	ISFLINE.*device-name.jesx*	CONTROL	All other functions such as start, stop, and disconnect a line

In the table:
- *device-name* is the name of the line, transmitter, or receiver
- *jesx* is the name of the JES2 subsystem

- *(ZISF0220: CAT II) The IAO will define SDSF line SAF resources to the ACP with no user access by default.*

- *(ZISF0220: CAT II) The IAO will define generic a resource such as ISFLINE. to the ACP to provide the default protection.*

- *(ZISF0220: CAT II) The IAO will restrict all access to SDSF line resources to operations personnel and systems programming personnel.*

13.2.1.7.14 Nodes

A node is one of the systems in a network of systems connected by communication lines or CTC adapters. Operations related to JES2 nodes displayed on the NO panel can be protected.

The following table lists the SAF resource information relative to the protection of JES2 nodes:

Table B-33. SDSF NODE SAF RESOURCES (13.2.1.7.14)

SDSF NODE SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFNODE.*node-name.jesx*	READ	Display information about a node
SDSF	ISFNODE.*node-name.jesx*	CONTROL	All other functions such as start node communication

In the table:
- *node-name* is the name of the JES2 node
- *jesx* is the name of the JES2 subsystem

- *(ZISF0230: CAT II) The IAO will define SDSF node SAF resources to the ACP with no user access by default.*

- *(ZISF0230: CAT II) The IAO will define generic a resource such as ISFNODE. to the ACP to provide the default protection.*

- *(ZISF0230: CAT II) The IAO will restrict all access to SDSF node resources to operations personnel and systems programming personnel.*

13.2.1.7.15 Offloaders

Spool offload devices are used to move jobs and work off the work queues to remove them from contention for system resources, or off spool to free up system work space. Operations related to spool offloaders on the SO panel can be protected.

The following table lists the SAF resource information relative to the protection of spool offloaders:

Table B-34. SDSF SPOOL OFFLOADER SAF RESOURCES (13.2.1.7.15)

SDSF SPOOL OFFLOADER SAF RESOURCES			
RESOURCE CLASS	***RESOURCE NAME***	***REQUIRED ACCESS***	***DESCRIPTION***
SDSF	ISFSO.*device-name.jesx*	READ	Display information about a spool offloader and associated transmitters and receivers
SDSF	ISFSO.*device-name.jesx*	ALTER	Cancel the job and output active on a transmitter and receiver
SDSF	ISFSO.*device-name.jesx*	CONTROL	All other functions such as start and drain an offloader

In the table:
- *device-name* is the name of the offloader, transmitter, or receiver
- *jesx* is the name of the JES2 subsystem

- *(ZISF0240: CAT II) The IAO will define SDSF spool offloader SAF resources to the ACP with no user access by default.*

- *(ZISF0240: CAT II) The IAO will define generic a resource such as ISFSO. to the ACP to provide the default protection.*

- *(ZISF0240: CAT II) The IAO will restrict all access to SDSF spool offloader resources to operations personnel and systems programming personnel.*

13.2.1.7.16 MAS Members

A MAS configuration allows multiple systems to share the JES2 input, job, and output queues through the use of a checkpoint data set or coupling facility. Operations related to members displayed on the MAS panel can be protected.

The following table lists the SAF resource information relative to the protection of MAS members:

Table B-35. SDSF MAS MEMBER SAF RESOURCES (13.2.1.7.16)

SDSF MAS MEMBER SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFMEMB.*member-name.jesx*	READ	Display information about a MAS member
SDSF	ISFMEMB.*member-name.jesx*	ALTER	Stop and restart a member in a MAS
SDSF	ISFMEMB.*member-name.jesx*	CONTROL	All other functions such as stop (abend) and stop (ignore activity) a MAS member

In the table:
- *member-name* is the name of the member defined in the MAS configuration
- *jesx* is the name of the JES2 subsystem

- *(ZISF0250: CAT II) The IAO will define SDSF MAS member SAF resources to the ACP with no user access by default.*

- *(ZISF0250: CAT II) The IAO will define generic a resource such as ISFMEMB. to the ACP to provide the default protection.*

- *(ZISF0250: CAT II) The IAO will restrict all access to SDSF MAS member resources to operations personnel and systems programming personnel.*

13.2.1.7.17 Job Classes

Job classes define many input and output JES2 characteristics associated with each job in each class. Operations related to JES2 job classes displayed on the JC panel can be protected.

The following table lists the SAF resource information relative to the protection of JES2 job classes:

Table B-36. SDSF JOB CLASS SAF RESOURCES (13.2.1.7.17)

SDSF JOB CLASS SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFJOBCL.*class.jesx*	READ	Display information about a job class
SDSF	ISFJOBCL.*class.jesx*	CONTROL	Modify job class characteristics

In the table:
- *class* is the job class
- *jesx* is the name of the JES2 subsystem

- *(ZISF0260: CAT II) The IAO will define SDSF job class SAF resources to the ACP with no user access by default.*

- *(ZISF0260: CAT II) The IAO will define generic a resource such as ISFJOBCL. to the ACP to provide the default protection.*

- *(ZISF0260: CAT II) The IAO will restrict all access to SDSF job class resources to operations personnel and systems programming personnel.*

13.2.1.7.18 Scheduling Environments

Scheduling environments are defined to the WLM and help ensure that units of work are sent to systems that have the appropriate resources to handle them. A scheduling environment is a list of resource names along with their required states. Operations related to WLM scheduling environments displayed on the SE panel can be protected.

The following table lists the SAF resource information relative to the protection of WLM scheduling environments:

Table B-37. SDSF SCHEDULING ENVIRONMENT SAF RESOURCES (13.2.1.7.18)

SDSF SCHEDULING ENVIRONMENT SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFSE.*sched-env.system*	READ	Display information about a scheduling environment

In the table:
- *sched-env* is the name of the scheduling environment
- *system* is the name of the MVS system (sysplex support)

- *(ZISF0270: CAT II) The IAO will define SDSF scheduling environment SAF resources to the ACP with no user access by default.*

- *(ZISF0270: CAT II) The IAO will define generic a resource such as ISFSE. to the ACP to provide the default protection.*

- *(ZISF0270: CAT II) The IAO will restrict all access to SDSF scheduling environment resources to operations personnel, systems programming personnel, and authorized SDSF end-users.*

13.2.1.7.19 WLM Resources

A list of resources makes up a scheduling environment. Resources can represent actual physical entities, such as a database or a peripheral device, or they can represent intangible qualities such as a certain period of time (like second shift or weekend). Operations related to WLM resources displayed on the RES panel can be protected.

The following table lists the SAF resource information relative to the protection of WLM resources:

Table B-38. SDSF WLM RESOURCE SAF RESOURCES (13.2.1.7.19)

SDSF WLM RESOURCE SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFRES.*resource.system*	READ	Display information about a WLM resource
SDSF	ISFRES.*resource.system*	CONTROL	Modify the state of a WLM resource

In the table:
- *resource* is the name of the WLM resource
- *system* is the name of the MVS system (sysplex support)

- *(ZISF0280: CAT II) The IAO will define SDSF WLM resource SAF resources to the ACP with no user access by default.*

- *(ZISF0280: CAT II) The IAO will define generic a resource such as ISFRES. to the ACP to provide the default protection.*

- *(ZISF0280: CAT II) The IAO will restrict all access to SDSF WLM resources to operations personnel and systems programming personnel.*

13.2.1.7.20 System Requests

The System Request (SR) panel allows users to access information about system messages requiring a reply or action. Operations related to system requests displayed on the SR panel can be protected.

The following table lists the SAF resource information relative to the protection of system request resources:

Table B-39. SDSF SYSTEM REQUEST SAF RESOURCES (13.2.1.7.20)

SDSF SYSTEM REQUEST SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFSR.*type.system.jobname*	READ	Display information about system request messages
SDSF	ISFSR.*ACTION.system.jobname*	READ	Remove action messages from the display
SDSF	ISFSR.*REPLY.system.jobname*	READ	Reply to a system message

In the table:
- *type* is the message type (ACTION or REPLY)
- *system* is the name of the originating system
- *jobname* is the name of the job issuing the message

- *(ZISF0290: CAT II) The IAO will define SDSF system request SAF resources to the ACP with no user access by default.*

- *(ZISF0290: CAT II) The IAO will define a generic resource such as ISFSR. to the ACP to provide the default protection.*

- *(ZISF0290: CAT II) The IAO will restrict all access to SDSF system request resources to operations personnel and systems programming personnel.*

13.2.1.7.21 WLM Enclaves

The Enclave (ENC) panel allows users to access information about WLM enclaves. Operations related to enclaves displayed on the ENC panel can be protected.

The following table lists the SAF resource information relative to the protection of WLM enclave resources:

Table B-40. SDSF WLM ENCLAVE SAF RESOURCES (13.2.1.7.21)

SDSF WLM ENCLAVE SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFENC.*subsystem-type.subsystem-name*	ALTER	Resume and quiesce an enclave

In the table:
- *subsystem-type* is the type of subsystem such as MQ or DB2
- *subsystem-name* is the name of the subsystem

NOTE: SDSF WLM enclave SAF resource protection only applies to z/OS V1R4 and above.

- *(ZISF0300: CAT II) The IAO will define SDSF WLM enclave SAF resources to the ACP with no user access by default.*

- *(ZISF0300: CAT II) The IAO will define a generic resource such as ISFENC. to the ACP to provide the default protection.*

- *(ZISF0300: CAT II) The IAO will restrict all access to SDSF WLM enclave resources to operations personnel and systems programming personnel.*

13.2.1.7.22 z/OS UNIX Processes

The Process (PS) panel allows users to access information about z/OS UNIX processes such as parent process, state of the process, and time the process was started. Operations related to processes displayed on the PS panel can be protected.

The following table lists the SAF resource information relative to the protection of z/OS UNIX process resources:

Table B-41. SDSF Z/OS UNIX PROCESS SAF RESOURCES (13.2.1.7.22)

SDSF Z/OS UNIX PROCESS SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFPROC.*owner*.*jobname*	READ	Display information about a process
SDSF	ISFPROC.*owner*.*jobname*	ALTER	Cancel a process

In the table:
- *owner* is the owner of the z/OS UNIX process
- *jobname* is the name of the z/OS UNIX process

NOTE: SDSF z/OS UNIX process SAF resource protection only applies to z/OS V1R2 and above.

- *(ZISF0310: CAT II) The IAO will define SDSF z/OS U0NIX process SAF resources to the ACP with no user access by default.*

- *(ZISF0310: CAT II) The IAO will define a generic resource such as ISFPROC. to the ACP to provide the default protection.*

- *(ZISF0310: CAT II) The IAO will restrict all access to SDSF z/OS UNIX process resources to operations personnel and systems programming personnel.*

13.2.1.7.23 Spool Volumes

The Spool Volumes (SP) panel displays statistics about each JES2 spool volume. Operations related to spool volumes displayed on the SP panel can be protected.

The following table lists the SAF resource information relative to the protection of spool volume resources:

Table B-42. SDSF SPOOL VOLUME SAF RESOURCES (13.2.1.7.23)

SDSF SPOOL VOLUME SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFSP.*volser.jesx*	READ	Display information about a spool volume
SDSF	ISFSP.*volser.jesx*	CONTROL	All other commands such as drain, start, and halt a spool volume

In the table:
- *volser* is the serial number of the spool volume
- *jesx* is the name of the JES2 subsystem

NOTE: SDSF spool volume resource protection only applies to z/OS V1R2 and above.

- *(ZISF0320: CAT II) The IAO will define SDSF spool volume SAF resources to the ACP with no user access by default.*

- *(ZISF0320: CAT II) The IAO will define a generic resource such as ISFSP. to the ACP to provide the default protection.*

- *(ZISF0320: CAT II) The IAO will restrict all access to SDSF spool volume resources to operations personnel and systems programming personnel.*

13.2.1.7.24 Jobs, Output Groups, and SYSIN/SYSOUT Data Sets

JES2 uses the JES2 spool to store information about jobs being processed on the operating system. The data on the JES2 spool can be protected using the JESSPOOL resource class. JES2 uses the JESSPOOL resource class to protect SYSIN/SYSOUT data sets. SDSF extends the use of the JESSPOOL resource class to protect SDSF job and output group resources as well.

SDSF uses SAF authorization to check the following elements:

- Job resources on the Display Active Users, Input Queue, and Status panels
- Output groups on the Held Output Queue, Job Data Set, Output Queue, and Output Descriptors panels
- SYSIN/SYSOUT data sets on the Job Data Set panel and any other panel used for browsing with the S or V action characters and printing with the X action character

The following table lists the SAF resource information relative to the protection of JES2 job resources:

Table B-43. JES2 JOB SAF RESOURCES (13.2.1.7.24 a)

JES2 JOB SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
JESSPOOL	*nodeid.userid.jobname.jobid.JCL*	READ	Edit job JCL
JESSPOOL	*nodeid.userid.jobname.jobid*	READ	Display job information and output status
JESSPOOL	*nodeid.userid.jobname.jobid*	ALTER	Modify job status such as cancel, hold, and release

The following table lists the SAF resource information relative to the protection of JES2 output group resources:

Table B-44. JES2 OUTPUT GROUP SAF RESOURCES (13.2.1.7.24 b)

JES2 OUTPUT GROUP SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
JESSPOOL	*nodeid.userid.jobname.jobid.GROUP .ogroupid*	READ	List job output and status
JESSPOOL	*nodeid.userid.jobname.jobid.GROUP .ogroupid*	ALTER	Modify job output status such as purge, release, and hold

The following table lists the SAF resource information relative to the protection of JES2 SYSIN/SYSOUT resources:

Table B-45. JES SYSIN/SYSOUT DATA SET SAF RESOURCES (13.2.1.7.24 c)

JES2 SYSIN/SYSOUT DATA SET SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
JESSPOOL	*nodeid.userid.jobname.jobid.Ddsid.dsname*	READ	Browse and print SYSIN/SYSOUT data sets

In the previous tables:
- *nodeid* is the NJE node ID of the target JES2 subsystem
- *userid* is the local user ID of the job owner
- *jobname* is the name of the job
- *jobid* is the JES2 job ID of the:
  - job (for jobs on the DA, I, and ST panel)
  - job with which the output group is associated (for output groups on the H, O, JDS, and OD panels)
  - job with which the data set is associated (for SYSIN or SYSOUT data sets). This contains the type of object that the job is (TSU, JOB, or STC), as well as the job number.
- *ogroupid* is the output group name as specified through the GRPID=keyword on the MVS //OUTPUT statement describing the group.
- *Ddsid* is the data set ID number that identifies the job data set prefixed by the required letter D.
- *dsname* is the user-specified or system-assigned data set name.

By default, JESSPOOL resources are fully protected and require no addition controls to restrict data access to only the job owner. Users can always access the JESSPOOL resources they own and do not require additional authority to access their jobs and output. However, situations may exist where one user legitimately requires access to jobs that run under another user's userid. Protection for each type of resource can be defined separately. For example, a user may be authorized to issue action characters for a job, but not be authorized to browse that job's data sets. Refer to *Section 5.1.4, Security Controls for JES2 SPOOL Data Sets*, for more information on protecting JESSPOOL resources.

- *(ZJES0046: CAT II) The IAO will ensure that the following items are in effect regarding JES2 job, output group, and SYSIN/SYSOUT data set SAF resources defined to the JESSPOOL resource class:*

  - *Resources definitions will be fully qualified and not generic in nature.*
  - *Resources definitions will have no user access by default.*
  - *All access to resources will be logged using the ACP.*
  - *Access to resources will be granted to specific individuals and not at the group level.*

- *Justification documentation with IAO approval will be filed with the IAO.*

13.2.1.7.25 SDSF Server Operations

The SDSF Server provides the configuration and operational characteristics of SDSF. The following table lists the SAF resource information relative to the protection of SDSF server operations.

Table B-46. SDSF SERVER SAF RESOURCES (13.2.1.7.25)

SDSF SERVER SAF RESOURCES			
RESOURCE CLASS	*RESOURCE NAME*	*REQUIRED ACCESS*	*DESCRIPTION*
SDSF	ISFCMD.OPT.SERVER	READ	Use of the SERVER parameter on the SDSF command
SDSF	SERVER.NOPARM	READ	Reverting to ISFPARMS in assembler macro format
OPERCMDS	*server*.MODIFY.DISPLAY	READ	Use of the DISPLAY parameter on the MVS MODIFY command (F) for the SDSF server
OPERCMDS	*server*.MODIFY.*mod-parm*	CONTROL	Use of various parameters on the MVS MODIFY command for the SDSF server

In the table:
- *server* is the name of the SDSF server specified either by the ISFPMAC macro or SDSF command.
- *mod-parm* is one of the following parameters specified on the MVS MODIFY command: DEBUG, FOLDMSG, LOGCLASS, LOGTYPE, REFRESH, START, STOP, TRACE, and TRCLASS.
- The server START and STOP commands are protected by MVS. The resources are MVS.START.STC.*server* and MVS.STOP.STC.*server* respectively. They are defined to the OPERCMDS resource class and require update authority.

- *(ZISF0330: CAT II) The IAO will define the SDSF Server SAF resources to the ACP with no user access by default.*

The SERVER parameter of the SDSF command allows you to override the server specified in the ISFPMAC macro when invoking SDSF. Since the SDSF server provides the configuration and security for SDSF, the ability to override the default server value should be restricted.

- *(ZISF0330: CAT II) The IAO will restrict all access to the ISFCMD.OPT.SERVER resource to systems programming personnel.*

SDSF connects to the server during SDSF initialization and uses the server to process the ISFPARMS statements. However, if the SDSF server is not active or if no statements are in effect, SDSF reverts to the ISFPARMS defined with the assembler macros and initialization proceeds.

Under normal operations, SDSF users should not be allowed to use SDSF with the assembler macro format in use. SDSF configuration and security is not fully supported using ISFPARMS assembler macro definitions. The use of SDSF with ISFPARMS macro format will be used for recovery situations only.

- *(ZISF0330: CAT II) The IAO will restrict all access to the SERVER.NOPARM resource to systems programming personnel. In addition, access is granted to specific individuals in the systems programming staff responsible for system recovery. Access is not granted at the group level.*

- *(ZISF0330: CAT II) The IAO will log all access to the SERVER.NOPARM resource using the ACP.*

The SDSF server MODIFY command can be used to refresh the ISFPARMS statements, change server options, and control server communications within an SDSF server group.

- *(ZISF0340: CAT II) The IAO will restrict all update and control access to server.MODIFY.mod-parm resources to systems programming personnel.*

- *(ZISF0340: CAT II) The IAO will log all update and control access to server.MODIFY.mod-parm resources.*

13.2.1.7.26 MQSeries for OS/390

SDSF uses MQSeries for OS/390 (MQ) to provide sysplex support. The security controls related to SDSF's use of MQ consists of:

- Protecting the queues used by SDSF
- Permitting the SDSF server to define queues
- Defining connection and context security

Refer to *Section 4.3, MQSeries*, for more information on controlling access to MQSeries resources.

13.2.1.7.26.1 Queue Protection

SDSF uses several MQ queues to provide sysplex data on various SDSF panels. Security is defined by permitting or denying the SDSF server and the SDSF client access to the queues. The SDSF client can be thought of as the SDSF user. The queues include request queues that handle work communications between the client and the server, as well as model and command queues used to dynamically create queues as needed.

SDSF uses both a server and a client request queue. The client request queue is actually an alias for the server request queue. The two queues work together so that SDSF users can put requests on the server queue, but cannot read the server queue. The client request queue is defined by SDSF so users are allowed by SAF to read the client queue, but are prohibited by MQ. The SAF profiles should prevent access by the user to the server request queue, and allow access to the client request queue. The server must have access to both queues.

The following table lists the SAF resource information relative to the protection of MQSeries queues:

Table B-47. MQ QUEUE SAF RESOURCES (13.2.1.7.26.1)

MQ QUEUE SAF RESOURCES				
RESOURCE CLASS	*RESOURCE NAME*	*DESCRIPTION*	*REQ'D ACCESS*	
			SERVER	*CLIENT*
MQQUEUE	*ssid.prefix*.SERVER.*server.system*.REQUESTQ	Server request queue	ALTER	NONE
MQQUEUE	*ssid.prefix*.CLIENT.*server.system*.REQUESTQ	Client request queue (used to send work to the server)	ALTER	UPDATE (PUT only)
MQQUEUE	*ssid.prefix*.USER.*userid.**	ReplyTo queue (used by the client to receive server responses)	UPDATE	UPDATE
MQQUEUE	*ssid.prefix*.MODEL.**	Model queue (used to create dynamic queues	UPDATE	UPDATE
MQQUEUE	*ssid.XMIT.QUEUE*	Transmission queue (used to send messages to remote SDSF servers)	UPDATE	NONE

In the table:

- *ssid* is the MQ subsystem ID. This is the queue manager name specified on the COMM statement of ISFPARMS.
- *prefix* is a string that identifies the queue name. It is defined by the QPREFIX parameter of the COMM statement in ISFPARMS.
- *server* is the name of the SDSF server specified either by the ISFPMAC macro or SDSF command.
- *system* is the name of the MVS system (sysplex support).

NOTE: The ssid.prefix.MODEL.** and ssid.XMIT.QUEUE resources affect functions outside of SDSF.

- *(ZWMQ0054: CAT II) The IAO will ensure that all MQSeries/WebSphere MQ queues are restricted using queue level security.*

13.2.1.7.26.2 Queue Definition Authority

When the SDSF server initializes, it checks for the presence of the model queue and the client request queue. If these are not defined, the server attempts to create them using the MQ MQSC interface. The SDSF server should have access to these resources. In addition, you may want the operator ID used by MQ for commands entered from the console to have access to these resources.

The following table lists the SAF resource information relative to the protection of MQSeries queue definition authority:

Table B-48. MQ QUEUE DEFINITION AUTHORITY SAF RESOURCES (13.2.1.7.26.2)

MQ QUEUE DEFINITION AUTHORITY SAF RESOURCES				
RESOURCE CLASS	*RESOURCE NAME*	*DESCRIPTION*	*REQ'D ACCESS*	
			SERVER	*CLIENT*
MQCMDS	*ssid*.DEFINE.QMODEL	Define queues	ALTER	NONE
MQCMDS	*ssid*.DEFINE.QALIAS	Define a queue alias	ALTER	NONE
MQADMIN	*ssid*.QUEUE.*prefix*.MODEL. QUEUE	Define queues	ALTER	NONE
MQQUEUE	*ssid*.SYSTEM.COMMAND. REPLY.MODEL.	Model queue (used to create the temporary ReplyTo queue)	ALTER	NONE
MQQUEUE	*ssid*.SYSTEM.COMMAND.INPUT	Command input queue (used to submit DEFINE commands)	ALTER	NONE

In the table:

- *ssid* is the MQ subsystem ID. This is the queue manager name specified on the COMM statement of ISFPARMS.
- *prefix* is a string that identifies the queue name. It is defined by the QPREFIX parameter of the COMM statement in ISFPARMS.

NOTE: All the resources in this table affect functions outside of SDSF.

- *(ZWMQ0054: CAT II) The IAO will ensure that all MQSeries/WebSphere MQ queues are restricted using queue level security.*

- *(ZWMQ0059: CAT II) The IAO will ensure that all MQSeries/WebSphere MQ commands are restricted to authorized personnel.*

- *(ZISF0350: CAT II) The IAO will define MQ queue definition authority SAF resources to the ACP with no user access by default.*

- *(ZISF0350: CAT II) The IAO will restrict SDSF server and SDSF client access to MQ queue definition authority resources as indicated in the previous table.*

13.2.1.7.26.3 Connection Security

Connection security may be used to control which users can connect to MQ. When connection security is enabled, both the SDSF server and the SDSF client must have access to the local queue manager. These both use the batch/TSO adapter. This resource affects functions outside of SDSF.

The following table lists the SAF resource information relative to the protection of MQSeries connection security:

Table B-49. MQ QUEUE CONNECTION SECURITY SAF RESOURCE (13.2.1.7.26.3)

MQ QUEUE CONNECTION SECURITY SAF RESOURCE				
RESOURCE CLASS	*RESOURCE NAME*	*DESCRIPTION*	*REQ'D ACCESS*	
			SERVER	***CLIENT***
MQCONN	*ssid*.BATCH	Connection security	READ	READ

In the table:
- *ssid* is the MQ subsystem ID. This is the queue manager name specified on the COMM statement of ISFPARMS.

- *(ZWMQ0052: CAT II) The IAO will ensure that all connections to MQSeries/WebSphere MQ resources are restricted using connection security.*

13.2.1.7.26.4 Context Security

Context security is used to protect setting of the identity context fields in the message header. The server needs this authority; clients should not have this authority. MQ itself also needs to be given this authority. This resource affects functions outside of SDSF.

The following table lists the SAF resource information relative to the protection of MQSeries context security:

Table B-50. MQ CONTEXT SECURITY SAF RESOURCE (13.2.1.7.26.4)

MQ CONTEXT SECURITY SAF RESOURCE				
RESOURCE CLASS	***RESOURCE NAME***	***DESCRIPTION***	***REQ'D ACCESS***	
			SERVER	***CLIENT***
MQADMIN	*ssid*.CONTEXT	Context security	UPDATE	NONE

In the table:

- *ssid* is the MQ subsystem ID. This is the queue manager name specified on the COMM statement of ISFPARMS.

- *(ZWMQ0058: CAT II) The IAO will ensure that use of context resources are restricted to authorized personnel.*

13.2.2 ACF2

This section describes the commands and rules needed to implement the security requirements discussed throughout *Section 13.2, System Display and Search Facility*, in an ACF2 environment. The following task categories are described:

- Data set protection
- Started task definitions
- Resource controls

13.2.2.1 Data Set Controls

The following rule may be added to the SYS1 rule set to provide the required data set access controls documented in *Section 13.2.1.1, SDSF Data Set Protection*:

```
$KEY(SYS1)
ISF.- UID(sysprog-group) READ(A) WRITE(A) ALLOC(A) EXEC(A) -
    DATA(SDSF SMP/E INSTALLATION DATA SETS)
```

13.2.2.2 Started Task Definitions

The following commands may be used to define the required STC controls documented in *Section 3.2.2.3, Started Task Control (STC) Users*:

- *(ZISFA360: CAT II) The IAO will create an ACF logonid named SDSF, or in the case of multiple SDSF servers, prefixed with SDSF.*

```
SET LID
INSERT SDSF NAME(SDSF SERVER) STC
```

13.2.2.3 Resource Controls

This section describes the commands and rules needed to implement the required controls for SDSF resources and functions discussed in *Section 13.2.1.7, SDSF Resource Protection*.

By default, ACF2 ignores SAF calls for SDSF, WRITER, JESSPOOL, and OPERCMDS resources. ACF2 internal SAFDEF records for these resource classes are coded with MODE(IGNORE). To enable ACF2 protection for these resources classes, locally defined SAFDEF records must be inserted into the ACF2 database. The following commands may be used to enable SAF security for these resources:

```
SET CONTROL(GSO)
    INSERT SAFDEF.SDSF ID(SDSF) MODE(GLOBAL) -
RACROUTE(REQUEST=AUTH, CLASS=SDSF) REP
    INSERT SAFDEF.WRITER ID(WRITER) MODE(GLOBAL) -
RACROUTE(REQUEST=AUTH, CLASS=WRITER) REP
    INSERT SAFDEF.JESSPL ID(JESSPL) MODE(GLOBAL) -
RACROUTE(REQUEST=AUTH, CLASS=JESSPOOL) REP
    INSERT SAFDEF.OPRCMDS ID(OPRCMDS) MODE(GLOBAL) -
        RACROUTE(REQUEST=AUTH, CLASS=OPERCMDS) REP
```

IMPORTANT NOTE: After these SAFDEF records are created and the ACF2 GSO options are refreshed, validation for these resources is active. Therefore ensure that all of the necessary rules are defined before activating these local SAF definitions.

ACF2 uses the resource type SAF for the SDSF, WRITER, JESSPOOL, and OPERCMDS resource classes by default.

The following commands may be used to map SAF resource classes to the STIG resource types:

```
SET CONTROL(GSO)
INSERT CLASMAP.SDSF RESOURCE(SDSF) RSRCTYPE(SDF) ENTITYLN(63)
INSERT CLASMAP.WRITER RESOURCE(WRITER) RSRCTYPE(WTR) -
    ENTITYLN(39)
INSERT CLASMAP.JESSPL RESOURCE(JESSPOOL) RSRCTYPE(SPL) -
    ENTITYLN(53)
INSERT CLASMAP.OPRCMDS RESOURCE(OPERCMDS) RSRCTYPE(OPR) -
    ENTITYLN(39)
```

13.2.2.3.1 SDSF Group Membership Controls

The following rules may be used to control access to SDSF groups as discussed in *Section 13.2.1.7.1, Membership in SDSF Groups*. This example establishes default protection, defines an SDSF group named sysprog that is configured in ISFPARMS for an SDSF server named sdsf, and allows access to a UID for systems programming personnel.

```
$KEY(GROUP) TYPE(SDF)
- UID(-) PREVENT DATA(SDSF GROUP DEFAULT PROTECTION)
sysprog.sdsfUID(sysprog-group) SERVICE(READ) ALLOW -
    DATA(SDSF GROUP FOR SYSTEMS PROGRAMMERS)
```

13.2.2.3.2 SDSF Resources Controls

This section shows examples of security controls as discussed in the following general sections:

Section 13.2.1.7.2, SDSF Panels
Section 13.2.1.7.3, SDSF Maintenance Commands
Section 13.2.1.7.4, SDSF Filtering Commands
Section 13.2.1.7.5, SDSF / Command
Section 13.2.1.7.7, Overtypeable Fields
Section 13.2.1.7.9, Destination Names
Section 13.2.1.7.10, Destination Operator Authority
Section 13.2.1.7.11, Initiators
Section 13.2.1.7.13, Lines
Section 13.2.1.7.14, Nodes
Section 13.2.1.7.15, Offloaders
Section 13.2.1.7.16, MAS Members
Section 13.2.1.7.17, Job Classes
Section 13.2.1.7.18, Scheduling Environments
Section 13.2.1.7.19, WLM Resources
Section 13.2.1.7.20, System Requests
Section 13.2.1.7.21, WLM Enclaves
Section 13.2.1.7.22, z/OS UNIX Processes
Section 13.2.1.7.23, Spool Volumes

The following rules may be used to establish default protection and permit access to SDSF resources that are restricted to both operations personnel and systems programming personnel:

```
$KEY(ISF-) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO ALL SDSF RESOURCES)

$KEY(ISFCMD) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO ALL SDSF COMMAND -
    RESOURCES)
DSP.- UID(sysprog-group, oper-group) SERVICE(READ) ALLOW -
    DATA(SDSF END USER DISPLAYS)
```

ODSP.- UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
DATA(SDSF OPERATOR DISPLAYS)
FILTER.- UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
DATA(SDSF FILTERING COMMANDS)

$KEY(ISFOPER) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO SDSF OPERATOR -
RESOURCES)
SYSTEM UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
DATA(SDSF / COMMAND)
ANYDEST.JES* UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
DATA(SDSF AUTHORITY TO ANY DESTINATION PRIMER)
DEST.JES* UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
DATA(SDSF DESTINATION OPERATOR AUTHORITY)

$KEY(ISFATTR) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO ALL SDSF OVERTYPEABLE -
FIELDS)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE) ALLOW -
DATA(ALL SDSF OVERTYPEABLE FIELDS)

$KEY(ISFAUTH) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO SDSF DESTINATION -
AUTHORITY RESOURCES)
DEST.******** UID(*sysprog-group, oper-group*) -
SERVICE(READ,UPDATE,ADD,DELETE) ALLOW -
DATA(SDSF DESTINATION AUTHORITY TO JOBS)
DEST.********.******** UID(sysprog-group, oper-group) -
SERVICE(READ,UPDATE,ADD,DELETE) ALLOW -
DATA(SDSF DESTINATION AUTHORITY TO JOB OUTPUT)
DEST.-.DATASET.- UID(-) PREVENT DATA(SDSF DESTINATION -
AUTHORITY TO STANDARD SYSIN/SYSOUT DATA SETS)
DEST.-DATASET.JES***** UID(*sysprog-group, oper-group*) SERVICE(READ) -
ALLOW DATA(SDSF DESTINATION AUTHORITY TO SYSTEM MESSAGE -
SYSIN/SYSOUT DATA SETS)

$KEY(ISFINIT) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 INITIATORS)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
ALLOW DATA(JES2 INITIATORS)

$KEY(ISFLINE) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 COMMUNICATION -
LINES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
ALLOW DATA(JES2 COMMUNICATION LINES)

$KEY(ISFNODE) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 NODES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(JES2 NODES)

$KEY(ISFSO) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 SPOOL OFFLOADERS)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(JES2 SPOOL OFFLOADERS)

$KEY(ISFMEMB) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 MAS MEMBERS)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(JES2 MAS MEMBERS)

$KEY(ISFJOBCL) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 JOB CLASSES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(JES2 JOB CLASSES)

$KEY(ISFSE) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO WLM SCHEDULING -
  ENVIRONMENTS)
- UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
  DATA(WLM SCHEDULING ENVIRONMENTS)

$KEY(ISFRES) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO WLM RESOURCES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(WLM RESOURCES)

$KEY(ISFSR) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO SYSTEM REQUESTS)
- UID(*sysprog-group, oper-group*) SERVICE(READ) ALLOW -
  DATA(SYSTEM REQUESTS)

$KEY(ISFENC) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO WLM ENCLAVES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(WLM ENCLAVES)

$KEY(ISFPROC) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO Z/OS UNIX PROCESSES)
- UID(*sysprog-group, oper-group*) SERVICE(READ,UPDATE,ADD,DELETE) -
  ALLOW DATA(Z/OS UNIX PROCESSES)

```
$KEY(ISFSP) TYPE(SDF)
- UID(-) PREVENT DATA(DEFAULT ACCESS TO JES2 SPOOL VOLUMES)
- UID(sysprog-group, oper-group) SERVICE(READ,UPDATE,ADD,DELETE) -
    ALLOW DATA(JES2 SPOOL VOLUMES)
```

The following rules may be used to allow access to SDSF resources that are restricted to systems programming personnel only:

```
$KEY(ISFCMD) TYPE(SDF)
MAINT.- UID(sysprog-group) SERVICE(READ) ALLOW -
    DATA(SDSF MAINTENANCE COMMANDS)
FILTER.INPUT UID(oper-group) PREVENT -
    DATA(SDSF INPUT FILTER COMMAND FOR SYS PROGS ONLY)
```

NOTE: The FILTER.INPUT rule removes oper-group access based on the previous example showing permits of SDSF resources that are restricted to both operations personnel and systems programming personnel.

The following rules may be used to allow access to SDSF resources that are permitted to authorized SDSF end-users:

```
$KEY(ISFCMD) TYPE(SDF)
DSP.- UID(end-user-group) SERVICE(READ) ALLOW -
    DATA(SDSF END USER DISPLAYS)

$KEY(ISFATTR) TYPE(SDF)
OUTPUT.BURST UID(end-user-group) SERVICE(UPDATE) ALLOW -
   DATA(SDSF H AND O PANEL BURST INDICATION FIELD)
OUTPUT.CLASS UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL JES2 OUTPUT CLASS FIELD)
OUTPUT.DEST UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL JES2 PRINT DESTINATION NAME FIELD)
OUTPUT.FCB UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL FCB ID FIELD)
OUTPUT.FLASH UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL FLASH ID FIELD)
OUTPUT.FORMS UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL FORM NUMBER FIELD)
OUTPUT.PRMODE UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL PRINTER PROCESS MODE FIELD)
OUTPUT.UCS UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL UCS ID FIELD)
OUTPUT.WRITER UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF H AND O PANEL EXTERNAL WRITER NAME FIELD)
OUTDESC.- UID(end-user-group) SERVICE(UPDATE) ALLOW -
```

```
    DATA(SDSF JDS AND OD PANEL OUTPUT DESCRIPTOR FIELDS)
JOB.PRTDEST UID(end-user-group) SERVICE(UPDATE) ALLOW -
    DATA(SDSF ST AND I PANEL JES2 PRINT DESTINATION NAME FIELD)

$KEY(ISFOPER) TYPE(SDF)
ANYDEST.JES* UID(end-user-group) SERVICE(READ) ALLOW -
    DATA(SDSF AUTHORITY TO ANY DESTINATION PRIMER)

$KEY(ISFSE) TYPE(SDF)
- UID(end-user-group) SERVICE(READ) ALLOW -
    DATA(WLM SCHEDULING ENVIRONMENTS)
```

13.2.2.3.3 MVS and JES2 Command Controls

Refer to *Section 3.2.5.6, OS/390 System Command Controls*, and *Section 5.2.5, Security Controls for JES2 Commands*, for general ACF2 controls regarding MVS and JES2 system command resources respectively. The following rules may be used to define MVS and JES2 command resources that are permitted to all SDSF users, including end-users, as discussed in *Section 13.2.1.7.8, MVS and JES2 Commands Generated by SDSF*:

```
$KEY(MVS) TYPE(OPR)
DISPLAY.- UID(sysprog-group, oper-group, end-user-group) SERVICE(READ) -
    ALLOW DATA(VARIOUS MVS DISPLAY COMMANDS)
CANCEL.ATX.- UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(CANCEL APPC TRANSACTION -
        PROGRAMS)
CANCEL.TSU.- UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(CANCEL TSO USER SESSIONS)

$KEY(JES2) TYPE(OPR)
DISPLAY.- UID(sysprog-group, oper-group, end-user-group) SERVICE(READ) -
    ALLOW DATA(VARIOUS JES DISPLAY COMMANDS)
MSEND.CMD UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(READ) LOG DATA(SEND MESSAGES)
MODIFY.BATOUT UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(MODIFY OUTPUT FILE STATUS FOR -
        BATCH JOBS)
MODIFY.TSUOUT UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(MODIFY OUTPUT FILE STATUS FOR -
        TSO JOBS)
MODIFY.STCOUT UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(MODIFY OUTPUT FILE STATUS FOR -
        STC JOBS)
CANCEL.BAT UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(CANCEL / PURGE BATCH JOBS)
CANCEL.TSU UID(sysprog-group, oper-group, end-user-group) -
    SERVICE(UPDATE) LOG DATA(CANCEL / PURGE TSO JOBS)
```

CANCEL.STC UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(CANCEL / PURGE STC JOBS)
CANCEL.DEV UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(CANCEL / PURGE BATCH JOBS ON JES2 -
DEVICES)
RELEASE.BATOUT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(RELEASE OUTPUT FILES FOR BATCH -
JOBS)
RELEASE.TSUOUT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(RELEASE OUTPUT FILES FOR TSO -
JOBS)
RELEASE.STCOUT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(RELEASE OUTPUT FILES FOR STC -
JOBS)
RESTART.DEV UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(RESTART JES2 DEVICES)
RESTART.BAT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE,DELETE) LOG DATA(RESTART BATCH JOBS)
MODIFYHOLD.BAT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(HOLD BATCH JOBS)
MODIFYHOLD.TSU UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(HOLD TSO JOBS)
MODIFYHOLD.STC UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(HOLD STC JOBS)
ROUTE.JOBOUT UID(*sysprog-group, oper-group, end-user-group*) -
SERVICE(UPDATE) LOG DATA(ROUTE JOB OUTPUT)

13.2.2.3.4 Printer and Punch Controls

Refer to *Section 5.2.3, Security Controls for Output*, for general controls regarding printer and punch resources in an ACF2 environment. The following rules may be used to control access to JES2 printer and punch resources defined to the WRITER resource class as discussed in *Section 13.2.1.7.12, Printers and Punches*:

$KEY(JES2) TYPE(WTR)
LOCAL.*device-name* UID(*sysprog-group, oper-group*) -
SERVICE(READ,UPDATE,ADD,DELETE) ALLOW -
DATA(JES2 LOCAL PRINTER / PUNCH)
RJE.*device-name* UID(*sysprog-group, oper-group*) -
SERVICE(READ,UPDATE,ADD,DELETE) ALLOW -
DATA(JES2 REMOTE PRINTER / PUNCH)

13.2.2.3.5 Jobs, Output Group, SYSIN/SYSOUT Controls

Refer to *Section 5.2.4, Security Controls for JES2 SPOOL Data Sets*, for general controls regarding JES2 spool resources in an ACF2 environment. The following rules may be used to control access to JES2 job and output group resources defined to the JESSPOOL resource class as discussed in *Section 13.2.1.7.24, Jobs, Output Group, and SYSIN/SYSOUT Data Sets*:

```
$KEY(nodeid) TYPE(SPL)
 logonid.jobname.jobid.JCL UID(logonid) SERVICE(READ) LOG -
    DATA(VIEW AND EDIT JOB JCL)
 logonid.jobname.jobid UID(logonid) SERVICE(READ) LOG -
    DATA(VIEW JOB STATUS)
 logonid.jobname.jobid UID(logonid) SERVICE(READ,UPDATE,ADD,DELETE) -
    LOG DATA(MODIFY JOB STATUS)
 logonid.jobname.jobid.GROUP.ogroupid UID(logonid) SERVICE(READ) LOG -
   DATA(VIEW JOB OUTPUT STATUS)
 logonid.jobname.jobid.GROUP.ogroupid UID(logonid) -
    SERVICE(READ,UPDATE,ADD,DELETE) LOG -
       DATA(MODIFY JOB OUTPUT STATUS)
```

13.2.2.3.6 SDSF Server Controls

The following rules may be used to control access to resources specific to the control of the SDSF Server as discussed in *Section 13.2.1.7.25, SDSF Server Operations*:

```
$KEY(ISFCMD) TYPE(SDF)
OPT.SERVER UID(sysprog-group) SERVICE(READ) ALLOW -
    DATA(USE OF THE SERVER PARAMETER ON THE SDSF COMMAND)

$KEY(SERVER) TYPE(SDF)
NOPARM UID(sysprog-logonid) SERVICE(READ) LOG -
    DATA(REVERT TO ISFPARMS IN ASSEMBLER MACRO FORMAT)

$KEY(server) TYPE(OPR)
MODIFY.DISPLAY UID(sysprog-group, oper-group) SERVICE(READ) ALLOW -
    DATA(USE OF DISPLAY PARAMETER ON MVS MODIFY COMMAND (F) -
       FOR THE SDSF SERVER)

$KEY(server) TYPE(OPR)
MODIFY.- UID(sysprog-group, oper-group) SERVICE(DELETE) -
    LOG DATA(USE OF VARIOUS MODIFY PARAMETERS ON MVS MODIFY -
       COMMAND (F) FOR THE SDSF SERVER)
```

13.2.2.3.7 MQ Controls

13.2.2.3.7.1 MQ Queue Protection

Refer to *Section 4.3.2.2.4, Queue Security*, for general controls regarding MQ queue resources in an ACF2 environment. The following rules may be used to control access to MQ queue resources defined to the MQQUEUE resource class as discussed in *Section 13.2.1.7.26.1, Queue Protection*:

```
$KEY(ssid) TYPE(MQQ)
prefix.SERVER.- UID(SDSF-server-logonid, MQ-logonid) -
    SERVICE(READ,UPDATE,ADD) ALLOW DATA(SDSF SERVER -
        REQUEST QUEUE)
prefix.CLIENT.- UID(SDSF-server-logonid) SERVICE(READ,UPDATE,ADD) -
    ALLOW DATA(SDSF CLIENT REQUEST QUEUE TO SEND WORK TO -
        SERVER)
prefix.CLIENT.- UID(sysprog-group, oper-group, end-user-group) -
   SERVICE(READ,UPDATE) ALLOW DATA(SDSF CLIENT REQUEST -
        QUEUE TO SEND WORK TO SERVER)
prefix.USER.- UID(SDSF-server-logonid, oper-group, sysprog-group, end-user-group) -
    SERVICE(READ,UPDATE) ALLOW DATA(SDSF REPLYTO QUEUE TO -
        RECEIVE SERVER MESSAGES)
prefix.MODEL.- UID(SDSF-server-logonid, oper-group, sysprog-group, -
    end-user-group) SERVICE(READ,UPDATE) ALLOW -
        DATA(SDSF MODEL QUEUE TO CREATE DYNAMIC QUEUES)
XMIT.QUEUE UID(SDSF-server-logonid) SERVICE(READ,UPDATE) ALLOW -
    DATA(TRANSMISSION QUEUE TO SEND MESSAGES TO REMOTE SDSF-
        SERVERS)
```

In the previous example, *MQ-logonid* is the logonid associated with the MQ started task.

IMPORTANT NOTE: Standard ACF2 controls do not provide a practical solution for securing individual ReplyTo queues to specific users. The fourth node of the resource that protects access to the ReplyTo queue is the user's logonid (i.e., *ssid.prefix.USER.logonid*.-). Using standard ACF2 controls, rules would have to be defined using specific logonids and specific UIDs to restrict each user's access to only their ReplyTo queue. Depending on the environment, this may require hundreds of unique resource rules defined. The use of logonid-specific rules to protect access to individual ReplyTo queues may be implemented at the site's discretion.

ACF2 provides an alternative to defining logonid-specific rules for ReplyTo queue protection. The ACF2 resource pre-validation exit, RSCXIT1, or ACF2 resource post-validation exit, RSCXIT2, may be used to restrict individual access to user ReplyTo queues instead of defining logonid-specific rules. Implementation of these ACF2 exits is subject to the requirements for exits as specified in *Section 2.1.2.7, Access Control Product Exits*.

13.2.2.3.7.2 MQ Queue Definition Authority Protection

Refer to *Section 4.3.2.2.4, Queue Security*, and *Section 4.3.2.2.9, Command Security,* for general controls regarding MQ queue and command resources in an ACF2 environment. The following rules may be used to control access to MQ queue definition authority resources as discussed in *Section 13.2.1.7.26.2, Queue Definition Authority*:

```
$KEY(ssid) TYPE(MQC)
DEFINE.QMODEL UID(SDSF-server-logonid, CSQ-oper-logonid) -
    SERVICE(READ,UPDATE,ADD) LOG DATA(DEFINE QUEUE COMMAND)
DEFINE.QALIAS UID(SDSF-server-logonid, CSQ-oper-logonid) -
    SERVICE(READ,UPDATE,ADD) LOG DATA(DEFINE QUEUE ALIAS -
        COMMAND)

$KEY(ssid) TYPE(MQA)
QUEUE.prefix.- UID(SDSF-server-logonid) SERVICE(READ,UPDATE,ADD) -
    ALLOW DATA(ADMIN AUTHORITY TO DEFINE QUEUES)

$KEY(ssid) TYPE(MQQ)
SYSTEM.- UID(SDSF-server-logonid) SERVICE(READ,UPDATE,ADD) -
    ALLOW DATA(ACCESS SYSTEM QUEUES)
```

In the previous example, *CSQ-oper-logonid* is the operator logonid used by MQ for commands entered from the console.

13.2.2.3.7.3 Connection Security Protection

Refer to *Section 4.3.2.2.3, Connection Security*, general controls regarding connection security in an ACF2 environment. The following rules may be used to control connect access to MQ as discussed in *Section 13.2.1.7.26.3, Connection Security*:

```
$KEY(ssid) TYPE(MQK)
BATCH UID(SDSF-server-logonid, oper-group, sysprog-group, end-user-group) -
    SERVICE(READ) LOG DATA(ALLOW CONNECTION FOR BATCH -
        AND TSO USERS)
```

13.2.2.3.7.4 Context Security Protection

Refer to *Section 4.3.2.2.8, Context Security*, general controls regarding context security in an ACF2 environment. The following rules may be used to control access to identity data in a message as discussed in *Section 13.2.1.7.26.4, Context Security*:

```
$KEY(ssid) TYPE(MQA)
CONTEXT UID(SDSF-server-logonid) SERVICE(READ,UPDATE) ALLOW -
    DATA(SETTING THE IDENTITY CONTEXT FIELDS IN THE -
        MESSAGE HEADER)
CONTEXT UID(MQ-logonid) SERVICE(READ,UPDATE,ADD) ALLOW -
    DATA(SETTING THE IDENTITY CONTEXT FIELDS IN THE -
        MESSAGE HEADER)
```

In the previous example, *MQ-logonid* is the logonid associated with the MQ started task.

13.2.3 RACF

This section describes the commands needed to implement the security requirements discussed throughout *Section 13.2, System Display and Search Facility,* in a RACF environment. The following task categories are described:

- Data set protection
- Started task definitions
- Resource controls

13.2.3.1 Data Set Controls

The following commands may be used to provide the required data set access controls documented in *Section 13.2.1.1, SDSF Data Set Protection*:

```
ADDSD 'SYS1.ISF.**' UACC(NONE) OWNER(SYS1)  -
    DATA('SDSF SMP/E INSTALLATION DATA SETS')

PERMIT 'SYS1.ISF.**' ID(sysprog-group) ACCESS(ALTER)
```

13.2.3.2 Started Task Definitions

The following commands may be used to define the required STC controls documented in *Section 3.3.2.3, Started Task Control (STC) Users*:

- *(ZISFR360: CAT II) The IAO will create a RACF userid named SDSF, or in the case of multiple SDSF servers, prefixed with SDSF.*

```
ADDUSER SDSF NAME('STC, SDSF') NOPASSWORD NOOIDCARD -
    DFLTGRP(stc-group) OWNER(admin) DATA('SDSF SERVER')
```

RDEFINE STARTED SDSF*.* STDATA(USER(=MEMBER) GROUP(*stc-group*) -
TRUSTED(NO)) UACC(NONE) OWNER(*admin*) DATA('SDSF SERVER')

13.2.3.3 Resource Controls

This section describes the commands needed to implement the required controls for SDSF resources and functions discussed in *Section 13.2.1.7, SDSF Resource Protection*.

Activate generic processing prior to defining generic profiles to ensure that profiles are recognized as generic and not discrete. The following commands may be used to activate generic processing for the resource classes used to protect the SDSF environment:

SETROPTS GENERIC(SDSF WRITER JESSPOOL OPERCMDS)
SETROPTS GENCMD(SDSF WRITER JESSPOOL OPERCMDS)

After all the necessary resource profiles are defined, activate the resource classes to enable SAF protection. The following commands may be used to activate the resource classes used to protect the SDSF environment:

SETROPTS CLASSACT(SDSF WRITER JESSPOOL OPERCMDS)
SETROPTS RACLIST(OPERCMDS) REFRESH

NOTE: The OPERCMDS resource class is required to be RACLISTed. The other resource classes may be RACLISTed at the site's discretion.

13.2.3.3.1 SDSF Group Membership Controls

The following commands may be used to control access to SDSF groups as discussed in *Section 13.2.1.7.1, Membership in SDSF Groups*. This example establishes default protection and defines an SDSF group named *sysprog* that is configured in ISFPARMS for an SDSF server named sdsf.

RDEFINE SDSF GROUP.** UACC(NONE) OWNER(*admin*) -
DATA('SDSF GROUP DEFAULT PROTECTION')
RDEFINE SDSF GROUP.*sysprog.sdsf*UACC(NONE) OWNER(*admin*) -
DATA('SDSF GROUP FOR SYSTEMS PROGRAMMERS')

The following command may be used to permit access to the SDSF sysprog group to systems programming personnel:

PERMIT GROUP.*sysprog.sdsf*CLASS(SDSF) ID(*sysprog-group*) ACCESS(READ)

13.2.3.3.2 SDSF Resources Controls

This section shows examples of security controls as discussed in the following general sections:

Section 13.2.1.7.2, SDSF Panels
Section 13.2.1.7.3, SDSF Maintenance Commands
Section 13.2.1.7.4, SDSF Filtering Commands
Section 13.2.1.7.5, SDSF / Command
Section 13.2.1.7.7, Overtypeable Fields
Section 13.2.1.7.9, Destination Names
Section 13.2.1.7.10, Destination Operator Authority
Section 13.2.1.7.11, Initiators
Section 13.2.1.7.13, Lines
Section 13.2.1.7.14, Nodes
Section 13.2.1.7.15, Offloaders
Section 13.2.1.7.16, MAS Members
Section 13.2.1.7.17, Job Classes
Section 13.2.1.7.18, Scheduling Environments
Section 13.2.1.7.19, WLM Resources
Section 13.2.1.7.20, System Requests
Section 13.2.1.7.21, WLM Enclaves
Section 13.2.1.7.22, z/OS UNIX Processes
Section 13.2.1.7.23, Spool Volumes

The following commands may be used to establish default protection for resources defined to the SDSF resource class:

```
RDEFINE SDSF ISF*.** UACC(NONE) OWNER(admin) -
    DATA('DEFAULT ACCESS TO ALL SDSF RESOURCES')
RDEFINE SDSF ISFCMD.DSP.** UACC(NONE) OWNER(admin) -
    DATA('SDSF END USER DISPLAYS')
RDEFINE SDSF ISFCMD.ODSP.** UACC(NONE) OWNER(admin) -
    DATA('SDSF OPERATOR DISPLAYS')
RDEFINE SDSF ISFCMD.MAINT.** UACC(NONE) OWNER(admin) -
    DATA('SDSF MAINTENANCE COMMANDS')
RDEFINE SDSF ISFCMD.FILTER.** UACC(NONE) OWNER(admin) -
    DATA('SDSF FILTERING COMMANDS')
RDEFINE SDSF ISFCMD.FILTER.INPUT UACC(NONE) OWNER(admin) -
    DATA('SDSF INPUT FILTER COMMAND')
RDEFINE SDSF ISFOPER.SYSTEM UACC(NONE) OWNER(admin) -
    DATA('SDSF / COMMAND')
RDEFINE SDSF ISFATTR.** UACC(NONE) OWNER(admin) -
    DATA('ALL SDSF OVERTYPEABLE FIELDS')
RDEFINE SDSF ISFATTR.OUTPUT.BURST UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL BURST INDICATION FIELD')
```

```
RDEFINE SDSF ISFATTR.OUTPUT.CLASS UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL JES2 OUTPUT CLASS FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.DEST UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL JES2 PRINT DESTINATION NAME FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.FCB UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL FCB ID FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.FLASH UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL FLASH ID FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.FORMS UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL FORM NUMBER FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.PRMODE UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL PRINTER PROCESS MODE FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.UCS UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL UCS ID FIELD')
RDEFINE SDSF ISFATTR.OUTPUT.WRITER UACC(NONE) OWNER(admin) -
    DATA('SDSF H AND O PANEL EXTERNAL WRITER NAME FIELD')
RDEFINE SDSF ISFATTR.OUTDESC.** UACC(NONE) OWNER(admin) -
    DATA('SDSF JDS AND OD PANEL OUTPUT DESCRIPTOR FIELDS')
RDEFINE SDSF ISFATTR.JOB.PRTDEST UACC(NONE) OWNER(admin) -
    DATA('SDSF ST AND I PANEL JES2 PRINT DESTINATION NAME FIELD')
RDEFINE SDSF ISFOPER.ANYDEST.JES% UACC(NONE) OWNER(admin) -
    DATA('SDSF AUTHORITY TO ANY DESTINATION PRIMER')
RDEFINE SDSF ISFAUTH.DEST.* UACC(NONE) OWNER(admin) -
    DATA('SDSF DESTINATION AUTHORITY TO JOBS')
RDEFINE SDSF ISFAUTH.DEST.*.* UACC(NONE) OWNER(admin) -
    DATA('SDSF DESTINATION AUTHORITY TO JOB OUTPUT')
RDEFINE SDSF ISFOPER.DEST.JES% UACC(NONE) OWNER(admin) -
    DATA('SDSF DESTINATION OPERATOR AUTHORITY')
RDEFINE SDSF ISFAUTH.DEST.**.DATASET.** UACC(NONE) -
    OWNER(admin) DATA('SDSF DESTINATION AUTHORITY TO -
        STANDARD SYSIN/SYSOUT DATA SETS')
RDEFINE SDSF ISFAUTH.DEST.**.DATASET.JES* UACC(NONE) -
    OWNER(admin) DATA('SDSF DESTINATION AUTHORITY TO -
        SYSTEM MESSAGE SYSIN/SYSOUT DATA SET')
RDEFINE SDSF ISFINIT.** UACC(NONE) OWNER(admin) -
    DATA('JES2 INITIATORS')
RDEFINE SDSF ISFLINE.** UACC(NONE) OWNER(admin) -
    DATA('JES2 COMMUNICATION LINES')
RDEFINE SDSF ISFNODE.** UACC(NONE) OWNER(admin) -
    DATA('JES2 NODES')
RDEFINE SDSF ISFSO.** UACC(NONE) OWNER(admin) -
    DATA('JES2 SPOOL OFFLOADERS')
RDEFINE SDSF ISFMEMB.** UACC(NONE) OWNER(admin) -
    DATA('JES2 MAS MEMBERS')
RDEFINE SDSF ISFJOBCL.** UACC(NONE) OWNER(admin) -
    DATA('JES2 JOB CLASSES')
```

RDEFINE SDSF ISFSE.** UACC(NONE) OWNER(*admin*) -
DATA('WLM SCHEDULING ENVIRONMENTS')
RDEFINE SDSF ISFRES.** UACC(NONE) OWNER(*admin*) -
DATA('WLM RESOURCES')
RDEFINE SDSF ISFSR.** UACC(NONE) OWNER(*admin*) -
DATA('SYSTEM REQUESTS')
RDEFINE SDSF ISFENC.** UACC(NONE) OWNER(*admin*) -
DATA('WLM ENCLAVES')
RDEFINE SDSF ISFPROC.** UACC(NONE) OWNER(*admin*) -
DATA('Z/OS UNIX PROCESSES')
RDEFINE SDSF ISFSP.** UACC(NONE) OWNER(*admin*) -
DATA('JES2 SPOOL VOLUMES')

The following commands may be used to permit access to SDSF resources that are restricted to both operations personnel and systems programming personnel:

PERMIT ISFCMD.DSP.** CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(READ)
PERMIT ISFCMD.ODSP.** CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(READ)
PERMIT ISFCMD.FILTER.** CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(READ)
PERMIT ISFOPER.SYSTEM CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(READ)
PERMIT ISFATTR.** CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.BURST CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.CLASS CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.DEST CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FCB CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FLASH CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FORMS CLASS(SDSF) ID(*sysprog-group oper-group* -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.PRMODE CLASS(SDSF) ID(*sysprog-group*
oper-group) – ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.UCS CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.WRITER CLASS(SDSF) ID(*sysprog-group* -
oper-group) - ACCESS(UPDATE)
PERMIT ISFATTR.OUTDESC.** CLASS(SDSF) ID(*sysprog-group oper-group*) -
ACCESS(UPDATE)

PERMIT ISFATTR.JOB.PRTDEST CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(UPDATE)
PERMIT ISFOPER.ANYDEST.JES% CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(READ)
PERMIT ISFAUTH.DEST.* CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFAUTH.DEST.*.* CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFOPER.DEST.JES% CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(READ)
PERMIT ISFAUTH.DEST.**.DATASET.JES* CLASS(SDSF) ID(*sysprog-group - oper-group*) - ACCESS(READ)
PERMIT ISFINIT.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFLINE.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFNODE.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFSO.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFMEMB.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFJOBCL.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFSE.** CLASS(SDSF) ID(*sysprog-group oper-group*) ACCESS(READ)
PERMIT ISFRES.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFSR.** CLASS(SDSF) ID(*sysprog-group oper-group*) ACCESS(READ)
PERMIT ISFENC.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFPROC.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)
PERMIT ISFSP.** CLASS(SDSF) ID(*sysprog-group oper-group*) - ACCESS(ALTER)

The following commands may be used to permit access to SDSF resources that are restricted to systems programming personnel only:

PERMIT ISFCMD.MAINT.** CLASS(SDSF) ID(*sysprog-group*) – ACCESS(READ)
PERMIT ISFCMD.FILTER.INPUT CLASS(SDSF) ID(*sysprog-group*) – ACCESS(READ)

The following commands may be used to permit access to SDSF resources that are permitted to authorized SDSF end-users:

```
PERMIT ISFCMD.DSP.** CLASS(SDSF) ID(end-user-group) –
    ACCESS(READ)
PERMIT ISFATTR.OUTPUT.BURST CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.CLASS CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.DEST CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FCB CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FLASH CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.FORMS CLASS(SDSF) ID(end-user-group) –
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.PRMODE CLASS(SDSF) ID(end-user-group) –
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.UCS CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTPUT.WRITER CLASS(SDSF) ID(end-user-group) –
    ACCESS(UPDATE)
PERMIT ISFATTR.OUTDESC.** CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFATTR.JOB.PRTDEST CLASS(SDSF) ID(end-user-group) -
    ACCESS(UPDATE)
PERMIT ISFOPER.ANYDEST.JES% CLASS(SDSF) ID(end-user-group) -
    ACCESS(READ)
PERMIT ISFSE.** CLASS(SDSF) ID(end-user-group)
    ACCESS(READ)
```

13.2.3.3.3 MVS and JES2 Command Controls

Refer to *Section 3.3.5.6, OS/390 System Command Controls*, and *Section 5.3.5, Security Controls for JES2 Commands*, for general RACF controls regarding MVS and JES2 system command resources respectively. The following commands may be used to define MVS and JES2 command resources that are permitted to all SDSF users, including end-users, as discussed in *Section 13.2.1.7.8, MVS and JES2 Commands Generated by SDSF*:

```
RDEFINE OPERCMDS MVS.DISPLAY.** UACC(NONE) OWNER(admin) -
    DATA('VARIOUS MVS DISPLAY COMMANDS')
RDEFINE OPERCMDS MVS.CANCEL.ATX.* UACC(NONE) OWNER(admin) -
    DATA('CANCEL APPC TRANSACTION PROGRAMS') -
        AUDIT(ALL(UPDATE))
```

RDEFINE OPERCMDS MVS.CANCEL.TSU.* UACC(NONE) OWNER(*admin*) -
DATA('CANCEL TSO USER SESSIONS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.DISPLAY.** UACC(NONE) OWNER(*admin*) -
DATA('VARIOUS JES2 DISPLAY COMMANDS')
RDEFINE OPERCMDS JES2.MSEND.CMD UACC(NONE) OWNER(*admin*) -
DATA('SEND MESSAGES') AUDIT(ALL(READ))
RDEFINE OPERCMDS JES2.MODIFY.BATOUT UACC(NONE) OWNER(*admin*) -
DATA('MODIFY OUTPUT FILE STATUS FOR BATCH JOBS') -
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.MODIFY.TSUOUT UACC(NONE) OWNER(*admin*) –
DATA('MODIFY OUTPUT FILE STATUS FOR TSO JOBS') -
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.MODIFY.STCOUT UACC(NONE) –
OWNER(*admin*) - DATA('MODIFY OUTPUT FILE STATUS FOR STC JOBS')
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.CANCEL.BAT UACC(NONE) OWNER(*admin*) -
DATA('CANCEL / PURGE BATCH JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.CANCEL.TSU UACC(NONE) OWNER(*admin*) -
DATA('CANCEL / PURGE TSO JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.CANCEL.STC UACC(NONE) OWNER(*admin*) -
DATA('CANCEL / PURGE STC JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.CANCEL.DEV UACC(NONE) OWNER(*admin*) -
DATA('CANCEL / PURGE JOBS ON JES2 DEVICES') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.RELEASE.BATOUT UACC(NONE) -
OWNER(*admin*) DATA('RELEASE OUTPUT FILES FOR BATCH JOBS') -
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.RELEASE.STCOUT UACC(NONE) -
OWNER(*admin*) DATA('RELEASE OUTPUT FILES FOR STC JOBS') -
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.RELEASE.TSUOUT UACC(NONE) -
OWNER(admin) DATA('RELEASE OUTPUT FILES FOR TSO JOBS') -
AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.RESTART.DEV UACC(NONE) OWNER(*admin*) -
DATA('RESTART JES2 DEVICES') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.RESTART.BAT UACC(NONE) OWNER(*admin*) -
DATA('RESTART BATCH JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.MODIFYHOLD.BAT UACC(NONE) -
OWNER(*admin*) DATA('HOLD BATCH JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.MODIFYHOLD.STC UACC(NONE) -
OWNER(*admin*) DATA('HOLD STC JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.MODIFYHOLD.TSU UACC(NONE) -
OWNER(*admin*) DATA('HOLD TSO JOBS') AUDIT(ALL(UPDATE))
RDEFINE OPERCMDS JES2.ROUTE.JOBOUT UACC(NONE) -
OWNER(*admin*) DATA('ROUTE JOB OUTPUT') AUDIT(ALL(UPDATE))

In preparation for permitting SDSF end-users access to system commands, conditional access using SDSF must be defined. The following commands may be used to define SDSF as a console and permit SDSF end-users access to the SDSF console:

RDEFINE CONSOLE SDSF UACC(NONE) OWNER(*admin*) -
DATA('DEFINE SDSF AS A CONSOLE FOR CONDITIONAL ACCESS')
PERMIT SDSF CLASS(CONSOLE) ID(*end-user-group*) ACCESS(READ)

The following commands may be used to permit access to MVS and JES2 command resources for SDSF users, including end-users:

PERMIT MVS.DISPLAY.** CLASS(OPERCMDS) ID(*oper-group sysprog-group* -
end-user-group) ACCESS(READ)
PERMIT MVS.CANCEL.ATX.* CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT MVS.CANCEL.ATX.* CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT MVS.CANCEL.TSU.* CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT MVS.CANCEL.TSU.* CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.DISPLAY.** CLASS(OPERCMDS) ID(*oper-group sysprog-group* -
end-user-group) ACCESS(READ)
PERMIT JES2.MSEND.CMD CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(READ)
PERMIT JES2.MSEND.CMD CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(READ) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFY.BATOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFY.BATOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFY.TSUOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFY.TSUOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFY.STCOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFY.STCOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.CANCEL.TSU CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)

PERMIT JES2.CANCEL.TSU CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.CANCEL.STC CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.CANCEL.STC CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.CANCEL.DEV CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.CANCEL.DEV CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.RELEASE.BATOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.RELEASE.BATOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.RELEASE.STCOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.RELEASE.STCOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.RELEASE.TSUOUT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.RELEASE.TSUOUT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.RESTART.DEV CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.RESTART.DEV CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.RESTART.BAT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(CONTROL)
PERMIT JES2.RESTART.BAT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(CONTROL) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFYHOLD.BAT CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFYHOLD.BAT CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFYHOLD.STC CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFYHOLD.STC CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))
PERMIT JES2.MODIFYHOLD.TSU CLASS(OPERCMDS) ID(*oper-group* -
sysprog-group) ACCESS(UPDATE)
PERMIT JES2.MODIFYHOLD.TSU CLASS(OPERCMDS) ID(*end-user-group*) -
ACCESS(UPDATE) WHEN(CONSOLE(SDSF))

PERMIT JES2.ROUTE.JOBOUT CLASS(OPERCMDS) ID(*oper-group* - *sysprog-group*) ACCESS(UPDATE)
PERMIT JES2.ROUTE.JOBOUT CLASS(OPERCMDS) ID(*end-user-group*) - ACCESS(UPDATE) WHEN(CONSOLE(SDSF))

13.2.3.3.4 Printer and Punch Controls

Refer to *Section 5.3.3, Security Controls for Output*, for general controls regarding printer and punch resources in a RACF environment. The following commands may be used to control access to JES2 printer and punch resources defined to the WRITER resource class as discussed in *Section 13.2.1.7.12, Printers and Punches*:

RDEFINE WRITER *jesx*.LOCAL.*device-name* UACC(NONE) OWNER(*admin*) - DATA('JES2 LOCAL PRINTER / PUNCH')
RDEFINE WRITER *jesx*.RJE.*device-name* UACC(NONE) OWNER(*admin*) - DATA('JES2 REMOTE PRINTER / PUNCH')

PERMIT *jesx*.LOCAL.*device-name* CLASS(WRITER) ID(*oper-group sysprog-group*) - ACCESS(ALTER)
PERMIT *jesx*.RJE.*device-name* CLASS(WRITER) ID(*oper-group sysprog-group*) - ACCESS(ALTER)

13.2.3.3.5 Jobs, Output Group, SYSIN/SYSOUT Controls

Refer to *Section 5.3.4, Security Controls for JES2 SPOOL Data Sets*, for general controls regarding JES2 spool resources in a RACF environment. The following commands may be used to control access to JES2 job and output group resources defined to the JESSPOOL resource class as discussed in *Section 13.2.1.7.24, Jobs, Output Group*, and SYSIN/SYSOUT Data Sets:

RDEFINE JESSPOOL *nodeid.userid.jobname.jobid*.JCL UACC(NONE) - OWNER(*admin*) DATA('VIEW AND EDIT JOB JCL') AUDIT(ALL(READ))
RDEFINE JESSPOOL *nodeid.userid.jobname.jobid* UACC(NONE) - OWNER(*admin*) DATA('VIEW AND MODIFY JOB STATUS') - AUDIT(ALL(READ))
RDEFINE JESSPOOL *nodeid.userid.jobname.jobid*.GROUP.*ogroupid* - UACC(NONE) OWNER(*admin*) DATA('VIEW AND MODIFY JOB OUTPUT - STATUS') AUDIT(ALL(READ))

PERMIT *nodeid.userid.jobname.jobid*.JCL CLASS(JESSPOOL) ID(*userid*) ACCESS(READ)
PERMIT *nodeid.userid.jobname.jobid* CLASS(JESSPOOL) ID(*userid*) ACCESS(READ)
PERMIT *nodeid.userid.jobname.jobid* CLASS(JESSPOOL) ID(*userid*) ACCESS(ALTER)
PERMIT *nodeid.userid.jobname.jobid*.GROUP.*ogroupid* CLASS(JESSPOOL) - ID(*userid*) ACCESS(READ)
PERMIT *nodeid.userid.jobname.jobid*.GROUP.*ogroupid* CLASS(JESSPOOL) -

ID(*userid*) ACCESS(ALTER)

13.2.3.3.6 SDSF Server Controls

The following commands may be used to control access to resources specific to the control of the SDSF Server as discussed in *Section 13.2.1.7.25, SDSF Server Operations*:

```
RDEFINE SDSF ISFCMD.OPT.SERVER UACC(NONE) OWNER(admin) -
   DATA('USE OF THE SERVER PARAMETER ON THE SDSF -
      COMMAND')
RDEFINE SDSF SERVER.NOPARM UACC(NONE) OWNER(admin) -
   DATA('REVERT TO ISFPARMS IN ASSEMBLER MACRO FORMAT') -
      AUDIT(ALL(READ))
RDEFINE OPERCMDS server.MODIFY.DISPLAY UACC(NONE) -
   OWNER(admin) DATA('USE OF DISPLAY PARAMETER ON MVS MODIFY -
      COMMAND (F) FOR THE SDSF SERVER')
RDEFINE OPERCMDS server.MODIFY.** UACC(NONE) -
   OWNER(admin) DATA('USE OF VARIOUS MODIFY PARAMETERS ON -
      MVS MODIFY COMMAND (F) FOR THE SDSF SERVER') -
         AUDIT(ALL(UPDATE))

PERMIT ISFCMD.OPT.SERVER CLASS(SDSF) ID(sysprog-group) -
   ACCESS(READ)
PERMIT SERVER.NOPARM CLASS(SDSF) ID(sysprog-userid) ACCESS(READ)
PERMIT server.MODIFY.DISPLAY CLASS(OPERCMDS) ID(oper-group -
   sysprog-group) ACCESS(READ)
PERMIT server.MODIFY.** CLASS(OPERCMDS) ID(oper-group sysprog-group) -
   ACCESS(CONTROL)
```

13.2.3.3.7 MQ Controls

13.2.3.3.7.1 MQ Queue Protection

Refer to *Section 4.3.3.2.4, Queue Security*, for general controls regarding MQ queue resources in a RACF environment. The following commands may be used to control access to MQ queue resources defined to the MQQUEUE resource class as discussed in *Section 13.2.1.7.26.1, Queue Protection*:

```
RDEFINE MQQUEUE ssid.prefix.SERVER.** UACC(NONE) OWNER(admin) -
   DATA('SDSF SERVER REQUEST QUEUE')
RDEFINE MQQUEUE ssid.prefix.CLIENT.** UACC(NONE) OWNER(admin) -
   DATA('SDSF CLIENT REQUEST QUEUE TO SEND WORK TO SERVER')
RDEFINE MQQUEUE ssid.prefix.USER.** UACC(NONE) OWNER(admin) -
   DATA('SDSF REPLYTO QUEUE TO RECEIVE SERVER MESSAGES')
```

RDEFINE MQQUEUE *ssid.prefix*.USER.&RACUID.** UACC(NONE) -
OWNER(*admin*) DATA('SDSF REPLYTO QUEUE FOR SPECIFIC USERS -
TO RECEIVE SERVER MESSAGES')
RDEFINE MQQUEUE *ssid.prefix*.MODEL.** UACC(NONE) OWNER(*admin*) -
DATA('SDSF MODEL QUEUE TO CREATE DYNAMIC QUEUES')
RDEFINE MQQUEUE *ssid*.XMIT.QUEUE UACC(NONE) OWNER(*admin*) -
DATA('TRANSMISSION QUEUE TO SEND MESSAGES TO REMOTE SDSF –
SERVERS')

PERMIT *ssid.prefix*.SERVER.** CLASS(MQQUEUE) ID(*SDSF-server-userid -
MQ-userid*) ACCESS(ALTER)
PERMIT *ssid.prefix*.CLIENT.** CLASS(MQQUEUE) ID(*SDSF-server-userid*) -
ACCESS(ALTER)
PERMIT *ssid.prefix*.CLIENT.** CLASS(MQQUEUE) ID(*oper-group sysprog-
group -end-user-group*) ACCESS(UPDATE)
PERMIT *ssid.prefix*.USER.** CLASS(MQQUEUE) ID(*SDSF-server-userid*) -
ACCESS(UPDATE)
PERMIT *ssid.prefix*.USER.&RACUID.** CLASS(MQQUEUE) -
ID(*oper-group sysprog-group end-user-group*) ACCESS(UPDATE)
PERMIT *ssid.prefix*.MODEL.** CLASS(MQQUEUE) ID(*SDSF-server-userid -
oper-group sysprog-group end-user-group*) ACCESS(UPDATE)
PERMIT *ssid*.XMIT.QUEUE CLASS(MQQUEUE) ID(*SDSF-server-userid*) -
ACCESS(UPDATE)

In the previous example, MQ-userid is the userid associated with the MQ started task.

13.2.3.3.7.2 MQ Queue Definition Authority Protection

Refer to *Section 4.3.3.2.4, Queue Security*, and *Section 4.3.3.2.9, Command Security,* for general controls regarding MQ queue and command resources in a RACF environment. The following commands may be used to control access to MQ queue definition authority resources as discussed in *Section 13.2.1.7.26.2, Queue Definition Authority*:

RDEFINE MQCMDS *ssid*.DEFINE.QMODEL UACC(NONE) OWNER(*admin*) -
DATA('DEFINE QUEUE COMMAND') AUDIT(ALL(UPDATE))
RDEFINE MQCMDS *ssid*.DEFINE.QALIAS UACC(NONE) OWNER(*admin*) -
DATA('DEFINE QUEUE ALIAS COMMAND') AUDIT(ALL(UPDATE))
RDEFINE MQADMIN *ssid*.QUEUE.*prefix*.** UACC(NONE) OWNER(*admin*) -
DATA('ADMIN AUTHORITY TO DEFINE QUEUES')
RDEFINE MQQUEUE *ssid*.SYSTEM.** UACC(NONE) OWNER(*admin*) -
DATA('ACCESS SYSTEM QUEUES')

PERMIT *ssid*.DEFINE.QMODEL CLASS(MQCMDS) ID(*SDSF-server-userid - CSQ-oper-userid*) ACCESS(ALTER)
PERMIT *ssid*.DEFINE.QALIAS CLASS(MQCMDS) ID(*SDSF-server-userid - CSQ-oper-userid*) ACCESS(ALTER)
PERMIT *ssid*.QUEUE.*prefix*.** CLASS(MQADMIN) ID(*SDSF-server-userid*) - ACCESS(ALTER)
PERMIT *ssid*.SYSTEM.** CLASS(MQQUEUE) ID(*SDSF-server-userid*) - ACCESS(ALTER)

In the previous example, CSQ-oper-userid is the operator userid used by MQ for commands entered from the console.

13.2.3.3.7.3 Connection Security Protection

Refer to *Section 4.3.3.2.3, Connection Security*, general controls regarding connection security in a RACF environment. The following commands may be used to control connect access to MQ as discussed in *Section 13.2.1.7.26.3, Connection Security*:

RDEFINE MQCONN *ssid*.BATCH UACC(NONE) OWNER(*admin*) -
DATA('ALLOW CONNECTION FOR BATCH AND TSO USERS') –
AUDIT(ALL(READ))

PERMIT *ssid*.BATCH CLASS(MQCONN) ID(SDSF-*server-userid - oper-group sysprog-group end-user-group*) ACCESS(READ)

13.2.3.3.7.4 Context Security Protection

Refer to *Section 4.3.3.2.8, Context Security*, general controls regarding context security in a RACF environment. The following commands may be used to control access to identity data in a message as discussed in *Section 13.2.1.7.26.4, Context Security*:

RDEFINE MQADMIN ssid.CONTEXT UACC(NONE) OWNER(*admin*) -
DATA('SETTING THE IDENTITY CONTEXT FIELDS IN THE -
MESSAGE HEADER')

PERMIT *ssid*.CONTEXT CLASS(MQADMIN) ID(*SDSF-server-userid*) –
ACCESS(UPDATE)
PERMIT *ssid*.CONTEXT CLASS(MQADMIN) ID(*MQ-userid*) –
ACCESS(ALTER)

In the previous example, *MQ-userid* is the userid associated with the MQ started task.

13.2.4 TOP SECRET

This section describes the commands needed to implement the security requirements discussed throughout *Section 13.2, System Display and Search Facility,* in a TOP SECRET environment. The following task categories are described:

- Data set protection
- Started task definitions
- Resource controls

13.2.4.1 Data Set Controls

The following commands may be used to provide the required data set access controls documented in *Section 13.2.1.1, SDSF Data Set Protection*:

```
TSS ADDTO(SYS1) DSN(SYS1.ISF.-)
TSS PERMIT(sysprog-group) DSN(SYS1.ISF.-) ACCESS(ALL)
```

13.2.4.2 Started Task Definitions

The following commands may be used to define the required STC controls documented in *Section 3.4.2.3, Started Task Control (STC) Users*:

- *(ZISFT360: CAT II) The IAO will create a TOP SECRET ACID named SDSF, or in the case of multiple SDSF servers, prefixed with SDSF.*

```
TSS CREATE(SDSF) TYPE(USER) NAME('SDSF SERVER STC')
    DEPT(dept-acid) FACILITY(STC) PASSWORD(password,0)
TSS ADDTO(STC) PROCNAME(SDSF) ACID(SDSF)
TSS ADDTO(SDSF) SOURCE(INTRDR)
```

13.2.4.3 Resource Controls

This section describes the commands needed to implement the required controls for SDSF resources and functions discussed in *Section 13.2.1.7, SDSF Resource Protection*.

The SDSF resource class is predefined in the TOP SECRET RDT. An administrator can give default protection to SDSF resources by modifying the SDSF resource class entry in the RDT to include the DEFPROT attribute. The following command may be used to assign default protection to resources in the SDSF resource:

```
TSS REPLACE(RDT) RESCLASS(SDSF) ATTR(DEFPROT)
```

- *(ZISFT370: CAT II) The IAO will assign the DEFPROT attribute to the SDSF resource class entry in the TOP SECRET RDT.*

13.2.4.3.1 SDSF Group Membership Controls

The following commands may be used to control access to SDSF groups as discussed in *Section 13.2.1.7.1, Membership in SDSF Groups*. This example establishes default protection for SDSF groups:

TSS ADDTO(dept-acid) SDSF(GROUP.)

This example presumes an SDSF group named sysprog is configured in ISFPARMS for an SDSF server named sdsf. The following command may be used to permit access to the SDSF sysprog group to systems programming personnel:

TSS PERMIT(sysprog-group) SDSF(GROUP.sysprog.sdsf) ACCESS(READ)

13.2.4.3.2 SDSF Resources Controls

This section shows examples of security controls as discussed in the following general sections:

Section 13.2.1.7.2, SDSF Panels
Section 13.2.1.7.3, SDSF Maintenance Commands
Section 13.2.1.7.4, SDSF Filtering Commands
Section 13.2.1.7.5, SDSF / Command
Section 13.2.1.7.7, Overtypeable Fields
Section 13.2.1.7.9, Destination Names
Section 13.2.1.7.10, Destination Operator Authority
Section 13.2.1.7.11, Initiators
Section 13.2.1.7.13, Lines
Section 13.2.1.7.14, Nodes
Section 13.2.1.7.15, Offloaders
Section 13.2.1.7.16, MAS Members
Section 13.2.1.7.17, Job Classes
Section 13.2.1.7.18, Scheduling Environments
Section 13.2.1.7.19, WLM Resources
Section 13.2.1.7.20, System Requests
Section 13.2.1.7.21, WLM Enclaves
Section 13.2.1.7.22, z/OS UNIX Processes
Section 13.2.1.7.23, Spool Volumes

The following command may be used to establish default protection for resources defined to the SDSF resource class:

TSS ADDTO(*dept-acid*) SDSF(ISF)

The following commands may be used to permit access to SDSF resources that are restricted to both operations personnel and systems programming personnel:

TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFCMD.DSP.) ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFCMD.ODSP.) ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFCMD.FILTER.)
ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFOPER.SYSTEM)
ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFATTR.) ACCESS(UPDATE)

TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFOPER.ANYDEST.JES+)
ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFAUTH.DEST.*)
ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFAUTH.DEST.*.*)
ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFOPER.DEST.JES+)
ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFAUTH.DEST.*.DATASET.)
ACCESS(NONE)
TSS PERMIT(*sysprog-group*, *oper-group*)
SDSF(ISFAUTH.DEST.*.DATASET.JES+++++) ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFINIT.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFLINE.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFNODE.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFSO.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFMEMB.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFJOBCL.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFSE.) ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFRES.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFSR.) ACCESS(READ)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFENC.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFPROC.) ACCESS(ALL)
TSS PERMIT(*sysprog-group*, *oper-group*) SDSF(ISFSP.) ACCESS(ALL)

The following commands may be used to permit access to SDSF resources that are restricted to systems programming personnel only:

TSS PERMIT(*sysprog-group*) SDSF(ISFCMD.MAINT.) ACCESS(READ)
TSS PERMIT(*oper-group*) SDSF(ISFCMD.FILTER.INPUT) ACCESS(NONE)

NOTE: The ISFCMD.FILTER.INPUT permission removes oper-group access based on the previous example showing permits of SDSF resources that are restricted to both operations personnel and systems programming personnel.

The following commands may be used to permit access to SDSF resources that are permitted to authorized SDSF end-users:

TSS PERMIT(*end-user-group*) SDSF(ISFCMD.DSP.) ACCESS(READ)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.BURST)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.CLASS)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.DEST)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.FCB)

ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.FLASH)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.FORMS)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.PRMODE)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.UCS)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTPUT.WRITER)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.OUTDESC.)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFATTR.JOB.PRTDEST)
ACCESS(UPDATE)
TSS PERMIT(*end-user-group*) SDSF(ISFOPER.ANYDEST.JES+)
ACCESS(READ)
TSS PERMIT(*end-user-group*) SDSF(ISFSE.) ACCESS(READ)

13.2.4.3.3 MVS and JES2 Command Controls

Refer to *Section 3.4.5.6, OS/390 System Command Controls*, and *Section 5.4.5, Security Controls for JES2 Commands*, for general TOP SECRET controls regarding MVS and JES2 system command resources respectively. The following commands may be used to permit access to MVS and JES2 command resources for SDSF users, including end-users, as discussed in *Section 13.2.1.7.8, MVS and JES2 Commands Generated by SDSF*:

TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(MVS.DISPLAY.) ACCESS(READ)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(MVS.CANCEL.ATX.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(MVS.CANCEL.TSU.) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.DISPLAY.) ACCESS(READ)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MSEND.CMD) ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFY.BATOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFY.TSUOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFY.STCOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.CANCEL.BAT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.CANCEL.TSU) ACCESS(UPDATE) ACTION(AUDIT)

TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.CANCEL.STC) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.CANCEL.DEV) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.RELEASE.BATOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.RELEASE.STCOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.RELEASE.TSUOUT) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.RESTART.DEV) ACCESS(UPDATE) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.RESTART.BAT) ACCESS(CONTROL) ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFYHOLD.BAT) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFYHOLD.STC) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.MODIFYHOLD.TSU) ACCESS(UPDATE)
ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
OPERCMDS(JES2.ROUTE.JOBOUT) ACCESS(UPDATE) ACTION(AUDIT)

13.2.4.3.4 Printer and Punch Controls

Refer to *Section 5.4.3, Security Controls for Output*, for general controls regarding printer and punch resources in a TOP SECRET environment. The following commands may be used to control access to JES2 printer and punch resources defined to the **WRITER** resource class as discussed in *Section 13.2.1.7.12, Printers and Punches*:

TSS PERMIT(*oper-group, sysprog-group*) WRITER(*jesx.LOCAL.device-name*)
ACCESS(ALL)
TSS PERMIT(*oper-group, sysprog-group*) WRITER(*jesx.RJE.device-name*)
ACCESS(ALL)

13.2.4.3.5 Jobs, Output Group, SYSIN/SYSOUT Controls

Refer to *Section 5.4.4, Security Controls for JES2 SPOOL Data Sets*, for general controls regarding JES2 spool resources in a TOP SECRET environment. The following commands may be used to control access to JES2 job and output group resources defined to the JESSPOOL resource class as discussed in *Section 13.2.1.7.24, Jobs, Output Group, and SYSIN/SYSOUT Data Sets*:

TSS PERMIT(*acid*) JESSPOOL(*nodeid.acid.jobname.jobid.*JCL)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*acid*) JESSPOOL(*nodeid.acid.jobname.jobid*)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*acid*) JESSPOOL(*nodeid.acid.jobname.jobid*)
ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(*acid*) JESSPOOL(*nodeid.acid.jobname.jobid.*GROUP.*ogroupid*)
ACCESS(READ) ACTION(AUDIT)
TSS PERMIT(*acid*) JESSPOOL(*nodeid.acid.jobname.jobid.*GROUP.*ogroupid*)
ACCESS(ALL) ACTION(AUDIT)

13.2.4.3.6 SDSF Server Controls

The following commands may be used to control access to resources specific to the control of the SDSF Server as discussed in *Section 13.2.1.7.25, SDSF Server Operations*:

TSS PERMIT(*sysprog-group*) SDSF(ISFCMD.OPT.SERVER) ACCESS(READ)
TSS PERMIT(*sysprog-acid*) SDSF(SERVER.NOPARM) ACCESS(READ)
ACTION(AUDIT)
TSS PERMIT(*oper-group, sysprog-group*) OPERCMDS(server.MODIFY.DISPLAY)
ACCESS(READ)
TSS PERMIT(*oper-group, sysprog-group*) OPERCMDS(server.MODIFY.)
ACCESS(CONTROL) ACTION(AUDIT)

13.2.4.3.7 MQ Controls

13.2.4.3.7.1 MQ Queue Protection

Refer to *Section 4.3.4.2.4, Queue Security*, for general controls regarding MQ queue resources in a TOP SECRET environment. The following commands may be used to control access to MQ queue resources defined to the MQQUEUE resource class as discussed in *Section 13.2.1.7.26.1, Queue Protection*:

TSS PERMIT(*SDSF-server-acid, MQ-acid*) MQQUEUE(*ssid.prefix*.SERVER.)
ACCESS(ALL)
TSS PERMIT(*SDSF-server-acid*) MQQUEUE(*ssid.prefix*.CLIENT.)
ACCESS(ALL)

TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
MQQUEUE(*ssid.prefix*.CLIENT.) ACCESS(UPDATE)
TSS PERMIT(*SDSF-server-acid*) MQQUEUE(*ssid.prefix*.USER.)
ACCESS(UPDATE)
TSS PERMIT(*oper-group, sysprog-group, end-user-group*)
MQQUEUE(*ssid.prefix*.USER.%.) ACCESS(UPDATE)
TSS PERMIT(*SDSF-server-acid, oper-group, sysprog-group, end-user-group*)
MQQUEUE(*ssid.prefix*.MODEL.) ACCESS(UPDATE)
TSS PERMIT(*SDSF-server-acid*) MQQUEUE(ssid.XMIT.QUEUE)
ACCESS(UPDATE)

In the previous example, **MQ-acid** is the ACID associated with the MQ started task.

13.2.4.3.7.2 MQ Queue Definition Authority Protection

Refer to *Section 4.3.4.2.4, Queue Security*, and *Section 4.3.4.2.9, Command Security,* for general controls regarding MQ queue and command resources in a TOP SECRET environment. The following commands may be used to control access to MQ queue definition authority resources as discussed in *Section 13.2.1.7.26.2, Queue Definition Authority*:

TSS PERMIT(*SDSF-server-acid, CSQ-oper-acid*)
MQCMDS(*ssid*.DEFINE.QMODEL) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(*SDSF-server-acid, CSQ-oper-acid*)
MQCMDS(*ssid*.DEFINE.QALIAS) ACCESS(ALL) ACTION(AUDIT)
TSS PERMIT(*SDSF-server-acid*) MQADMIN(*ssid*.QUEUE.*prefix*.)
ACCESS(ALL)
TSS PERMIT(*SDSF-server-acid*) MQQUEUE(*ssid*.SYSTEM.)
ACCESS(ALL)

In the previous example, CSQ-oper-acid is the operator ACID used by MQ for commands entered from the console.

13.2.4.3.7.3 Connection Security Protection

Refer to *Section 4.3.4.2.3, Connection Security*, for general controls regarding connection security in a TOP SECRET environment. The following commands may be used to control connect access to MQ as discussed in *Section 13.2.1.7.26.3, Connection Security*:

TSS PERMIT(*SDSF-server-acid*, *oper-group*, *sysprog-group*, *end-user-group*)
MQCONN(*ssid*.BATCH) ACCESS(READ) ACTION(AUDIT)

13.2.4.3.7.4 Context Security Protection

Refer to *Section 4.3.4.2.8, Context Security*, for general controls regarding context security in a TOP SECRET environment. The following commands may be used to control access to identify data in a message as discussed in *Section 13.2.1.7.26.4, Context Security*:

TSS PERMIT(*SDSF-server-acid*) MQADMIN(*ssid*.CONTEXT) ACCESS(UPDATE)
TSS PERMIT(*MQ-acid*) MQFADMIN(*ssid*.CONTEXT) ACCESS(ALL)

In the previous example, MQ-acid is the ACID associated with the MFQF started task.

This page is intentionally left blank.

14. SYSTEMS MANAGEMENT AND CONTROL SOFTWARE

14.1 General Considerations

Systems management and control software serves many purposes. The most common purposes include controlling production batch processing and automating operations functions. Systems management products may be acquired separately or as integrated product suites.

All security and product interfaces must be carefully evaluated for possible system and data integrity problems, and for potential security exposures. These include interfaces delivered with the management and control software, and interfaces offered by other software packages that may interact with the suite. These interfaces may offer their own internal security, provide the potential to circumvent ACP security controls, or expose new or existing weaknesses in protection.

Depending on the product, control access authority by using one of the following three methods:

- Exclusive use of ACP controls
- A combination of ACP controls and Internal Product Security Controls
- Internal Product Security Controls only

The IAO administers access authority assignments for users.

Use ACP controls whenever possible. However, it may not be possible to provide a totally secure environment using only ACP controls. In this case, the use of internal security may be warranted and must be investigated for possible use. If it is determined that an enhanced level of protection is gained that the ACP does not provide, the internal security may be activated. Under no circumstances are base-level ACP controls compromised.

Use the following recommendations when securing access to systems management software:

(1) Strictly control access to the on-line applications, and restrict access only to authorized personnel. Rigidly control the use of commands, options, and functions within the products. Restrict access only to those functions necessary for users to accomplish their assigned responsibilities.

(2) Review all interfaces for possible system and data integrity problems, and for potential security exposures. Document any potential security exposures and notify DISA FSO.

The ACP controls access authority. Evaluate internal security for possible use, providing it does not replace or compromise existing ACP security controls.

14.2 INCONTROL for OS/390

Vendor: BMC Software

BMC's INCONTROL for OS/390 is a suite of fully integrated products designed to automate, manage, and streamline operations on the OS/390 platform. The following products from the INCONTROL suite as standard components are included:

- IOA (Common interface)
- CONTROL-O (Operations automation package)
- CONTROL-M (Job scheduling package)

14.2.1 IOA

IOA acts as the installation path for the CONTROL-M and CONTROL-O products via the INCONTROL Installation and Customization Engine (ICE). This process sets up and maintains the INCONTROL operating environment. It is through the ICE process that system security is specified. The system security product is specified once for the entire suite of products, not during the installation of each product.

The ICE is an ISPF application consisting of a set of dialogs that provide a simplified method of specifying data and creating installation jobs to install the INCONTROL products. Each activity in the installation menu is invoked by selecting a product ID and an option number. The options direct various activities during the installation of IOA. The options that directly affect security are as follows:

SECURITY Option 5 of the Main menu. It allows the site to install IOA security interfaces based on which resident ACP is installed (ACF2, RACF, or TOP SECRET). The security product is specified during the IOA installation process using the SECURITY installation parameter.

CUSTOMIZE Option 6 of the Main menu. This selection is used to customize certain INCONTROL product operational parameters and other activities that affect the operation of the INCONTROL products.

Once a major installation activity is selected from the Main menu, secondary screens are displayed listing all the major and minor steps associated with the selected activity.

The IOA common security services module, IOASECUR, is invoked each time an INCONTROL product requires a security service (such as creating the security environment, checking a user's authority, extracting user information, or deleting a security environment). Module IOASECUR is installed during the installation of IOA.

The Extended Definition security mode for the IOA common components is implemented at all sites. The Extended Definition mode grants each user discrete access for a specific action to a protected item. A user granted access to an item may be granted or denied any action (*add*, *change*, and *update*) separately. This mode requires the Administrator to define additional access rules, as for each action there is an associated resource structure. However, it provides the maximum flexibility and accuracy for granting authorizations.

The following table lists the IOA resources protected with Extended Definition mode enabled:

Table B-51. IOA EXTENDED DEFINITION SECURITY CALLS (14.2.1 a)

IOA EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
IOA Online Facility	$$IOAONLINE.*qname*	Verifies user access to the IOA Online Facility. From the main menu, access to BMC products (e.g., CONTROL-O, CONTROL-M) is available.
VTAM Monitor		Verifies userid/password when entering IOA Online Facility under VTAM.
IOA Condition	$$ADDCND.*qname.cond* $$DELCND.*qname.cond* $$CHKCND.*qname.cond*	Verifies user access to add/delete/change IOA conditions and CONTROL-M resources.
CONTROL-M Quantitative Resource	$$ADDRES.*qname.res* $$DELRES.*qname.res* $$CHARES.*qname.res* $$CHKRES.*qname.res*	
CONTROL-M Control Resource	$$ADDCTL.*qname.cond* $$DELCTL.*qname.cond* $$CHKCTL.*qname.cond*	
IOA Manual Condition	$$NEWCND.*qname.mancnd* $$ERACND.*qname.mancnd*	
Operator Command	$$IOACMD.*qname.cmndtext*	Verifies authorization to issue operator commands from within an IOA environment (i.e., utilities and monitors).
User Data Set	*data.set.name* (Defined to the DATASET resource class) $$IOADIR.*qname.* $$IOAVIW.*qname.mem* $$IOAEDT.*qname.mem* $$IOASAV.*qname.mem* $$IOADEL.*qname.mem*	From the IOA Online Facility, verifies user access to data sets that contain items such as JCL, documentation, and IOA tables and calendars.

IOA EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Executing Batch Utilities	$$IOAUTL.*qname.utility-name*	Verifies user access to IOA Online Facility functions via batch.

Use the following implementation and security recommendations for the IOA common component:

(1) Install and maintain IOA product software using SMP/E.

(2) Install IOA to use the resident ACP (ACF2, RACF, or TOP SECRET). Specify the ACP during the installation of IOA using the SECURITY option from the main ICE menu.

(3) Using ICE, specify the following STIG standard values for the IOA security parameters for all ACP environments. Additional IOA security parameters with standard values specific to the ACP are documented in *Sections 14.3.1 (ACF)*, *14.4.1 (RACF)*, and *14.5.1 (TOP SECRET*):

Table B-52. IOA SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS (14.2.1 b)

REQUIRED IOA SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
SECTOL SECTOLI (IOA Version 6 and above)	Do not allow any operation when the ACP inactive or when a specific resource is not defined to the ACP.	NO
IOATCBS	Set each task in the IOA Online monitor to be activated with the logged on user authorizations.	YES
DFMI06	Definition mode for security module IOASE06	EXTEND
DFMI07	Definition mode for security module IOASE07	EXTEND
DFMI09	Definition mode for security module IOASE09	EXTEND
DFMI12	Definition mode for security module IOASE12	EXTEND
DFMI16 (IOA Version 6 and above)	Definition mode for security module IOASE16	EXTEND
DFMI32	Definition mode for security module IOASE32	EXTEND
DFMI40 (IOA Version 6 and above)	Definition mode for security module IOASE40	EXTEND

(4) IOA security exits are not modified by the site. If a modification is deemed necessary, it must be pre-approved by DISA FSO. A final source code review must be performed by DISA FSO prior to the implementation of the modified exit into a production environment.

(5) Access to the IOA Online facility and other IOA resources listed in the *IOA EXTENDED DEFINITION SECURITY CALLS* table is restricted to system-level support personnel. Authorized personnel include systems programmers, system operators, automation operators, and production control staff.

With the granularity and flexibility Extended Definition mode provides, access authorization to IOA resources outside the system-level support realm may be permitted for the purposes of job scheduling (i.e., CONTROL-M) only. For these authorized users, the following recommendations are in effect:

- Access is granted to specific individuals and not at the group level.
- Resource access rules are fully qualified and not generic in nature.
- Justification documentation with IAO approval is required and must be filed with the IAO.

In addition, access to IOA resources allowing the issuing of system commands (i.e., $$IOACMD.*qname.cmndtext*) comply with the recommendations documented in *Section 3.1.5.6, OS/390 System Command Controls,* to include authorization and logging.

(6) Restrict access to IOA product data sets to system-level support personnel and IOA product suite of STCs. Authorized personnel include systems programmers, system operators, automation operators, and production control staff. More specifically:

- *Alter* access to IOA product data sets are restricted to systems programmers.

- *Update* access to IOA Base, Installation, and Maintenance libraries is restricted to the systems programmers.

- *Update* access to IOA Operations, Core, and Repository libraries is restricted to system-level support personnel and IOA product suite STCs.

As noted in the previous item, access authorization to IOA resources outside the system-level support realm may be permitted for the purposes of job scheduling (i.e., CONTROL-M) only. For these authorized users, , the following recommendations are in effect:

- Access is granted to specific individuals and not at the group level.
- Data set access rules are fully qualified and not generic in nature.
- *Update* access to IOA Core, Repository, and Operations files is permitted and logged.
- Program pathing is in effect to ensure data set access is performed using INCONTROL products.
- Justification documentation with IAO approval is required and must be filed with the IAO.

- *(ZIOA0010: CAT II) The IAO will ensure that IOA product data sets are protected in accordance with STIG requirements.*
- *(ZIOA0022: CAT II) The IAO will ensure that IOA product security exits are installed and configured in accordance with STIG requirements.*
- *(ZIOA0032: CAT II) The IAO will ensure that IOA security parameter values are specified in accordance with STIG requirements.*

14.2.2 CONTROL-O

CONTROL-O is the automated console operations component of the INCONTROL suite of products. It automatically detects messages, commands, and events, and responds by performing console actions according to predefined user specifications.

The following table contains CONTROL-O operational parameters that have relevance to the security of the product and depicts the STIG required values:

Table B-53. REQUIRED CONTROL-O OPERATIONAL PARAMETERS (14.2.2 a)

REQUIRED CONTROL-O OPERATIONAL PARAMETERS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
AUTOMLOG	Automation Log facility is used. The Automation Log file resides in a DIV (Data in Virtual) VSAM Linear data set. ***NOTE:*** The Automation Log file must be large enough to not wrap between system backups.	V
RUNTCACH	Number of security cache entries allocated. The security cache improves runtime security check performance by saving security blocks used for the authority check and reusing them in the subsequent authority checks.	Site Defined Vendor recommends 100.
RUNTSEC	Activate runtime security checks (according to the value of a rule's runtime security parameter RUNTSEC). ***NOTE:*** This parameter is obsolete with CONTROL-O Version 6 and above.	Y
RUNTDFT	Runtime security checks are performed according to the authority of the owner of the rule. ***NOTE:*** The RUNTSEC field in CONTROL-O rules can be used to override the standard value of OWNER for the RUNTDFT parameter. To ensure runtime security is always in effect, RUNTSEC is set to NONE in CONTROL-O rules.	OWNER

The Extended Definition security mode for CONTROL-O is implemented at all sites. The Extended Definition mode grants each user discrete access for a specific action to a protected item. A user granted access to an item may be granted or denied any action (*add*, *change*, and *update*) separately. This mode requires the Administrator to define additional access rules, as for each action there is an associated resource structure. However, it provides the maximum flexibility and accuracy for granting authorizations.

The following table lists the CONTROL-O resources protected with Extended Definition mode enabled:

Table B-54. REQUIRED CONTROL-O EXTENDED DEFINITION SECURITY CALLS (14.2.2 b)

REQUIRED CONTROL-O EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Ordering a rule	$$CTOORD.*qname.owner*	Verifies if the current user has authorization to order a rule using the value specified in the OWNER field of the CONTROL-O rule.
	ON statements: $$CTOONC.*qname.cmd-text* $$CTODSN.*qname.jobname* $$CTOENV.*qname.event-name* $$CTOJAR.*qname.jobname* $$CTOJED.*qname.jobname* $$CTOONM.*qname.msg-id* $$CTOORL.*qname.owner.rule* $$CTOSTP.*qname.jobname* $$CTOOMG.*qname.exception* $$CTOJSO.*qname.jobname* $$CTOMSG.*qname.msg-string* $$CTOONP.*qname.msg-txt*	Verifies that the owner of a CONTROL-O rule has the authorization to use various ON and DO statements. ON statements define events and DO statements define actions. This check is performed when the rule is ordered. Since the STIG required runtime value is OWNER, authorization checking for DO statements using the owner of the CONTROL-O rule is performed when the rule is executed.

REQUIRED CONTROL-O EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
	DO statements: $$CTOASK.*qname.wtor-text* $$CTOCMD.*qname.cmd-text* $$CTORES.*qname.res-name* $$CTOPCM.*qname.msg-text* $$CTODSP.*qname.new-msg-txt* $$CTOMSG.*qname* $$CTODOM.*qname* $$CTOTSO.*qname.comnd* $$CTOCMO.*qname.lib-name.tbl* $$CTOKSL.*qname.ksl-name* $$CTODRL.*qname.ownr.rule* $$CTOSET.*qname.var-name* $$CTOJST.*qname* $$CTOSRQ.*qname.sysreq-type* Runtime Security Option: $$CTORTS.*qname.runtime-sec* ***NOTE:*** *The STIG requirement is to default to the RUNTDFT operational parameter value of OWNER.*	Validates if the owner of a CONTROL-O rule is authorized to use specific RUNTSEC rule values.
Use of TSO commands and KOA scripts	DO TSO $$CTOPTS.*qname.envprc.cmd-txt* DO KSL $$CTOPKS.*qname.envprc.cmd-txt*	Since the STIG required runtime value is OWNER, verifies that the owner of a CONTROL-O rule has the authorization to execute a TSO command or REXX and activate a KOA script.
Access and use of the Automation Options screen	$$CTOAOP.*qname.optnam*. ENTRY $$CTOAOP.*qname.optnam.* obj	Verifies user authorization to access the Automation Options screen and perform various actions (e.g., issuing operator commands, controlling CONTROL-O servers).
Access and use of the Rule Status screen	$$CTOPNLOS.*qname* $$RUL1ZOO.*qname.owner* $$RUL1LOG.*qname.owner* $$RUL1WHY.*qname.owner* $$RUL2HLD.*qname.owner* $$RUL2FRE.*qname.owner* $$RUL2MOD.*qname.owner* $$RUL3DEL.*qname.owner* $$RUL3CAN.*qname.owner*	Verifies user authorization to access the Rule Status screen and perform actions (hold, delete, and so on) on the rules displayed.

REQUIRED CONTROL-O EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Access to functions handled by the XAM interface	$$CTOXAM.*qname*.TYPE*xrrr*	Since the STIG required runtime value is OWNER, verifies that the owner of a CONTROL-O rule has authorization to XAM services.

In the above entities, *msg-text* or *command-text* represents the first 26 characters of the command text (or message text). Note the following regarding the text of commands and messages within ACF2 entities:

All non-alphanumeric characters (blanks, commas, etc.) are changed to periods.
Multiple non-alphanumeric characters are changed to one period.
The period at the end of the text is dropped.
Commands that include the JES2 Backspace character are denied.

Use the following implementation and security recommendations for CONTROL-O:

(1) Install and maintain CONTROL-O product software using SMP/E.

(2) Install CONTROL-O to use the resident ACP (ACF2, RACF, or TOP SECRET). Specify the ACP during the installation of IOA using the SECURITY option from the main ICE menu.

(1) Using ICE, specify the following STIG required values for the CONTROL-O security parameters for all ACP environments:

Table B-55. REQUIRED CONTROL-O SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS (14.2.2 b)

REQUIRED CONTROL-O SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
SECTOLO (IOA Version 6 and above)	Do not allow any operation when the ACP inactive or when a specific resource is not defined to the ACP.	NO
DFMO01	Definition mode for security module CTOSE01	EXTEND
DFMO02	Definition mode for security module CTOSE02	EXTEND
DFMO03	Definition mode for security module CTOSE03	EXTEND
DFMO04	Definition mode for security module CTOSE04	EXTEND
DFMO08	Definition mode for security module CTOSE08	EXTEND

REQUIRED CONTROL-O SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
DFMO15 (IOA Version 6 and above)	Definition mode for security module CTOSE15	EXTEND

(4) CONTROL-O security exits are not modified by the site. If a modification is deemed necessary, it must be pre-approved by DISA FSO. A final source code review must be performed by DISA FSO prior to the implementation of the modified exit into a production environment.

(5) Access to the CONTROL-O resources listed in the *CONTROL-O EXTENDED DEFINITION SECURITY CALLS* table will be restricted to systems programmers, system operators, and automation operators only.

(6) Restrict access to CONTROL-O product sets to systems programmers, system operators, automation operators, and IOA product suite of STCs only. More specifically:

- *Alter* access to CONTROL-O product data sets will be restricted to systems programmers

- *Update* access to CONTROL-O Installation libraries will be restricted to the systems programmers

- *Update* access to CONTROL-O Operations and Repository libraries will be restricted to systems programmers, system operators, automation operators, and IOA product suite STCs

- *(ZIOA0010: CAT II) The IAO will ensure that IOA product data sets are protected in accordance with STIG requirements.*

- *(ZIOA0024: CAT II) The IAO will ensure that Control-O product security exits are installed and configured in accordance with STIG requirements.*

- *(ZIOA0034: CAT II) The IAO will ensure that Control-O Operational parameter values are specified in accordance with STIG requirements.*

- *(ZIOA0036: CAT II) The IAO will ensure that Control-O Security parameter values are specified in accordance with STIG requirements.*

14.2.3 CONTROL-M

CONTROL-M is the scheduling component of the INCONTROL suite of products. It provides the facilities to initiate, trigger, restart, intervene, and control the execution of jobs in a production environment. This adds flexibility to daily processing and scheduling of jobs, enables the operator to manage the timing and flow of work, and controls the allocation of resources. CONTROL-M also provides continual data and status information regarding jobs processing.

The Extended Definition security mode for CONTROL-M is implemented at all sites. The Extended Definition mode grants each user discrete access for a specific action to a protected item. A user granted access to an item may be granted or denied any action (*add*, *change*, and *update*) separately. This mode requires the Administrator to define additional access rules, as for each action there is an associated resource structure. However, it provides the maximum flexibility and accuracy for granting authorizations.

The following table lists the CONTROL-M resources protected with Extended Definition mode enabled:

Table B-56. CONTROL-M EXTENDED DEFINITION SECURITY CALLS (14.2.3 a)

CONTROL-M EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Order a job	$$JOBORD.qname.owner	Verifies if the current user is allowed to order jobs/STCs on behalf of the user ID specified in the OWNER field of the job definition.
JOBDSN security check	$$REGSTR.qname.dataset	
Order a started task	$$STCORD.*qname.stcname*	
Access JCL library	*data.set.name* (Defined to the DATASET resource class)	Verifies that the owner of a job is allowed to read the JCL library specified in the job definition, and enforces the USER=job-statement
Starting a STC	$$STRSTC.qname.stcname	

CONTROL-M EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Submitting a job	If the job statement does not contain parameter USER=, USER=owner is added to the job statement. If parameter USER= exists on the job statement, the userid specified with this parameter is not the same as the owner, and parameter MSUBCHK is set to N, the job submission is canceled. ***NOTE:*** *The STIG standard is to set MSUBCHK to NO.*	parameter to match the specification made on the job order.
Accessing the Active Jobs List screen	$$CTMPNL3.*qname*	Verifies that the user is authorized to access the Job List screen and perform actions (e.g., rerun, hold, delete, etc.) on jobs displayed.

CONTROL-M EXTENDED DEFINITION SECURITY CALLS		
PROTECTED ELEMENT	*ENTITY NAME*	*DESCRIPTION*
Performing operations in the Job List screen	$$JOB1ACT.*qname.owner* $$JOB1SYS.*qname.owner* $$JOB1STA.*qname.owner* $$JOB1ZOO.*qname.owner* $$JOB1LOG.*qname.owner* $$JOB2HLD.*qname.owner* $$JOB2FRE.*qname.owner* $$JOB2FOK.*qname.owner* $$JOB2RRN.*qname.owner* $$JOB2CNF.*qname.owner* $$JOB3CHA.*qname.owner* $$JOB3PRI.*qname.owner* $$JOB3DEL.*qname.owner* $$JOB3EDI.*qname.owner*	
Performing refresh commands in the Job Dependency Network screen	$$REFNET.*qname* $$REFPROP.*qname* $$REFDEAD.*qname* $$REFALL.*qname*	

Use the following implementation and security recommendations for CONTROL-M:

(1) Install and maintain the CONTROL-M product software using SMP/E.

(2) Install CONTROL-M to use the resident ACP (ACF2, RACF, or TOP SECRET). Specify the ACP during the installation of IOA using the **SECURITY** option from the main ICE menu.

(1) Using ICE, specify the following STIG required values for the CONTROL-M security parameters for all ACP environments. Additional CONTROL-M security parameters with standard values specific to the ACP are documented in sections 14.3.3 (ACF), 14.4.3 (RACF), and 14.5.3 (TOP SECRET):

Table B-57. REQUIRED CONTROL-M SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS (14.2.3 b)

REQUIRED CONTROL-M SECURITY PARAMETERS FOR ALL ACP ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
DFMM01	Definition mode for security module CTMSE01	EXTEND
DFMM02	Definition mode for security module CTMSE02	EXTEND
DFMM08	Definition mode for security module CTMSE08	EXTEND

(4) CONTROL-M security exits are not modified by the site. If a modification is deemed necessary, it must be pre-approved by DISA FSO. A final source code review must be performed by DISA FSO prior to the implementation of the modified exit into a production environment.

(5) Access to the CONTROL-M resources listed in the *CONTROL-M EXTENDED DEFINITION SECURITY CALLS* table will be restricted to systems programmers, system operators, and production control staff.

With the granularity and flexibility Extended Definition mode provides, access authorization to CONTROL-M resources outside the system-level support realm may be permitted. For these authorized users, the following recommendations will be in effect:

- Access will be granted to specific individuals and not at the group level.
- Resource access rules will be fully qualified and not generic in nature.
- Justification documentation with IAO approval is required and must be filed with the IAO.

(6) Restrict access to CONTROL-M product data sets to system-level support personnel and IOA product suite of STCs. Authorized personnel include systems programmers, system operators, and production control staff. More specifically:

- *Alter* access to CONTROL-M product data sets will be restricted to systems programmers

- *Update* access to CONTROL-M Installation libraries will be restricted to the systems programmers

- *Update* access to CONTROL-M Operations and Repository libraries will be restricted to system-level support personnel and IOA product suite STCs

As noted in the previous item, access authorization to CONTROL-M resources outside the system-level support realm may be permitted. For these authorized users, the following recommendations will be in effect:

- Access will be granted to specific individuals and not at the group level.

- Data set access rules will be fully qualified and not generic in nature.

- *Update* access to CONTROL-M Repository and Operations files will be permitted and logged.

- Program pathing will be in effect to ensure data set access is performed using INCONTROL products.

- Justification documentation with IAO approval is required and must be filed with the IAO.

- *(ZIOA0010: CAT II) The IAO will ensure that IOA product data sets are protected in accordance with STIG requirements.*

- *(ZIOA0026: CAT II) The IAO will ensure that Control-M product security exits are installed and configured in accordance with STIG requirements.*
-
- *(ZIOA0038: CAT II) The IAO will ensure that Control-M Security parameter values are specified in accordance with STIG requirements.*

14.3 ACF2

The following sections define the ACF2 security requirements for the INCONTROL products.

14.3.1 IOA

In addition to the general security recommendations discussed in *Section 14.2.1*, the following items outline ACF2 specific recommendations for the IOA component:

(1) Using ICE, specify the following required standard values for the IOA security parameters on all ACF2 domains:

NOTE: Additional IOA security parameters with STIG standard values are required to be specified. These parameters and values are independent of the ACP and are referenced in the general IOA section (14.2.1).

Table B-58. REQUIRED IOA SECURITY PARAMETERS FOR ACF2 EIVIRONMENTS (14.3.1)

REQUIRED IOA SECURITY PARAMETERS FOR ACF2 ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
ACF2VER	Security product version and release. The STIG required value applies to ACF2 Version 6.1 and above. ***NOTE:*** This parameter is obsolete with IOA Version 6 and above.	6.1
IOACLASS	ACF2 resource class used by the IOA security interface for authority checks to INCONTROL protected elements.	IOAFAC
SAFSCLAS	ACF2 resource class used by the IOA security interface to check the user's authority to submit jobs on behalf of other users. ***NOTE:*** With the STIG required recommendations of Extended Definition security mode for all INCONTROL security exits and CONTROL-M parameter MSUBCHK set to NO, this process will not be in effect. However, this is a required IOA parameter and therefore must have a value.	SURROGAT

(2) If the IOA Online Monitor (IOAOMON) and VTAM Monitor (IOAVMON) are installed, define the logonids IOAOMON and IOAVMON for the started tasks of the same name with the following attributes:

MUSASS
NO-SMC
STC

(3) For ACF2 environments, the STIG recommended resource class is IOAFAC and the STIG recommended resource type is IOA for all INCONTROL product resources. Edit and customize member IOASSAF5 in the IOA INSTALL library. This member contains ACF2 commands that, by vendor default, translate the SAF resource class FACILITY to ACF2 resource type CMF. Change all instances of FACILITY to IOAFAC and CMF to IOA in member IOASSAF5.

Within the ACF2 database, define a CLASMAP record to translate resource class IOAFAC to resource type IOA. For example:

CLASMAP.IOA RESOURCE(IOAFAC) RSRCTYPE(IOA)

(4) Using specific and generic ACF2 resource rules for TYPE(IOA), protect all the IOA resources listed in the table in *Section 14.2.1, IOA*. At the minimum all resource rules must be defined to include the entire first node of the IOA resource it is protecting. All rules specify a default access of *prevent*.

Limit access to IOA resources as stated in *Paragraph (5)* of *Section 14.2.1, IOA*. Pay special attention to resources $$IOAONLINE and $$IOACMD as they control access to the IOA Online Facility and the issuing of operator commands respectively. For example:

$KEY($$IOAONLINE) TYPE(IOA)
qname UID(*user1*) ALLOW
UID(*sys-prog-grp*) ALLOW
UID(*ops-grp*) ALLOW
UID(*prod-cntl-grp*) ALLOW
- UID(-) PREVENT

$KEY($$ADDCND) TYPE(IOA)
qname.condition UID(*user1*)
UID(*prod-cntl-grp*) ALLOW
UID(*ops-grp*) ALLOW
- UID(-) PREVENT

$KEY($$IOACMD) TYPE(IOA)
S.- UID(*ops-grp*) LOG
qname.D.J.*myjobs*- UID(*user1*) ALLOW
D.J- UID(*prod-cntl-grp*) ALLOW
D.- UID(*sys-prog-grp*) ALLOW
D.- UID(*ops-grp*) ALLOW
- UID(-) PREVENT

(5) Protect all IOA product data sets using ACF2 data set rules. Limit access to IOA data sets as stated in *Paragraph 6, Section 14.2.1*. All rules specify a default access of *prevent*.

For authorized users outside the system-support realm access to IOA data sets is permitted using program pathing and logging. The following example permits user access to the IOA Conditions file only when using INCONTROL products:

$KEY(*sys2.ioa*)
-.*cnd* UID(*user1*) LIBRARY(*sys2a.ioa.loadlib*) PGM(IOA-)
READ(A) WRITE(L)
-.*cnd* UID(*user1*) LIBRARY(*sys2a.ioa.loadlib*) PGM(CTM-)
READ(A) WRITE(L)

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.3.2 CONTROL-O

In addition to the general security recommendations discussed in *Section 14.2.2*, the following items outline ACF2 specific recommendations for CONTROL-O:

(1) Define the logonids CONTROLO and CTOSRVxx for the started tasks of the same name with the following attributes:

MUSASS
STC
NO-SMC

(2) Using specific and generic ACF2 resource rules for TYPE(IOA), protect all the CONTROL-O resources listed in the table in *Section 14.2.2*. At the minimum all resource rules must be defined to include the entire first node of the CONTROL-O resource it is protecting. All rules specify a default access of *prevent*.

Limit access to CONTROL-O resources to systems programming personnel and operations personnel only. For example:

$KEY($$CTOORD) TYPE(IOA)
UID(*sys-prog-grp*) ALLOW
UID(*ops-grp*) ALLOW
- UID(-) PREVENT

(3) Protect all CONTROL-O product data sets using ACF2 data set rules. Limit access to CONTROL-O data sets to systems programming personnel and operations personnel only. All rules specify a default access of *prevent.*

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.3.3 CONTROL-M

In addition to the general security recommendations discussed in *Section 14.2.3*, the following items outline ACF2 specific recommendations for CONTROL-M:

(1) Using ICE, specify the following STIG required values for the CONTROL-M security parameters on all ACF2 domains:

NOTE: Additional CONTROL-M security parameters with STIG standard values are required to be specified. These parameters and values are independent of the ACP and are referenced in the general CONTROL-M *Section 14.2.3*.

Table B-59. REQUIRED CONTROL-M SECURITY PARAMETERS FOR ACF2 ENVIRONMENTS (14.3.3)

REQIRED CONTROL-M SECURITY PARAMETERS FOR ACF2 ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
MSUBCHK	Reject the submission of a job by CONTROL-M if the JCL contains the JOB card USER parameter and the owner ID of the job definition is not the same as the value specified in the USER parameter or //*JOBFROM.	NO
SAFJCARD	Add the USER parameter to the JOB statement of a job submitted by CONTROL-M if one does not exist.	U

(2) Define the logonids CONTROLM and CONTDAY for the started tasks of the same name with the following attributes:

MUSASS
NO-SMC
STC

(3) Using specific and generic ACF2 resource rules for TYPE(IOA), protect all the CONTROL-M resources listed in the table in *Section 14.2.3*. At the minimum all resource rules must be defined to include the entire first node of the CONTROL-M resource it is protecting. All rules specify a default access of *prevent*.

Limit access to CONTROL-M resources as stated in *Section 14.2.3, Paragraph (5)*. For example:

$KEY($$CTMPNL3) TYPE(IOA)
qname UID(*user1*) ALLOW
UID(*sys-prog-grp*) ALLOW
UID(*ops-grp*) ALLOW
UID(*prod-cntl-grp*) ALLOW
- UID(-) PREVENT

$KEY($$STCORD) TYPE(IOA)
UID(*sys-prog-grp*) ALLOW
UID(*ops-grp*) ALLOW
- UID(-) PREVENT

$KEY($$JOB1ACT)
qname.owner UID(*user1*)
UID(*prod-cntl-grp*)
- UID(-) PREVENT

(4) Protect all CONTROL-M product data sets using ACF2 data set rules. Limit access to CONTROL-M data sets as stated in *Paragraph 6, Section 14.2.3*. All rules specify a default access of *prevent*.

For authorized users outside the system-support realm access to CONTROL-M data sets is permitted using program pathing and logging. The following example permits a user access to the CONTROL-M Active Job file only when using INCONTROL products:

$KEY(*sys2.ioa*)
-.*ckp* UID(*user1*) LIBRARY(*sys2a.ioa.loadlib*) PGM(IOA-)
READ(A) WRITE(L)
-. *ckp* UID(*user1*) LIBRARY(*sys2a.ioa.loadlib*) PGM(CTM-)
READ(A) WRITE(L)

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.4 RACF

The following sections define the RACF security requirements for the INCONTROL products.

14.4.1 IOA

In addition to the general security recommendations discussed in *Section 14.2.1, IOA*, the following items outline RACF specific recommendations for the IOA component:

(1) Using ICE, specify the following STIG required values for the IOA security parameters on all RACF domains:

NOTE: Additional IOA security parameters with STIG standard values are required to be specified. These parameters and values are independent of the ACP and are referenced in *Section 14.2.1*, IOA (general IOA section).

Table B-60. REQUIRED IOA SECURITY PARAMETERS FOR RACF ENVIRONMENTS (14.4.1)

REQUIRED IOA SECURITY PARAMETERS FOR RACF ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
RACFVER	Security product version and release. The STIG required value applies to RACF Version 2.1 and above. ***NOTE:*** *This parameter is obsolete with IOA Version 6 and above.*	2.1
IOACLASS	RACF resource class used by the IOA security interface for authority checks to INCONTROL protected elements.	$IOA
RACSCLAS	RACF resource class used by the IOA security interface to check the user's authority to submit jobs on behalf of other users. ***NOTE:*** With the STIG requirement of Extended Definition Security mode for all INCONTROL security exits and CONTROL-M parameter MSUBCHK set to NO, this process will not be in effect. However, this is a required IOA parameter and therefore must have a value.	SURROGAT

(2) If the IOA Online Monitor (IOAOMON) and VTAM Monitor (IOAVMON) are installed, define the userids IOAOMON and IOAVMON for the started tasks of the same name. The Default Group for these userids is a group for INCONTROL product STCs only.

Define a matching profile for the IOAOMON and IOAVMON STCs to the STARTED resource class with no special attributes. For example:

```
RDEFINE STARTED IOAOMON.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))
RDEFINE STARTED IOAVMON.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))
```

(3) For RACF environments, the STIG recommended resource class is $IOA for all INCONTROL product resources. If not previously performed, the $IOA resource class must be added to the RACF Class Descriptor Table and the RACF Router Table. Use the following macro examples to add the $IOA resource class to RACF:

(a) Define the Class Descriptor Table entry:

```
ICHERCDE
    CLASS=$IOA,
    ID=n,
    MAXLNTH=39,
    POSIT=n,
    OTHER=ANY,
    RACLIST=ALLOWED,
    OPER=NO,
    DEFTUACC=NONE
```

(b) Define the Router Table entry:

```
ICHRFRTB
    CLASS=$IOA,
    ACTION=RACF
```

(4) Using specific and generic RACF resource profiles defined to the $IOA resource class, protect all the IOA resources listed in the table in *Section 14.2.1, IOA*. At the minimum all resource profiles must be defined to include the entire first node of the IOA resource it is protecting. All profiles specify a universal access of *none*.

Limit access to IOA resources as stated in *Section 14.2.1, Paragraph (5)*. Pay special attention to resources $$IOAONLINE and $$IOACMD as they control access to the IOA Online Facility and the issuing of operator commands respectively. For example:

```
RDEFINE $IOA $$IOAONLINE.** UACC(NONE)
RDEFINE $IOA $$IOAONLINE.qname UACC(NONE)

PERMIT $$IOAONLINE.** CLASS($IOA) ID(sys-prog-grp) ACCESS(READ)
PERMIT $$IOAONLINE.** CLASS($IOA) ID(ops-grp) ACCESS(READ)
PERMIT $$IOAONLINE.** CLASS($IOA) ID(prod-cntl-grp) ACCESS(READ)
PERMIT $$IOAONLINE.qname CLASS($IOA) ID(user1) ACCESS(READ)
PERMIT $$IOAONLINE.qname CLASS($IOA) ID(sys-prog-grp)
    ACCESS(READ)
PERMIT $$IOAONLINE.qname CLASS($IOA) ID(ops-grp) ACCESS(READ)
PERMIT $$IOAONLINE.qname CLASS($IOA) ID(prod-cntl-grp)
    ACCESS(READ)

RDEFINE $IOA $$ADDCND.** UACC(NONE)
```

RDEFINE $IOA $$ADDCND.*qname.condition** UACC(NONE)

PERMIT $$ADDCND.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$ADDCND.** CLASS($IOA) ID(*prod-cntl-grp*) ACCESS(READ)
PERMIT $$ADDCND.*qname.condition** CLASS($IOA) ID(*user1*)
ACCESS(READ)
PERMIT $$ADDCND.*qname.condition** CLASS($IOA) ID(*ops-grp*)
PERMIT $$ADDCND.*qname.condition** CLASS($IOA) ID(*prod-cntl-grp*)

RDEFINE $IOA $$IOACMD.** UACC(NONE)
RDEFINE $IOA $$IOACMD.S.** AUDIT(ALL) UACC(NONE)
RDEFINE $IOA $$IOACMD.D.** UACC(NONE)
RDEFINE $IOA $$IOACMD.D.J.** UACC(NONE)
RDEFINE $IOA $$IOACMD.D.J.*myjobs** UACC(NONE)

PERMIT $$IOACMD.S.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.** CLASS($IOA) ID(*sys-prog-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.J.** CLASS($IOA) ID(*prod-cntl-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.J.** CLASS($IOA) ID(*sys-prog-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.J.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$IOACMD.D.J.*myjob** CLASS($IOA) ID(*user1*)
ACCESS(READ)
PERMIT $$IOACMD.D.J.*myjob** CLASS($IOA) ID(*prod-cntl-grp*)
ACCESS(READ)
PERMIT $$IOACMD.D.J.*myjob** CLASS($IOA) ID(*sys-prog-grp*)
ACCESS(READ)
PERMIT $$IOACMD.D.J.*myjob** CLASS($IOA) ID(*ops-grp*)
ACCESS(READ)

(5) Protect all IOA product data sets using RACF data set profiles. Limit access to IOA data sets as stated in *Section 14.2.1, Paragraph (6)*. All profiles specify a universal access of *none*.

For authorized users outside the system-support realm access to IOA data sets is permitted using program pathing and logging.

(a) In order for program pathing to work, the IOA load library must be defined as a controlled library to RACF. For example:

RDEFINE PROGRAM ** UACC(READ)
ADDMEM('*sys2a.ioa.loadlib*'//NOPADCHK)

(b) Data set logging is specified in the RACF data set profile. Therefore a fully qualified data set profile must be defined to limit logging to the specific data set. For example, to enable update logging for the IOA Conditions file use the following command:

ADDSD '*sys2.ioa.cnd*' UACC(NONE) GENERIC AUDIT(ALL(UPDATE))

NOTE: There is no way to limit data set logging to only certain users such as authorized users outside the system-support realm.

(c) Permit user access to the IOA Conditions file only when using INCONTROL products. For example:

```
PERMIT 'sys2.ioa.cnd' ID(user1) ACCESS(UPDATE)
    WHEN(PROGRAM(IOATBMN,IOARKSL,IOACND))
PERMIT 'sys2.ioa.cnd' ID(user1) ACCESS(UPDATE)
    WHEN(PROGRAM(CTMCND,CTMRLR,CTMTWHY,CTMTSTA))
```

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.4.2 CONTROL-O

In addition to the general security recommendations discussed in *Section 14.2.2, CONTROL-O*, the following items outline RACF specific recommendations for CONTROL-O:

(1) Define the userids CONTROLO and CTOSRV*xx* for the started tasks of the same name. The Default Group for these userids is a group for INCONTROL product STCs only.

(2) Define a matching profile for the CONTROLO and CTOSRV*xx* STCs to the STARTED resource class with no special attributes. For example:

```
RDEFINE STARTED CONTROLO.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))
RDEFINE STARTED CTOSRVxx.* UACC(NONE) OWNER(admin)
    STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))
```

(3) Using specific and generic RACF resource profiles defined to the $IOA resource class, protect all the CONTROL-O resources listed in the table in *Section 14.2.2, CONTROL-O*. At the minimum all resource profiles must be defined to include the entire first node of the CONTROL-O resource it is protecting. All profiles specify a universal access of *none*.

Limit access to CONTROL-O resources to systems programming personnel and operations personnel only. For example:

```
RDEFINE $IOA $$CTOORD.** UACC(NONE)
```

PERMIT $$CTOORD.** CLASS($IOA) ID(*sys-prog-grp*) ACCESS(READ)
PERMIT $$CTOORD.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)

(4) Protect all CONTROL-O product data sets using RACF data set profiles. Limit access to CONTROL-O data sets to systems programming personnel and operations personnel only. All profiles specify a universal access of *none*.

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.4.3 CONTROL-M

In addition to the general security recommendations discussed in *Section 14.2.3, CONTROL-M*, the following items outline RACF specific recommendations for CONTROL-M:

(1) Using ICE, specify the following STIG required values for the CONTROL-M security parameters on all RACF domains:

NOTE: Additional CONTROL-M security parameters with STIG required values are to be specified. These parameters and values are independent of the ACP and are referenced in the general CONTROL-M section (*Section 14.2.3*).

Table B-61. REQUIRED CONTROL-M SECURITY PARAMETERS FOR RACF ENVIRONMENTS (14.4.3)

REQUIRED CONTROL-M SECURITY PARAMETERS FOR RACF ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
MSUBCHK	Reject the submission of a job by CONTROL-M if the JCL contains the JOB card USER parameter and the owner ID of the job definition is not the same as the value specified in the USER parameter.	NO
RACJCARD	Add the USER parameter to the JOB statement of a job submitted by CONTROL-M if one does not exist.	U

(2) Define the userids CONTROLM and CONTDAY for the started tasks of the same name. The Default Group for these userids is a group for INCONTROL product STCs only.

Utilize propagation control for both CONTROL-M started tasks. The following commands may be used to define the CONTROLM and CONTDAY STC userids to the PROPCNTL resource class:

RDEFINE PROPCNTL CONTROLM

RDEFINE PROPCNTL CONTDAY

The PROPCNTL resource class must be active and *RACLISTed* for this protection to be in effect. For example:

SETROPTS CLASSACT(PROPCNTL)
SETROPTS RACLIST(PROPCNTL)

(3) Define a matching profile for the CONTROLM and CONTDAY STCs to the STARTED resource class with no special attributes. For example:

RDEFINE STARTED CONTROLM.* UACC(NONE) OWNER(*admin*)
STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))
RDEFINE STARTED CONTDAY.* UACC(NONE) OWNER(*admin*)
STDATA(USER(=MEMBER) GROUP(STCIOA) TRUSTED(NO))

(4) Using specific and generic RACF resource profiles defined to the $IOA resource class, protect all the CONTROL-M resources listed in the table in *Section 14.2.3, CONTROL-M*. At the minimum all resource profiles must be defined to include the entire first node of the CONTROL-M resource it is protecting. All profiles specify a universal access of *none*.

Limit access to CONTROL-M resources as stated in *Section 14.2.3, Paragraph (5)*. For example:

RDEFINE $IOA $$CTMPNL3.** UACC(NONE)
RDEFINE $IOA $$CTMPNL3.*qname* UACC(NONE)

PERMIT $$CTMPNL3.** CLASS($IOA) ID(*sys-prog-grp*) ACCESS(READ)
PERMIT $$CTMPNL3.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$CTMPNL3.** CLASS($IOA) ID(*prod-cntl-grp*) ACCESS(READ)
PERMIT $$CTMPNL3.*qname* CLASS($IOA) ID(*user1*) ACCESS(READ)
PERMIT $$CTMPNL3.*qname* CLASS($IOA) ID(*sys-prog-grp*)
ACCESS(READ)
PERMIT $$CTMPNL3.*qname* CLASS($IOA) ID(*ops-grp*) ACCESS(READ)
PERMIT $$CTMPNL3.*qname* CLASS($IOA) ID(*prod-cntl-grp*)
ACCESS(READ)

RDEFINE $IOA $$STCORD.** UACC(NONE)

PERMIT $$STCORD.** CLASS($IOA) ID(*sys-prog-grp*) ACCESS(READ)
PERMIT $$STCORD.** CLASS($IOA) ID(*ops-grp*) ACCESS(READ)

RDEFINE $IOA $$JOB1ACT.** UACC(NONE)
RDEFINE $IOA $$JOB1ACT.*qname.owner* UACC(NONE)

PERMIT $$JOB1ACT.** CLASS($IOA) ID(*prod-cntl-grp*) ACCESS(READ)
PERMIT $$JOB1ACT.*qname.owner* CLASS($IOA) ID(*user1*) ACCESS(READ)
PERMIT $$JOB1ACT.*qname.owner* CLASS($IOA) ID(*prod-cntl-grp*)
ACCESS(READ)

(5) Protect all CONTROL-M product data sets using RACF data set profiles. Limit access to CONTROL-M data sets as stated in *Section 14.2.3, Paragraph (6)*. All profiles specify a universal access of *none*.

For authorized users outside the system-support realm access to CONTROL-M data sets is permitted using program pathing and logging.

(a) In order for program pathing to work, the IOA load library must be defined as a controlled library to RACF. For example:

RDEFINE PROGRAM ** UACC(READ)
ADDMEM('*sys2a.ioa.loadlib'*//NOPADCHK)

(b) Data set logging is specified in the RACF data set profile. Therefore a fully qualified data set profile must be defined to limit logging to the specific data set. For example, to enable update logging for the CONTROL-M Active Job file use the following command:

ADDSD '*sys2.ioa.ckp*' UACC(NONE) GENERIC AUDIT(ALL(UPDATE))

NOTE: There is no way to limit data set logging to only certain users such as authorized users outside the system-support realm.

(c) Permit user access to the CONTROL-M Active Job file only when using INCONTROL products. For example:

PERMIT '*sys2.ioa.ckp*' ID(*user1*) ACCESS(UPDATE)
WHEN(PROGRAM(CTMUCK,CTMTVEW,CTMTWHY,CTMTNET,
CTMTSTA,CTMAJF,CTMCAF,CTMCAJ,CTMBLD,CTMCDI,
CTMCHJ,CTMCOP,CTMEDA,CTMILY,CTMILU,
CTMFDO,CTMFRM,CTMJNL,CTMJOB,CTMRLR,
CTMTJRQC,CTMQSB,CTMCCR,IOATBMN,IOARKSL))

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.5 TOP SECRET

The following sections define the TOP SECRET security requirements for the INCONTROL products.

14.5.1 IOA

In addition to the general security recommendations discussed in *Section 14.2.1, IOA*, the following items outline TOP SECRET specific recommendations for the IOA component:

(1) Using ICE, specify the following STIG required values for the IOA security parameters on all TOP SECRET domains:

NOTE: Additional IOA security parameters with STIG standard values are required to be specified. These parameters and values are independent of the ACP and are referenced in the general IOA section (*Section 14.2.1*).

Table B-62. REQUIRED IOA SECURITY PARAMETERS FOR TOP SECRET ENVIRONMENTS (14.5.1)

REQUIRED IOA SECURITY PARAMETERS FOR TOP SECRET ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
TSSVER	Security product version and release. The STIG required value applies to TOP SECRET Version 5.0 and above. ***NOTE:*** This parameter is obsolete with IOA Version 6 and above.	5.0
IOACLASS	TOP SECRET resource class used by the IOA security interface for authority checks to INCONTROL protected elements.	IOA
TSSSCLAS	TOP SECRET resource class used by the IOA security interface to check the user's authority to submit jobs on behalf of other users. ***NOTE:*** With the STIG requirement recommendations of Extended Definition Security mode for all INCONTROL security exits and CONTROL-M parameter MSUBCHK set to NO, this process will not be in effect. However, this is a required IOA parameter and therefore must have a value.	SURROGAT

(2) Define IOA as a Facility to TOP SECRET in the Facility Matrix table using the following example:

FACILITY(USER*xx*=NAME=IOA)
FACILITY(IOA=MODE=FAIL,ACTIVE,SHRPRF,SIGN(S))
FACILITY(IOA=PGM=IOA,ASUBM,NOABEND,NOXDEF)
FACILITY(IOA=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW)
FACILITY(IOA=NORNDPW,NOAUDIT,NOTSOC)

- *(ZIOAT060: CAT II) IOA will be defined to TOP SECRET in the Facility Matrix Table using the above parameters.*

(3) If the IOA Online Monitor (IOAOMON) and VTAM Monitor (IOAVMON) are installed, define the ACIDs IOAOMON and IOAVMON for the started tasks of the same name.

TSS CREATE(IOAOMON) NAME('IOA ONLINE MONITOR')
TYPE(USER) DEPT(*dept-acid*) PASS(*password*,0) FAC(STC)
MASTFAC(IOA) SOURCE(INTRDR)

TSS CREATE(IOAVMON) NAME('IOA VTAM MONITOR')
TYPE(USER) DEPT(*dept-acid*) PASS(*password*,0) FAC(STC)
MASTFAC(IOA) SOURCE(INTRDR)

Define the IOA started tasks to TOP SECRET.

TSS ADD(STC) PROCNAME(IOAOMON) ACID(IOAOMON)
TSS ADD(STC) PROCNAME(IOAVMON) ACID(IOAVMON)

(4) For TOP SECRET environments, the STIG recommended resource class is IOA for all INCONTROL product resources. If not previously performed, the IOA resource class must be added to the TOP SECRET Resource Definition Table (RDT). Use the following command example to add the IOA resource class to the RDT:

TSS ADD(RDT) RESCLASS(IOA) RESCODE(*xx*) ATTR(LONG,DEFPROT)
DEFACC(NONE) ACLST(NONE,READ,SCRTCH,UPDATE,ALL)

(5) Protect all the IOA resources listed in the table in *Section 14.2.1, IOA*, using TOP SECRET. Assign ownership of the IOA resources specifying the appropriate department ACID and IOA resource class. For example:

TSS ADD(*security-dept-acid*) IOA($$)

NOTE: This example assigns ownership of all INCONTROL product resources.

Using specific and generic TOP SECRET permissions, limit access to IOA resources as stated in *Section 14.2.1, Paragraph (5)*. At the minimum all resource permissions must be defined to include the entire first node of the IOA resource it is protecting. Default access to IOA resources is not allowed. Pay special attention to resources $$IOAONLINE and $$IOACMD as they control access to the IOA Online Facility and the issuing of operator commands respectively. For example:

TSS PERMIT(*sys-prog-grp*) IOA($$IOAONLINE) ACCESS(READ)
TSS PERMIT(*ops-grp*) IOA($$IOAONLINE) ACCESS(READ)
TSS PERMIT(*prod-cntl-grp*) IOA($$IOAONLINE) ACCESS(READ)
TSS PERMIT(*user1*) IOA($$IOAONLINE.*qname*) ACCESS(READ)

TSS PERMIT(*ops-grp*) IOA($$ADDCND) ACCESS(READ)
TSS PERMIT(*prod-cntl-grp*) IOA($$ADDCND) ACCESS(READ)
TSS PERMIT(*user1*) IOA($$ADDCND.*qname.condition*) ACCESS(READ)

TSS PERMIT(*ops-grp*) IOA($$IOACMD.S.) ACCESS(READ)
TSS PERMIT(*sys-prog-grp*) IOA($$IOACMD.D.) ACCESS(READ)
TSS PERMIT(*ops-grp*) IOA($$IOACMD.D.) ACCESS(READ)
TSS PERMIT(*prod.cntl-grp*) IOA($$IOACMD.D.J.) ACCESS(READ)
TSS PERMIT(*user1*) IOA($$IOACMD.D.J.*myjob*) ACCESS(READ)

(6) Protect all IOA product data sets using TOP SECRET. Limit access to IOA data sets as stated in *Section 14.2.1, Paragraph (6)*. Default access is not allowed.

For authorized users outside the system-support realm access to IOA data sets is permitted using program pathing and logging. The following example permits user access to the IOA Conditions file only when using INCONTROL products:

TSS PERMIT(*user1*) DSNAME('*sys2.ioa.cnd*') ACCESS(UPDATE)
PRIVPGM(IOA(G), CTM(G)) LIBRARY('*sys2a.ioa.loadlib*')
ACTION(AUDIT)

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.5.2 CONTROL-O

In addition to the general security recommendations discussed in *Section 14.2.2, CONTROL-O*, the following items outline TOP SECRET specific recommendations for CONTROL-O:

(1) Define CONTROLO as a Facility to TOP SECRET in the Facility Matrix table using the following example:

```
FACILITY(USERxx=NAME=CONTROLO)
FACILITY(CONTROLO=MODE=FAIL,ACTIVE,SHRPRF,SIGN(S))
FACILITY(CONTROLO =PGM=CTO,ASUBM,NOABEND,NOXDEF)
FACILITY(CONTROLO=ID=nn,MULTIUSER,RES,LUMSG,STMSG)
FACILITY(CONTROLO =NORNDPW,NOAUDIT,NOTSOC,WARNPW)
```

(2) Define the ACIDs CONTROLO and CTOSRV*xx* for the started tasks of the same name.

```
TSS CREATE(CONTROLO) NAME('CONTROLO MONITOR') TYPE(USER)
    DEPT(dept-acid)   PASS(password,0) FAC(STC)
MASTFAC(CONTROLO) SOURCE(INTRDR)

TSS CREATE (CTOSRVxx) NAME(CONTROLO SERVER) TYPE(USER)
    DEPT(dept-acid)   PASS(password,0) FAC(STC)
        SOURCE(INTRDR)
```

- *(ZIOAT060: CAT II) IOA will be defined to TOP SECRET in the Facility Matrix Table using the above parameters.*

(3) Define the CONTROL-O started tasks to TOP SECRET.

```
TSS ADD(STC) PROCNAME(CONTROLO) ACID(CONTROLO)
TSS ADD(STC) PROCNAME(CTOSRVxx) ACID(CTOSRVxx)
```

(4) Protect all the CONTROL-O resources listed in the table in *Section 14.2.2, CONTROL-O*, using TOP SECRET. Assign ownership of the CONTROL-O resources specifying the appropriate department ACID and IOA resource class. For example:

```
TSS ADD(security-dept-acid) IOA($$)
```

NOTE: This example assigns ownership of all INCONTROL product resources.

Using specific and generic TOP SECRET permissions, limit access to CONTROL-O resources to systems programming personnel and operations personnel only. At the minimum all resource permissions must be defined to include the entire first node of the CONTROL-O resource it is protecting. Default access to CONTROL-O resources is not allowed. For example:

TSS PERMIT(*sys-prog-grp*) IOA($$CTOORD) ACCESS(READ)
TSS PERMIT(*ops-grp*) IOA($$CTOORD) ACCESS(READ)

(5) Protect all CONTROL-O product data sets using TOP SECRET. Limit access to CONTROL-O data sets to systems programming personnel and operations personnel only. Default access is not allowed.

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

14.5.3 CONTROL-M

In addition to the general security recommendations discussed in *Section 14.2.3, CONTROL-M*, the following items outline TOP SECRET specific recommendations for CONTROL-M:

(1) Using ICE, specify the following STIG required values for the CONTROL-M security parameters on all TOP SECRET domains:

NOTE: Additional CONTROL-M security parameters with STIG required values are to be specified. These parameters and values are independent of the ACP and are referenced in *Section 14.2.3, CONTROL-M* (the general CONTROL-M section).

Table B-63. REQUIRED CONTROL-M SECURITY PARAMETERS FOR TOP SECRET ENVIRONMENTS (14.5.3)

REQUIRED CONTROL-M SECURITY PARAMETERS FOR TOP SECRET ENVIRONMENTS		
OPTION	*DESCRIPTION*	*REQUIRED VALUE*
MSUBCHK	Reject the submission of a job by CONTROL-M if the JCL contains the JOB card USER parameter and the owner ID of the job definition is not the same as the value specified in the USER parameter.	NO
TSSJCARD	Add the USER parameter to the JOB statement of a job submitted by CONTROL-M if one does not exist.	U

(2) Define CONTROLM as a Facility to TOP SECRET in the Facility Matrix table using the following example:

FACILITY(USER*xx*=NAME=CONTROLM)
FACILITY(IOA=MODE=FAIL,ACTIVE,SHRPRF,SIGN(S))
FACILITY(IOA=PGM=CTM,ASUBM,NOABEND,NOXDEF)
FACILITY(IOA=ID=*nn*,MULTIUSER,RES,LUMSG,STMSG,WARNPW)
FACILITY(IOA=NORNDPW,NOAUDIT,NOTSOC)

- *(ZIOAT060: CAT II) IOA will be defined to TOP SECRET in the Facility Matrix Table using the above parameters.*

(3) Define the ACIDs CONTROLM and CONTDAY for the started tasks of the same name.

TSS CREATE(CONTROLM) NAME('CONTROLM MONITOR') TYPE(USER)
DEPT(*dept-acid*) PASS(*password*,0) FAC(STC) MASTFAC(CONTROLM)
SOURCE(INTRDR)

TSS CREATE(CONTDAY) NAME(NEW DAY PROC) TYPE(USER)
DEPT(*dept-acid*) PASS(*password*,0) FAC(STC)
SOURCE(INTRDR)

Utilize propagation control for both CONTROL-M started tasks. The following commands may be used to define the CONTROLM and CONTDAY STC ACIDs to the PROPCNTL resource class:

TSS ADD(*deptacid*) PROPCNTL(CONTROLM)
TSS ADD(*deptacid*) PROPCNTL(CONTDAY)

(4) Define the CONTROL-M started tasks to TOP SECRET.

TSS ADD(STC) PROCNAME(CONTROLM) ACID(CONTROLM)
TSS ADD(STC) PROCNAME(CONTDAY) ACID(CONTDAY)

(5) Protect all the CONTROL-M resources listed in the table in *Section 14.2.3, CONTROL-M*, using TOP SECRET. Assign ownership of the CONTROL-M resources specifying the appropriate department ACID and IOA resource class. For example:

TSS ADD(*security-dept-acid*) IOA($$)

NOTE: This example assigns ownership of all INCONTROL product resources.

Using specific and generic TOP SECRET permissions, limit access to CONTROL-M resources as stated in *Section 14.2.3, CONTROL-M, Paragraph (5)*. At the minimum all resource permissions must be defined to include the entire first node of the CONTROL-M resource it is protecting. Default access to CONTROL-M resources is not allowed. For example:

TSS PERMIT(*sys-prog-grp*) IOA($$CTMPNL3) ACCESS(READ)
TSS PERMIT(*ops-grp*) IOA($$CTMPNL3) ACCESS(READ)
TSS PERMIT(*prod-cntl-grp*) IOA($$CTMPNL3) ACCESS(READ)
TSS PERMIT(*user1*) IOA($$CTMPNL3.*qname*) ACCESS(READ)

TSS PERMIT(*sys-prog-grp*) IOA($$STCORD) ACCESS(READ)
TSS PERMIT(*ops-grp*) IOA($$STCORD) ACCESS(READ)

TSS PERMIT(*prod-cntl-grp*) IOA($$JOB1ACT) ACCESS(READ)
TSS PERMIT(*user1*) IOA($$JOB1ACT.*qname.owner*) ACCESS(READ)

(6) Protect all CONTROL-M product data sets using TOP SECRET. Limit access to CONTROL-M data sets as stated in *Section 14.2.3, CONTROL-M, Paragraph (6)*. Default access is not allowed.

For authorized users outside the system-support realm access to CONTROL-M data sets is permitted using program pathing and logging. The following example permits a user access to the CONTROL-M Active Job file only when using INCONTROL products:

TSS PERMIT(*user1*) DSNAME('*sys2.ioa.ckp*') ACCESS(UPDATE)
PRIVPGM(IOA(G), CTM(G)) LIBRARY('*sys2a.ioa.loadlib*')
ACTION(AUDIT)

- *(ZIOA0040: CAT II) The IAO will ensure that IOA product resources are protected in accordance with STIG requirements.*

- *(ZIOA0050: CAT II) The IAO will ensure that IOA product started tasks are defined in accordance with STIG requirements.*

15. WEB APPLICATION SERVICES

15.1 Overview

With the increased usage of the Internet and the migration to Open Systems, the role of the mainframe has changed. Mainframes not only support the tremendous processing requirements of legacy systems, but also serve as large repositories of data. Mainframe architecture and technology has changed. Mainframes are able to run the UNIX operating system and applications written in C and JAVA are supported.

Mainframes still provide a safe environment for processing sensitive systems and are becoming more and more reliable in up time performance. This section addresses Web applications and the systems software used to support their requirements.

15.2 WebSphere Application Server

15.2.1 Overview

WebSphere is a set of IBM software products designed to enable the development, implementation, and management of web sites, web applications, and enterprise wide applications. Although there are three different versions of WebSphere, the WebSphere Application Standard Edition and the WebSphere Application Enterprise Edition are designed to run on OS/390 platforms. (Under z/OS, both the standard and enterprise editions are merged to form WebSphere Version 4.0.1 for z/OS.)

The WebSphere Application Server (WAS) Standard Edition V3.5 is a Java application server plug-in to the IBM HTTP server that uses the HTTP address space. When WebSphere is installed, the HTTP configuration file is modified to enable the web server to redirect certain requests to WebSphere for processing.

In a WebSphere environment, WAS is automatically started and shutdown when the HTTP web server is started and stopped. The HTTP web server is responsible for providing the communications link between browser-based applications and the application server. WAS provides the run-time environment for enterprise beans, handles low-level programming tasks, and interfaces with the OS/390 resources such as CICS and the databases.

WebSphere makes use of the Java development kit (JDK) and the JAVA Run-Time Environment (JRE) to execute Java programs and web applications. (Also, it provides support for the creation of an active web site and basic web applications.)

Whenever HTTP clients access web applications, they enter through the HTTP web server using TCP/IP. The types of web server resources they access are HTML, images, and Common Gateway Interface (CGI) programs. Java clients access WebSphere resources using Internet Inter ORB Protocol (IIOP). WebSphere resources include Enterprise Java Beans (EJBs), servlets, and Java Server Pages (JSPs). IIOP enables Java clients to locate and use objects across platforms written in a variety of languages. IIOP is based on the Common Object Request Broker Architecture CORBA industry standard.

The primary differences between the advanced edition and the standard edition are the support for Enterprise Java Bean development, multiple server support, and additional features provided by the WebSphere administration application. The Enterprise edition encompasses all of the features of both the standard and advanced editions.

NOTE: This section primarily addresses WebSphere Application Server Standard Edition V3.5 for OS/390. Wherever possible, WebSphere 4.0.1 for z/OS differences will be noted.

- *The web server application software and the WebSphere application server software will be a version supported by the vendor and appropriate to the host operating system of the server.*

- *Web server resources will be protected in accordance with the Web and appropriate platform STIGs.*

- *WebSphere Application Server resources will be protected in accordance with the Web and appropriate platform STIGs.*

- *The Web Manager or SA will ensure that before installing the web server application, the server host platform operating system will be configured in accordance with the appropriate STIG.*

- *The Web Manager or SA will ensure the WebSphere Application Server is configured such that a user cannot traverse from a document directory to a directory that does not contain web content.*

- *The Web Manager or SA will ensure that each readable web document directory contains a default, home, index, or equivalent file.*

- *The Web Manager or SA will ensure that the server root directory is not NFS mountable or sharable in the case of an NT server.*

- *When using Java Servlets Engines or Java Server Pages, any sample files that accompany the product's installation will be removed.*

- *When using Java Server Pages (JSPs), the IAO will ensure that all user-provided input is checked for malicious code.*

15.2.2 General Security Considerations

The WebSphere Application Server Standard Edition V3.5 does not interface with OS/390 security. It depends on the HTTP web server to perform this function. In addition, WebSphere security is designed to sit on top of and compliment the operating system, Java-language, and CORBA and EJB security. Under WebSphere V4.0.1 for z/OS the WebSphere Application Server interfaces with the ACP.

The WebSphere Application Server provides security components that collaborate with other elements to secure a WebSphere environment. Security is established at two levels. The first level is global security. Global security applies to all applications running in the environment. Global values are specified in the *admin.config* file.

The second level of security is application security. Application security can vary from userid/password to PKI or a combination of both. In some cases, these values can override global defaults. WAS values are specified in the *was.config* file. The WebSphere Administrative Console is used to maintain the *admin.config* and the *was.config* files.

Security can be applied to applications and to individual resources. Setting up security involves the following general steps:

1. Setting global values for use by all applications.
2. Refining settings for individual applications.
3. Securing specific HTTP and EJB methods. This may be optional.

- *The IAO and IAM, in coordination with the SA and Web Manager, will be responsible for ensuring that all IAVA bulletins are responded to within the specified time period.*

- *The Web Manager or SA will ensure that before installing the web server application, the server host platform operating system will be configured in accordance with the appropriate STIG.*

- *The Web Manager or SA will ensure that users do not have access to the JAVA development kit compiler in a production environment.*

- *The IAO will ensure that in the case of web applications or java clients, services will, at a minimum, restrict the userid and password. Shared user accounts are not authorized.*

- *The IAO will ensure that the web server password and the WebSphere application server password are entrusted to the SA or Web Manager.*

- *The IAO will ensure that the web server and the application services passwords are changed at least annually.*

- *Development servers will comply with the recommendations set forth in the Web Server STIG and the appropriate platform STIG.*

- *Remote authors or content providers will not be able to upload files to the Document Root directory without the use of a secure logon and a secure connection.*

- *The IAO will ensure that the admin.config file is password protected and access is restricted to authorized personnel.*

- *The IAO will ensure that the was.config file is password protected and its access is restricted to authorized personnel.*

- *The IAO will ensure that the WebSphere Administrative console is restricted to authorized personnel. Restrictions will be applied in accordance with the appropriate STIG.*

Within the WebSphere Application Server, security requirements are defined in terms of:

1. Resources:

   Files or programs that require restricted access. They belong to an application and the methods are associated with method groups. Web pages, enterprise beans, servlets, and JSP files are examples of resources.

2. Applications:

   A collection of resources that encapsulates a piece of business logic. Web applications (a group of servlets) and enterprise applications (a collection of Web applications) are examples of applications.

- *Uniform Resource Identifier (URI) resources will be protected in accordance with the Web Server STIG.*

- *The HelloWorld servlet will be removed from the server.*

- *Enterprise bean resources will be restricted by home and in accordance with the Web Server STIG and the appropriate platform STIG. (An Enterprise JAVA Bean is a cross platform component that enables the development and deployment of JAVA applications.)*

- *Authentication and authorization policies for enterprise applications will be defined by the Web Administrator.*

Applications can be secured by completing the following steps:

1. Identify the users who are given access to the application.
2. Identify which methods an application is authorized to use.
3. Develop WebSphere policies that reflect Steps 1 and 2, and load them into WebSphere.
4. Update the ACP rules in the ACP database.

- *Users will be required, at a minimum, to access WebSphere applications by the userid and password. Applications will specify this as Basic mode for application security.*

- *Application userids and passwords will not be shared.*

- *Security IDs will be assigned to realms.*

15.2.3 Specific Security Considerations

WebSphere Application Server Standard Edition V3.5 security complements operating system, Java-language, and CORBA and EJB security. Each of the above provides a security layer that has been addressed in other STIGs (i.e., Web, UNIX, NT). WebSphere provides an administration/security application and an administrative console to address WebSphere security.

NOTE: Because the architecture of the OS/390 system and security is different from the mid-tier platforms, some of the guidelines specified in the mid-tier STIGs may not apply. In that case, this section identifies the guideline.

15.2.3.1 WebSphere Security Application

The WebSphere Security Application is a security runtime consisting of two components: the security plug-in and the security collaborator. The security plug-in is attached to the HTTP web server and is used to control access to web resources such as HTML files and servlets. The security collaborator is attached to the application server and is used to control access to methods calls hosted by WAS.

Requests are submitted to WebSphere either through the HTTP server or through the application server. The type of client and request determines whether the HTTP server or the WebSphere application server processes the request. Web client requests are submitted through the HTTP web server. Java clients submit requests through the application server. Both servers utilize the security application and repository to determine authentication and authorization.

Whenever a web client submits a request to the HTTP server, the service directives within the Web server's httpd.conf file indicate which requests the Application Server is to process. If the requested URL matches a URL or URL pattern specified in a directive in the httpd.conf file, the request is routed to the application server. The Application Server then uses the webapp.webapp-name property in the was.config file to determine to which web application the request should be routed.

Whenever a request is to be submitted to the application server by a Java client, the client is prompted for a userid and password. The security collaborator authenticates the information against the user registry. If the user is authorized, the method invocation request is authenticated against the security policies as specified in security application repository. (The repository can be a DB2 database or an LDAP directory.) The method is then executed and the results passed back to the client.

- *The IAO or IAM will verify that local policies have been developed to ensure that all DOD originated information posted to the Internet and/or Intranet (i.e., Open and/or Limited or Certificate-based web servers) is reviewed and approved by the respective Deputy Director or Commander and as needed by the Public Affairs Officer (PAO).*

- *The IAO or IAM will verify that local policies have been developed to ensure that all information that is hosted on a its site, which originated from a DOD or other Federal organization, has been reviewed and approved for posting by the originating organization according to the Web Site Administration Policies and Procedures, dated 25 November 1998.*

- *The IAO or IAM will verify that the approval of the Chief Information Officer (CIO) is obtained prior to entering into any agreements with commercial Internet service providers or non-DOD web hosting services.*

- *A Web Manager and a System Administrator will be appointed for each web server and administration server on the OS/390 platform. (The Web Manager may be an additional duty or a separate role.)*

- *The httpd.conf and was.config files will be protected in accordance with requirements as specified in the Web Server STIG, the UNIX STIG, and the Windows Addendum.*

- *The SA or Web Manager will ensure that the web server is configured to use a local or related .mil DNS service.*

- *An Open web server will be isolated in accordance with the Enclave Security Instruction dated 30 March 2001. That is to say, an open web server will be on a separate public enclave (subnet), isolated from the internal systems.*

- *An Open web server will not allow, or be allowed, a trust relationship with any asset that is not also in a separate public enclave.*

- *A Limited or Certificate-based web server will be located inside the premise router or site firewall.*

- *The Web Manager or SA will ensure that utility/productivity programs, development tools, and system files (both operating system and WebSphere/HTTP files) are not accessible through the production web and application servers.*

- *The Web Manager will ensure the web and application servers are configured such that a user cannot traverse from a document directory to a directory that does not contain web/application content.*

- *The Web Manager will ensure that each readable web/application document directory contains a default, home, index, or equivalent file.*

- *Remote administration of an OS/390 WebSphere security application server will not be allowed.*

- *The IAO will ensure that access to the web and WebSphere administration tools are restricted to the Web Manager, SA, and/or the Web/SA Manager's designees.*

- *The IAO will ensure that the SA or Web Manager performs all administrative tasks through a secure path.*

- *Web/JAVA users, either anonymous or authenticated, will have their access restricted to web/application document (content) directories on the web and application servers.*

- *The Web Manager or SA will ensure that logs of web/application server access and errors are established and maintained.*

- *The IAO will ensure that the auditors are the only users with greater than read access to log files. This will not apply to the active log files.*

15.2.3.2 WebSphere Security Components

As mentioned earlier, security in the WebSphere Application Server Standard Edition is a collaborative effort between the WebSphere security application and the security runtime. Security policies for Web resources and enterprise beans are configured using the security application that resides on the WebSphere administrative server. Security for the WebSphere Application Server product is managed as a collaborative effort by the following components distributed throughout WebSphere Application Server:

Security server:

The security server controls security policies and provides authentication and authorization services. The run-time components enforce these policies. In essence, the security server acts as a trusted third-party for security policy and control. The runtime components consult the security server for policy information and for services such as authentication and authorization, including token services for Lightweight Third Party Authentication (LTPA). The security server uses persistent storage (such as a DB2 database) to store its configuration information.

Security collaborator:

The security collaborator is a component of the application server process. It acts as a common runtime environment for servlets, Java Server Pages (JSP) files, and enterprise beans. When a Java client attempts to invoke a method on a servlet or an enterprise bean, the security collaborator performs the authorization checking in conjunction with the security server.

Security plug-in:

The security plug-in resides with the Web server and protects access to HTML pages served by the Web server. The security collaborator interfaces with the ACP security server to perform userid and password authentication. When a Web resource is protected by WebSphere Application Server security, the security plug-in consults the security server for authentication and authorization services. If a client is authorized to use a URL, the plug-in sets up a security context for the client, including the security credentials, and passes the request to the servlet engine in the application server.

- *The IAO will ensure that Uniform Resource Identifier (URI) resources will be protected in accordance with the Web Server STIG.*

- *The IAO will ensure that the HelloWorld servlet will be removed from the server.*

- *The IAO will ensure that Enterprise beans resource will be restricted by home and in accordance with the Web Server STIG and the appropriate platform STIG.*

- *The Web Administrator will define the authentication and authorization policies for enterprise applications.*

- *The Web Manager will ensure that each readable web/application document directory contains a default, home, index, or equivalent file.*

- *The IAO will ensure that remote administration of an OS/390 WebSphere security application server will not be allowed.*

- *The IAO will ensure that access to the web and WebSphere administration tools are restricted to the Web Manager, SA, and/or the Web/SA Manager's designees.*

- *The IAO will ensure that the SA or Web Manager performs all administrative tasks through a secure path.*

- *Web/JAVA users, either anonymous or authenticated, will have their access restricted to web/application document (content) directories on the web and application servers.*

- *The Web Manager or SA will ensure that logs of web/application server access and errors are established and maintained.*

- *The IAO will ensure that the auditors are the only users with greater than read access to log files. This will not apply to the active log files.*

- *The IAO will ensure that the WebSphere Administrative Console is restricted to authorized personnel.*

- *The Web Manager or SA will ensure that the IBM WebSphere default administrator ID CBADMIN is not used. This includes the removal of the CBADMIN user ID from all appropriate configuration files. Additionally, the IAO will ensure that the CBADMIN user account is removed or not defined to the ACP.*

- *(ZWAS0040: CAT I /CAT II) The IAO will ensure that the CBADMIN user account is removed or not defined to the ACP.*

15.2.3.3 WebSphere Administrative Console

The WebSphere Administrative Console (WAC) is used to control the WebSphere Administrative Application. The WebSphere Administrative Application runs on the WebSphere Application Server. It can be used for configuring resources, setting security policies, identifying and responding to system failures, and monitoring usage patterns. Changes are applied to the administrative domain's configuration. Access to the wizards is based on the role being performed.

During installation of the WebSphere Application Server, an initial administrative account is created. This account is the only one authorized to administer WebSphere. Other administrator accounts can be created at a later time.

To authorize other administration accounts perform the following:

1. Define the user in the operating system user registry or in the LDAP directory service.

2. Use the Assign Permissions task in the Security Task Group to authorize the user access to the protected functions. The functions are listed in the format AdminApplication-function_name in the task.

NOTE:
- On UNIX platforms use the root account.
- On Windows, the WebSphere administrator account must be a member of the Windows Administrators group and must have the rights to "Log on as a service" and to "Act as part of the operating system."
- On Windows 2000, the WebSphere administrator account must be a member of the Windows 2000 Administrators group and must have the rights to "Log on as a service" and to "Act as part of the operating system."
- If using an LDAP directory service for authentication, then the process identity does not require any special privileges.
- Remote authors or content providers will not be able to upload files to the Document Root directory without the use of a secure logon and secure connection.
- Administrators must be limited to a minimal number of userids.
- Resource controls as specified in the appropriate STIG, (i.e., Database) will be restricted in accordance with the Resource STIG.
- The IAO will ensure that the appropriate class restrictions and file permissions are enforced for the servers and data sets.

17.2.3.4 Changing Passwords for Administrative Accounts

Passwords for administrative accounts are changed on a regular basis as specified in the *Web Server STIG* and appropriate platform STIG. In order to do this, the passwords have to be changed in two places, and in a particular order. If this is done incorrectly, it can create a situation in which the WebSphere administrative server cannot restart. The following steps describe the procedures for changing WebSphere Administrative Account passwords and the order in which to apply the changes.

Steps:

1. Make sure the WebSphere administrative server is running. This is crucial. Do not change an administrative password unless the server is running.

2. Change the password in the user registry by using the utility for the operating system or LDAP service.

3. Log on to the WebSphere administrative console using the new password. Attempts to use the old password will fail.

4. Change to Global Settings User Registry in the administrative console.

5. Change the password for the administrative user to the new password.

6. Stop and restart the administrative server.

- *Remote administration of an OS/390 WebSphere application server will not be allowed.*

- *The IAO will ensure that a Web Server Administration ID and its ACP group are established.*

- *The IAO will ensure that a unique user ID is created for each instance of the web server. Refer to Section H.3.1.1, Web Server Identification, of the Web Server STIG for requirements regarding web server user IDs.*

- *The IAO will restrict the anonymous access userid (PUBLIC) as it is specified in the Web Server STIG.*

- *Program control will be used to restrict access to authorized libraries.*

15.2.3.5 WebSphere Application Server Data Sets

Some of the vendor-supplied components of WebSphere for OS/390 are stored in data sets as follows:

- Distribution data sets hold the master copy of the product's elements. There is no typical need for general users to access these data sets. The standard naming convention for these data sets is to use the prefix SYS1.

  Target data sets hold the execution copy of the product's elements. General users may require *read* access to some of these data sets.

The following table describes the products and data sets that interface with WebSphere V3.5:

PRODUCT	*DATA SET PREFIX*
WebSphere	SYSX.EJS.V3500108
Java	SYSX.OE.* and SYS2.JAVA*
DB2	SYSX.DB2.V710107
	SYSX.DB2.V710107
LDAP	SYSX.GLD SYSX.GLD

- *Update and alter access to product data sets will be restricted to systems programming personnel.*

- *Systems programming personnel will be given read access to facility BPX.FILEATTR.PROGCTL in order to provide ongoing maintenance support.*

The WebSphere Application Server uses the contents of the following libraries for resolving link edits for the WebSphere Application Server. The following list identifies the libraries as provided by IBM.

SYS1.CSSLIB
SYS1.LE.SCEELKED
SYS1.LE.SCEELKEX
SYS1.LE.SCEEOBJ

* *Read-only* access is given to WebSphere.

The following describes the data set prefix used for WebSphere V4.0.1:

SYS2.WAS.V401.xxxxxxx

- *(ZWAS0010: CAT II) The IAO will ensure that WebSphere server data sets restrict UPDATE and/or ALLOCATE access to systems programming personnel.*

15.2.3.6 WebSphere Application Server Files and Tables

The WebSphere Application Server accesses multiple files and tables during execution. These files provide WAS with the information necessary to determine how the Application Server handles Web applications deployed within it. The following table lists files that are used by WebSphere and a description of each:

WEBSPHERE/OS/390 CONFIGURATION FILES	
FILE	*USAGE*
httpd.conf	Web Server main configuration files
httpd.envvars	Web Server environment variables
mvsds.conf	MVSDS function config file
ics_pics.conf	PICS Rating file
javelin.conf	Web Traffic Express (Proxy) config file
socks.conf	Another Proxy config file
lgw_fcgi.conf	Fast CGI config file
IMWSendMail.cfg	"old" SendMail config file

- *(ZWAS0020: CAT II) The IAO will ensure that the above configurations are protected in accordance with the Web Server STIG, the UNIX STIG, and OS/390 STIG guidelines. Access will be restricted to authorized personnel.*

- *The WebSphere Application Server files will have permissions of owner: read/write, group: read, and others: none (640) or more restrictive (configuration files need only read permission), where the group is the SA or Web Manager account that controls the web service.*

- *The Web server files will be protected in accordance with the Web Server STIG guidelines.*

As mentioned earlier the admin.config file contains global values. This file is maintained by the WebSphere Administration Application. Because this file contains passwords, it must be restricted from view from non-authorized personnel. The following table is a layout of the property files.

PROPERTY FILES CONTAINING PASSWORDS		
PROPERTY FILES	*TYPE OF PASSWORD*	*LOCATION*
admin.config	Admin repository password	bin directory
sas.server.props sas.client.props sas.server.props.future	WebSphere Administrator Key and trust store passwords	properties directory
initial_ssl.properties	Key and trust store Passwords	Properties directory

Permission bit settings for the environment variables file and the directories and files specified in environment variables are discussed in the *Web Server STIG*, *Section H.3.3, Web Server HFS Objects*.

- *The IAO will ensure that the above property files are protected in accordance with the Web Server STIG, the UNIX STIG, and OS/390 STIG guidelines. Access will be restricted to authorized personnel.*

- *The WebSphere Application Server Property files will have permissions of owner**:** read/write, group: read, and others: none (640) or more restrictive (configuration files need only read permission), where the group is the SA or Web Manager account that controls the web service.*

- *The Web Manager and SA will ensure that the above property files are protected from manual editing.*

- *The IAO will ensure that the makeserver.sh program is restricted to authorized personnel.*

The following path entries were added to the /etc/httpd.conf file for WebSphere 3.5:

```
ServerInit /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:init_exit
      /usr/lpp/WebSphere/etc/WebSphere/AppServer/properties/was.conf
Service /webapp/examples/*
      /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service   /*.jhtml
      /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service   /*.shtml
      /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service   /servlet/*
      /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
Service   /*.jsp
      /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:service_exit
ServerTerm  /usr/lpp/WebSphere/AppServer/bin/was350plugin.so:term_exit
```

The following path entries are added to the /etc/httpd.conf file for WebSphere 4.0.1:

ServerInit -
/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:init_exit
Service -
/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:service_exit
ServerTerm -
/usr/lpp/WebSphere401/WebServerPlugIn/bin/was400plugin.so:term_exit

NOTE: The /etc/WebSphere clause for ServerInit matches the directory name above where the site customization was.conf file was established.

- *(ZWAS0050: CAT II) The IAO will ensure that the WebSphere Application Server directives in the httpd.conf file are configured as outlined in this STIG.*

- *The Web Manager or SA will ensure that the above path entries are added into the httpd.conf file.*

- *The Web Manager will follow the guidelines for local server permission bits as specified in the Web Server STIG (Appendix I, Guidelines for Software Review of Vendor-provided Programs and Scripts).*

- *The Web Manager will follow the permission and user audit bits and owner and group settings for the local server configuration files as specified in the Web Server STIG, Appendix H.*

- *The Web Manager will follow the permission and user audit bits and owner and group settings for the local server log directories as specified in the Web Server STIG, Appendix H.*

15.3 WebSphere Application Server and LDAP

LightWeight Directory Access Protocol (LDAP) is an easy-to-use client-server protocol designed to retrieve and manage directory information. An LDAP directory is able to support any type of data and may be configured to play any desired role. The directory's organization must comply with the LDAP subset of the X.500 standard's tree hierarchy data model. LDAP was developed as a complement to the full X.500 standard and was developed to enable "light weight" implementations over TCP/IP, desktop applications, and web browsers.

The LDAP Server product provides secure access to directory information held on an OS/390 platform from applications and systems on the network, enabling clients to add, delete, search, and extract data via the server using Lightweight Directory Access Protocol. The LDAP Server is packaged as part of the OS/390 Security Server. This reinforces the concept that directory services and security services are closely tied together. The LDAP server makes use of DB2 to store directory content. This allows the server to take advantage of the data storage and searching capabilities of DB2. LDAP uses access control lists to control client access to naming services.

WebSphere security authenticates clients based on policies that are associated with the resource the client has requested. When a request is made for a protected resource from either a web server or a WebSphere application server, the web server authenticates the user. WebSphere supports authentication mechanisms based on validating such credentials as PKI certificates, tokens, or userid and password pairs. Credentials are verified against a user registry that supports the scheme.

A user registry usually contains user, group, and user's authentication information (i.e., password). This information is provided by a client so that it can be verified or validated by the user registry. The user registry is also consulted to obtain user and group information when configuring authorization. WebSphere supports user registries based on two user domains—LDAP user registry and native operating system. In the case of the Windows NT operating system, the NT Domain and NT WorkGroup registries are supported. Though other directories that comply with the LDAP protocol can be configured to perform the function of user registries, they are not supported.

When an application is created, the administrator identifies through WebSphere Administration Application the type of challenge that is used. The table below describes the challenge types, the types of authentication performed, the registry used, and the type of client.

CHALLENGE TYPE	*AUTHENTICATION MECHANISM*	*USER REGISTRY*	*CLIENT SUPPORT*
None	None	None	Web, Java
Basic	LTPA Native OS	LDAP Native OS	Web, Java
Certificate	LTPA (trusted delegation-similar to Kerberos)	LDAP (cred.mapping)	Web
Custom	LTPA (Single Sign-on should be enabled)	LDAP	Web

A WebSphere application with a challenge type of None specified causes the runtime to not challenge a client for authentication data. If the requested resource is protected, then the client is not served the resource.

A WebSphere application with a challenge type of Basic specified causes the web server to challenge a client for userid and password. The userid and password are used to authenticate access and usage of resources.

A WebSphere application with a challenge type of Certificate specified causes the web server to perform mutual authentication over SSL. The client is required to present an X.509 certificate in order to establish the connection. This certificate is then credential mapped to a user registry. In WebSphere Application Server Standard Editions V3.5, an LDAP directory is the only registry that can be configured to support certificate-based authentication. Therefore, LTPA must be use as the authentication mechanism.

A WebSphere application with a challenge type of Custom specified causes the web server to use an HTML form to retrieve the userid and password. The administrator specifies the URL to which a client requesting a resource is redirected in order to be authenticated.

NOTE: Limited or Certificate-based web servers will be protected from unauthorized remote access at the enclave perimeter and host levels. All sensitive WWW applications will use 128-bit SSL encryption, and will migrate to Public Key Infrastructure (PKI) in accordance with the Assistant Secretary of Defense (C3I) Memorandum, subject: "Department of Defense (DOD) Public Key Infrastructure (PKI) 8520.2," 1 April 2004. Sensitive WWW applications are defined as web sites that contain unclassified information that would not be released to the public (i.e., FOUO, SBU), or information that is sensitive by aggregation or compilation. WWW applications not deemed to be sensitive, but are not intended for complete access by the general public, may use 40-bit or 58-bit SSL encryption and/or some combination of domain name, IP, userid, and password constraints.

- *The Web Server STIG will be used to provide guidance regarding the access limitations on Limited or Certificate-based web servers.*

- *The Program Manager or content manager will determine an appropriate method to limit access to the Limited or Certificate-based web server based on the STIG on Enclave Security.*

- *The Web Manager or SA will set the secure channel constraint (SSL property) through the administrative console when SSL is required.*

- *The Web Server STIG or the appropriate platform STIG will establish the guideline for userids and passwords.*

- *The IAO will ensure that the guidelines for creating, obtaining, maintaining, and using PKI Certificates are followed as specified in the Web Server STIG.*

- *The IAO will ensure that the guidelines, as specified in the Web Server STIG, are followed with respect to the use of cookies on a Web server.*

- *The LDAP started task will be protected using the started task class in accordance with the OS/390 STIG.*

15.4 WebSphere Application Server and DB2

WebSphere Application Standard Edition V4.0 uses DB2 as a persistent store. (A persistent store is used to describe the storage of objects in a database to allow them to persist over time rather than being destroyed when the application.) When WebSphere is installed on an OS/390 system a DB2 database is installed as part of the process. The database is used to store information about WebSphere and the applications.

Before DB2 can be used to store data required by servlets running under the Application Server, the Application Server must be able to locate and communicate with DB2. This is accomplished in the following way:

1. The name of the DB2 JDBC driver classes file, db2jdbcclasses.zip, is added to the appserver.classpath property. This enables the Application Server to locate the DB2 JDBC driver.

2. The location of the DB2 JDBC driver is added to the values specified on the appserver.libpath property.

At startup, the Application Server constructs an in-memory name space from the information in the was.conf file. The Application Server also registers an implementation of a Java Naming and Directory Interface (JNDI) naming context with JNDI Context Factory services. Applications use this class as input to JNDI Factory services to produce an initial naming context that serves as the starting point for name resolution within the Application Server name space.

For performance reasons, applications often establish pools of connections that are serially reusable to DB2 databases. Java Database Connectivity (JDBC) handles connections to the DB2 database. Applications have no knowledge or dependency on how a connection is established. The data source may have gotten the connection from a pool of JDBC connections that it is maintaining or may have been required to instantiate a new JDBC connection using the JDBC Core driver package that is configured on each request.

At request time, the servlet prepares a specification object identifying information necessary for connection to a DB2 JDBC database. If the connection pool property (useServerIdentity=true) is specified for the Connection Manager pool, the Application Server gets a connection using the Web server's identity even if %%CLIENT is specified or a userid and password are coded in the connection specification.

If useServerIdentity=false, the Application Server gets a connection using the identity specified by the user and password in the connection specification. The servlet asks the Connection Manager for a connection to a DB2 JDBC database using the connection specification. The connection object returned is from a Connection Manager pool, and is an instance of a class defined in the Connection Manager APIs. It is not an object from a class in the JDBC API set. This first connection is called a Connection Manager connection. Usually, a servlet gets a Connection Manager connection for every client request. The Connection Manager connection is not part of the JDBC API set. The connection class is from the JDBC API and is documented with the java.sql package. Methods of the Connection class are used to interact with DB2.

WebSphere stores this type of information in the admin.config file and the was.conf file, ncf.jvm.classpath property. The following table describes the database connections referenced in the admin.config file.

ADMIN.CONFIG FILE/DATABASE CONNECTIONS	
com.ibm.ejs.sm.adminServer.dbUrl	URL for JDBC access
com.ibm.ejs.sm.util.adminServer.dbSchema	Database schema name
com.ibm.ejs.sm.adminServer.dbDriver	Classname of JDBC driver
com.ibm.ejs.sm.adminServer.dbPassword	Password for database access
com.ibm.ejs.sm.adminServer.dbUser	Userid for database access

- *The Web Manager or SA will ensure that the database connection controls follow the guidelines as specified in the Database STIG.*

- *Passwords and userids for database access will be created in accordance with the Web Server STIG, the Database STIG, and the appropriate platform STIG.*

- *The DB2 Administrator will set up DB2 tables in accordance with the Database STIG.*

- *The IAO will ensure that the DB2 resources are protected in accordance with the DB2 resource profiles. The DB2 resource profile protects databases by protecting the ability to access DB2 itself and the DB2 tables.*

15.5 Component Broker

The Component Broker runtime (specifically the application adaptor to which the object is configured) is responsible for authenticating requests made on the data system for that object's persistent data. To do this, credentials are mapped between the Component Broker security credentials and those of an entity in the data system's security mechanism.

When an object in a Component Broker application server calls a method that accesses the backing data system, the credential mapping is used to authenticate and authorize the Component Broker credentials to the data system's security mechanism (ACF2, RACF, or TOP SECRET). In some cases, an application uses several backing data systems with different security mechanisms. Credential mappings can be used to map from one Component Broker principal to multiple different data system entities.

The Component Broker authorization services enable a client to control access to individual methods on business objects in application servers. Component Broker uses Distributed Computing Environment (DCE) security for all authentication of application servers and for authentication of clients to servers.

A DCE account must be created for each client that uses Component Broker. Component Broker clients must have accounts created in the DCE user registry. In DCE, cells are sometimes also referred to as realms. DCE uses cells to organize administrative domains. The Component Broker Administration application is used to maintain realms. Thus by working in conjunction with security services provided by the OS/390 Security Server, the Component Broker is able to ensure resource security.

- *The data sets BBO.SBBOLOAD, BBO.SBBOLD2, and BBO.SBBOLPA will be APF authorized.*

- *The data set BBO.SBBOULIB or SBBOMIG will not be APF authorized because it should run under the authority of the client.*

- *The data sets BBO.SBBOLOAD, BBO.SBBOLD2, and BBO.SBBOLPA will be restricted from unauthorized updates in accordance with OS/390 STIG guidelines.*

- *(ZWAS0010: CAT II) The IAO will ensure that WebSphere server data sets restrict UPDATE and/or ALLOCATE access to systems programming personnel.*

- *The SOMDOBJS class will be used to control a client's access to and invoking of methods.*

- *The IAO will ensure that access to the Component Broker Administration application will be restricted to authorized personnel.*

- *The IAO will ensure that method-level access checking as performed through the OS/390 Component Broker Administration application will follow the guidelines of the Web Server STIG.*

Resource Recovery Services (RRS) is used by the Component Broker backup persistent DB2 objects. RRS uses System Logger to record events related to protected resources in log streams. RRS is defined as a subsystem in an OS/390 environment by placing the following statement in the IEFSSNxx member in SYS1.PARMLIB:

```
SUBSYS SUBNAME(RRS)
```

The following RRS log streams are used by System Logger to support backup:

1. RM.DATA
2. MAIN.UR
3. DELAYED.UR
4. RESTART
5. ARCHIVE

15.6 WebSphere for z/OS

WebSphereVersion 4.0.1 for z/OS uses many of the same profiles and rules as WebSphere V3.5. A major difference between WebSphere 3.5 and WebSphere 4.0.1 for z/OS is in the area of security. Under WebSphere 4.0.1 for z/OS, the WebSphere Application Server interfaces with the security ACPs. WebSphere 3.5 runs as a plug-in to the HTTP server and as a result runs under HTTP server's address space and depends on HTTP server for ACP support. WebSphere 4.0.1 for z/OS is capable of servicing multiple machines, sysplexes, servers and nodes. It fully implements the J2EE Standard. WebSphere 4.0.1 for z/OS supports the development and maintenance of Enterprise Java Beans (EJBs).

By default, WebSphere 4.0.1 for z/OS provides four system servers. They are as follows:

SYSTEM SERVER	*FUNCTION*
Daemon Server	Used for administration and the starting and stopping of the other systems servers.
Naming Server	Used to provide object reference support.
Systems Management Server	Controls all configuration data.
Interface Repository Server	Provides a repository of information used by WebSphere.

NOTE: Any number of application servers may be run under WebSphere V4.0.1 for z/OS.

Each server has a control region that handles the management of the workloads and the allocation and de-allocation of server regions. All application processing is handled by the server regions. Securing these servers is described in the upcoming sections.

NOTE: The default servers are as follows:

Started tasks for WAS:

Server Name	*Server Type*
WSTDMN	Daemon
WSTIR	Interface Repository
WSTJ2E	J2EE IVP
WSTLDAP	LDAP
WSTNM	Naming Server
WSTSM	System Management

Application environments for WAS Servers (IVP):

Server Name	*Server Type*
WSTJ2E	WAS APPLICATION SERVER REGION 2

15.7 WebSphere RACF Implementation

The following section describes the considerations that must be addressed during a RACF implementation of WebSphere. Some of the classes identified are available under z/OS and examples have been created for z/OS. In addition, this section assumes that the present file authorization already exists and that the V3.5 file replaces the V3.2 that is loaded in the RACF database.

15.7.1 Classes and Profiles

The following table lists all the RACF classes as they relate to WebSphere and provides a description of each:

RACF CLASS	*DESCRIPTION*
APPL	Controls access to applications. Kerberos is set up as an application required so the users can enter the *kpasswd* command.
CBIND	Controls a client's ability to bind to and access a server.
DATASET	Controls access to datasets.
DIGTCERT	Contains digital certificates and information about them.
DSNR	Controls access to DB2 subsystems.
EJBROLE	Identifies the member class for Enterprise Java Beans authorization roles. The APPLDATA field in an EJBROLE profile defines the target JAVA identity when running in RUNAS ROLE mode.
FACILITY	Profiles are defined in this class so that resource managers can check the user's access to profiles when an action is taken. Profiles are placed for Digital Certificate, DCE, Kerberos, and UNIX System Services, BPX.DAEMON are placed here.
GEJBROLE	Describes the grouping class for Enterprise Java Beans authorization roles.
KERBLINK	Defines the mapping class for user identities of local and foreign principals. Used in Kerberos so that unique RACF userids can be mapped to each foreign principal.
LOGSTRM	Controls applications access to the system logger resources.
OPERCMDS	Required to allow the WebSphere started task, to stop and start other WebSphere servers. Restricts control of Application Servers to by userids.
PROGRAM	Defines trusted programs when the NOPADS option is set. Any security relevant program that changes the identity of its Address space or thread from USS needs to be declared here.

RACF CLASS	*DESCRIPTION*
PTKTDATA	The PassTicket key class enables the Security Administrator to associate a RACF secured signon secret key with a particular mainframe application that uses RACF for user authentication. It is required for Kerberos set up. Profiles do not have to be created within this class, just activated.
REALM	Defines local and foreign realms. (Required for Kerberos set up to define a local realm.) z/OS, OS/390, and Windows are examples of foreign realms that can be defined.
RRSFDATA	Used to control RACF remote sharing facility functions. Required as part of Kerberos set up.
SERVAUTH	Identifies profiles that are used by servers to check a client's access authorization to the server and the resources managed by the server. This class can be used to protect TCP/IP ports. ***NOTE:*** WebSphere and Kerberos must be given access if this class is used.
SERVER	Controls the server's ability to register with the daemon. WebSphere uses this class to control calls to authorized programs by server regions in control regions.
SOMDOBJS	Controls the client's ability to invoke a method in a class. ***NOTE:*** This is only used for Web Applications running in the WebSphere Application Server 3.5 for z/OS and OS/390.
STARTED	Used in preference to the started procedures table to assign an identity during the processing of an MVS start command. ***NOTE:*** WebSphere and Kerberos are defined as a started task within this profile.
SURROGAT	Used in conjunction with BPX.SRV.* profiles in the SURROGAT class to allow security context switches for unauthenticated userids. If surrogate submission or logon by is allowed, it identifies which userids can act as surrogates.

15.7.2 CBIND Class

There are two profiles to create when using the CBIND class. They are the CB.BIND.*server_name* profile, which controls whether a local or remote client can access servers. The CB.BIND is mandatory for the first two qualifiers for the profile; the third qualifier is the server name. Also, there is the CB.*server_name* profile that controls whether a client can use components in a server; again these definitions are mandatory.

```
SETROPTS CLASSACT(CBIND)
SETROPTS RACLIST(CBIND)
SETROPTS GENERIC(CBIND)
```

Once the class is defined, the server needs to be defined (it has the name of the started task) to the CBIND class.

```
RDEFINE CBIND CB.BIND.server_name UACC(NONE)
RDEFINE CBIND CB.server_name UACC(READ)
```

Now that the CBIND class is activated the CBIND class and the WebSphere server needs to be given the started task id CONTROL access to the new profile.

```
PERMIT CB.BIND.server_name CLASS(CBIND) ID(web_server_userid) -
    AC(CONTROL)
```

To finish we need to refresh the class.

```
SETROPTS RACLIST(CBIND) REFRESH
```

To activate the SERVER class for server access the following could be used.

```
SETROPTS CLASSACT(SERVER)
SETROPTS RACLIST(SERVER)
```

Once the SERVER class is activated, add the WebSphere profiles for our server as profiles within the SERVER class.

```
RDEFINE SERVER CB.*.server_name  UACC(NONE)
```

NOTE: Need to authorize WebSphere to have read access.

```
PERMIT CB.*. server_name CLASS(SERVER) -
    ID(web_server_userid) AC(R)
```

To complete the SERVER class setup, refresh RACF.

```
SETROPTS RACLIST(SERVER) REFRESH
SETROPTS GENERIC(SERVER) REFRESH
```

- *(ZWAS0030: CAT II) The IAO will ensure that the CBIND resource is defined to the ACP with an access of none.*

15.7.3 Activating the SERVAUTH Class to Control z/OS Communication Server Resources

The z/OS Communication Server can use the SERVAUTH class to perform authorization checks and determine if specific users can connect to servers using specific communication ports. Servers can be authorized to accept connections for clients whose certificates contain a hostIdMappings extension by administering profiles in the SERVAUTH class. Be sure that each server to be authorized has a unique RACF userid, if not already defined. Servers may run as jobs or started procedures. TCP/IP ports can also be protected using the SERVAUTH class.

To activate the SERVAUTH class:

```
SETROPTS CLASSACT(SERVAUTH)
SETROPTS RACLIST(SERVAUTH)
SETROPTS GENERIC(SERVAUTH)
```

To define resources in the SERVAUTH class use the following:

```
RDEFINE SERVAUTH IRR.HOST.hostname UACC(NONE)
```

Read authority to the IRR.HOST.hostname resource in the SERVAUTH class allows a server to accept client connections for the host name specified in the resource name.

```
PERMIT IRR.HOST.hostname CLASS(SERVAUTH) ID(web_server_userid) –
    ACCESS(READ)
```

Permitting servers to access this resource with *read* authority, allows them to accept logons for the host name specified in the resource name.

We now need to refresh RACF.

```
SETROPTS RACLIST(SERVAUTH) REFRESH
```

Now that we are protecting the host using the SERVAUTH class, we can now go a step further and protect the ports. We can protect the stack and any individual port.

```
RDEFINE SERVAUTH EZB.STACKACCESS.hostname.TCPstartedtask -
    UACC(NONE)
```

The TCP qualifier is the name of the TCP/IP started task. Now that we have protected the TCP/IP stack, give *read* access to specific servers.

PERMIT EZB.STACKACCESS.*hostname.TCPstartedtask* ID(*web_server_userid*) -
ACCESS(READ)

Now we define a port to the SERVAUTH class.

RDEFINE SERVAUTH EZB.PORTACCESS.*hostname.TCPportnumber* -
UACC(NONE)

Again we need to give the port *read* access to the started tasks, userids, and so forth.

PERMIT EZB.PORTACCESS.*hostname.TCP.portnumber* ID(*web_server_userid*) -
ACCESS(READ)

Now web server clients can logon to the host, access the TCP/IP stack, and access by a specific port. All ports can be protected and access restricted to ensure any access from the outside world is controlled.

15.7.4 Activating the PTKTDATA Class to Enable PassTickets Support

The application data field in a resource profile in the PTKTDATA class is used to control the replay protection function of PassTicket support. Replay protection prevents the reuse of PassTickets. Since by design PassTickets has a one second granularity, replay protection needs to be turned off if more than one PassTicket might be generated for a single userid within the same second. In the application data field, if no replay protection is specified, the result would be replay protection being bypassed. Before using the secured signon function, the PTKTDATA class must be activated. All profiles that contain PassTicket information are defined in this class:

SETROPTS CLASSACT(PTKTDATA)
SETROPTS RACLIST(PTKTDATA)

At least one profile in the PTKTDATA class must be created for each application that users can gain access to with a PassTicket. The profile associates a secret secured signon application key with a particular application on a particular system.

To define a profile to the PTKTDATA class:

RDEFINE PTKTDATA applicationname SSIGNON(key description) -UACC(NONE)

The application name can be an application name only, an application name appended (or qualified) by a RACF connect group, an application name qualified by a RACF userid, or an application name qualified by both a RACF connect group name and a RACF userid.

The key description defines the signon application key and specifies the method RACF is to use to protect it in the RACF database on the host. When defining the secured signon application keys, RACF either masks or encrypts each key. If the system has a cryptographic product installed and available, the secured signon application keys may be encrypted for added protection.

NOTE: The profile must be a discrete profile due to each application being uniquely defined. Generic profiles cannot be specified. If a generic profile was specified, it would be ignored and there would be no authentication for the PassTicket.

To define a profile for an application in the PTKTDATA class with a masked signon application key value of encodedkeyvalue, code the following:

```
RDEFINE PTKTDATA name - SSIGNON(KEYMASKED(encodedkeyvalue))
    UACC(NONE)
```

To refresh the PTKTDATA profile, code the following:

```
SETROPTS RACLIST(PTKTDATA) REFRESH
```

15.7.5 DIGTCERT General Resource Class

NOTE: It is recommended by IBM that the DIGTCERT class is RACLISTed to improve performance when using digital certificates to access WebSphere Applications. If the class is not RACLISTed, digital certificates can still be used, but performance may be impacted.

For best performance, RACLIST the DIGTCERT class by issuing the SETROPTS RACLIST(DIGTCERT) command.

After creating a new digital certificate, refresh the DIGTCERT class by issuing the SETROPTS RACLIST(DIGTCERT) REFRESH command.

NOTE: If the RACLISTed DIGTCERT profiles are not refreshed, RACF will still use the new digital certificate. Performance may be impacted.

RACF uses RACLISTed digital certificates first, so any RACLISTed digital certificates that have been altered, re-added, or deleted does not reflect those changes until the DIGTCERT class has been refreshed.

NOTE: Profiles in the DIGTCERT and DIGTRING classes are maintained automatically through RACDCERT command processing. Do not administer profiles in the DIGTCERT and DIGTRING classes using the RDEFINE, RALTER, and RDELETE commands. These commands do not operate with profiles in the DIGTCERT and DIGTRING classes. Since these profiles contain lower-case characters, the SEARCH FILTER and RLIST commands are not intended for use and will deliver unpredictable results.

Profile names in the DIGTCERT class are in the form as follows:

serial-number.issuer's-distinguished-name

15.7.6 File Permissions and UNIX Permissions under RACF

1. The data set permissions for the HTTP server have already been specified in the *Web Server STIG*. WebSphere runs under the HTTP server userid. The RACF rules defined in the *Web Server STIG* cover WebSphere. The only difference is that the HTTP server userid need *read* access to the following data sets:

   SYS2.EJS.** and SYS2.OE.**

2. The HTTP server userid requires *read* authority for all structures subordinate to /usr/lpp/WebSphere.

15.8 WebSphere CA-ACF2 Implementation

CA-ACF2 protects information systems and the data they manage from unauthorized disclosure, modification, and destruction. It does this by authenticating the users of the system and then by limiting each user to the authorizations established for them. CA-ACF2 helps ensure the integrity and security of the critical information assets.

The various resources used within the WebSphere environment are divided into classes or profiles that are used to secure the resource. The following table lists all of the relevant resources for the CA-ACF2 environment with their resource rule default type code and a brief description of them.

15.8.1 Classes and Descriptions

CLASS	*TYPE CODE*	*DESCRIPTION*
APPL	APL	Controls access to applications. Kerberos is set up as an application; required so the users can enter the *kpasswd* command.
CBIND	SAF	Controls the client's ability to bind to the server. With WebSphere we need to control access to the server.
DATASET		Controls access to data sets.
DSNR	SAF	Controls access to DB2 subsystems.
EJBROLES	EJB	Controls access to Enterprise Java Beans authorization roles.
FACILITY	FAC	Miscellaneous uses. Resources are defined in this class to enable resource managers to check a user's access to the resource when the user takes some action. Examples of resource checks would

CLASS	*TYPE CODE*	*DESCRIPTION*
		be Digital Certificates, DCE, Kerberos, and UNIX System Services such as BPX.DAEMON.
KERBLINK	_	Mapping class for user identities of local and foreign principals. Used in Kerberos we can map a unique CA-ACF2 logonid to each foreign principal.
LOGSTRM	SAF	Reserved for MVS/ESA.
OPERCMDS	OPR	Controlling who can issue operator commands (i.e., JES and MVS). Required to allow WebSphere started task to stop and start other WebSphere servers.
PROGRAM	PGM	Controlled programs (load modules).
PTKTDATA	PTK	PassTicket key class enables the Security Administrator to associate a CA-ACF2 secured signon secret key with a particular mainframe application that uses CA-ACF2 for user authentication.
REALM		Used to define the local and foreign realms. Required for Kerberos set up, as defined by the local realm to this class. Also, use this class to define foreign realms, such as other z/OS, OS/390, Windows, etc.
SERVAUTH	SER	Defines resources that are used by servers to check a client's authorization to use the server or to use the resources managed by the server. Use this class to protect TCP/IP ports. If using this class, WebSphere and Kerberos must be given access.
SERVER	SAF	Controls the servers' ability to register with the daemon. In WebSphere, this class is used to control whether a server region can call an authorized program in the control region.
SOMOBJS	SAF	Controls the client's ability to invoke the method.
SURROGAT	SUR	If surrogate submission is allowed, or logon by is allowed, it defines which userids can act as surrogates. Required for RunAs.

CA-ACF2 protects resources by default, assuming access is denied unless specifically permitted by a CA-ACF2 rule or privilege. This means that the resources do not need to be activated to ensure their protection. If a site deems that a particular class of resource does not need protection, then a generic rule similar to the following can be added for that resource.

```
COMPILE *
$KEY(********) TYPE(type_code) UID(*) ALLOW
```

If desired, a resource sharing a type code can have a unique type code by redefining the class and type code in a GSO CLASMAP record. If the APPL class was not being protected and a unique type code of APP was used instead of SAF, code the following CLASMAP record:

```
SET CONTROL(GSO)
INSERT CLASMAP.APPL RESOURCE(APL) RSRCTYPE(APP) -ENTITYLN(8)
```

Because the resource rule $KEY, as specified above, contains masking, create a directory for the specific set of rules under that type code. This is done by adding the group of resource rules to the GSO INFODIR record as follows:

```
SET CONTROL(GSO)
CHANGE INFODIR TYPES(APL)
```

To activate all of these changes without waiting for the next initialization of CA-ACF2, issue the following commands:

```
F ACF2,REFRESH(CLASMAP)
F ACF2,REFRESH(INFODIR)
F ACF2,REBUILD(APL)
```

15.8.2 CBIND Class

Use the CBIND class to restrict a client's ability to access servers. There are two types of resources that WebSphere uses in the CBIND class:

- One that controls whether a local or remote client can access servers. The name of the resource has the form CB.BIND.*server_name* where *server_name* is the name of the server.

- One that controls whether a client can use objects in a server. The name of the resource has the form CB.*server_name* where *server_name* is the name of the server.

NOTE: When adding a new server, all systems management logonids (e.g., WebSphere administrator ID) must be authorized to have read access to the CB.server_name and CB.BIND.server_name resources.

Example: To allow the WebSphere administrator ID *read* authority to the CB.BBOASR1 and CB.BIND.BBOASR1 resources, add the following to the CBIND class CB resource rule:

```
BBOASR1 UID(was_admin_uid) SERVICE(READ) ALLOW
BIND.BBOASR1 UID(was_admin_uid) SERVICE(READ) ALLOW
```

The CBIND class defaults to a generic type code of SAF. It is recommended that a GSO CLASMAP record be added to change this to a site selected resource unique to the CBIND class such as CBI. The following shows how the suggested change example would be coded:

SET CONTROL(GSO)
INSERT CLASMAP.*cbind* RESOURCE(CBIND) RSRCTYPE(*cbi*) -ENTITYLN(41)

To activate the change immediately, issue the following command:

F, ACF2,REFRESH(CLASMAP)

- *(ZWAS0030: CAT II) The IAO will ensure that the CBBIND resource is defined to the ACP with an access of none.*

15.8.3 EJBROLE Classes

Access to an enterprise bean can be controlled through security roles that are the group of permissions that a user must have to successfully use an application. Using a Java method called isCallerInRole, the application programmer or systems administrator specifies the security role names, in the WebSphere Administration Application, that are allowed to access a particular bean. Only users having access to these security role names are granted access to the bean. Execution of isCallerInRole in an OS/390 environment causes invokes IRRPNL00 profile name list service routine.

This routine returns a list of all of the Java security roles that a user has access to. CA-ACF2 fully supports this use of the IRRPNL00 routine through the use of EJB generalized resource rules. (By default, the internal CLASMAP record maps the EJBROLE resource class to an EJB type code.) When SAF processing passes the IRRPNL00 routine request to external security, CA-ACF2 processes each EJB resource rule to determine if the specified user has access to each defined role. After processing all of the EJB rules, CA-ACF2 passes a list of all allowed roles for use by the Java isCallerInRole method, which then allows or prevents access to the bean based on this list.

To set up the external security environment, do the following:

1. Identify the security roles specified by the application programmers or OEM/ISV providers and the users that should have access to each role. The role name used in the EJB resource rules is the security role specified in the jar file or for the application.

2. Write and store EJB resource rules for each security role. There are some special guidelines that apply to EJBROLE resource rules as follows:

   - Since the purpose of the EJB rules is to provide a specific list of allowable roles for each user, each defined role in an environment must have a specific rule for it. Thus, masking is not allowed in the resource name of an EJB rule.

   - EJBROLE names use mixed case names. The CA-ACF2 resource rules now support mixed case resource names. To identify this, the resource class is designated as mixed by using the MIXED operand in the appropriate CLASMAP record. The SHOW CLASMAP output now indicates that the MIXED operand is turned on when a yes was placed in the column labeled MIXED.

- Once the MIXED keyword is set on, mixed case in the $KEY, the $PREFIX, the $USERDATA, the resource name, and the NEXTKEY parameter can be used. Ensure that the administrative platform used for processing the EJB rules supports the entry and display of mixed case.

- EJBROLE processing can be used to retrieve data for use in an application. To access the APPLDATA, the application performs a SAFEXTRACT call. In a CA-ACF2 environment, the APPLDATA is stored in the $USERDATA control card of the EJBROLE resource rule. The value placed in the $USERDATA is returned as APPLDATA in response to the EXTRACT call. The value in the $USERDATA can be mixed case.

EJB resource rules must be globally resident by means of a resident directory so that CA-ACF2 can process them. To accomplish this, enter the following commands:

```
SET CONTROL(GSO)
CHANGE INFODIR TYPES(R-REJB)
```

When a resident resource rule is created or changed, the directory for it must be rebuilt through the following command:

```
F ACF2,REBUILD(EJB)
```

Example: The ACCOUNT bean is an isCallerInRole Java method coded to allow access only by those users having access to the accounting.clerk and the accounting.manager security roles. The following resource rule can be written to accomplish this:

```
COMPILE
$KEY(ACCOUNTING) TYPE(EJB)
CLERK UID(uid_string_clerk) ALLOW
MANAGER UID(uid_string_manager) ALLOW
END
```

15.8.4 SOMDOBJS Class

The application assembler must assign method permissions to the bean or method using the Application Assembly Tool. To do this:

1. Define the roles relevant to the application.

2. Once defined, the role can be assigned to access an application (as a method permission).

3. After the application assembly is complete, the application must be reinstalled using the Administration application.

Use the SOMDOBJS class in CA-ACF2 to control a client's access to CORBA objects. Resource names in SOMDOBJS have the form server_name.home.method, where server_name is the server name.

If a method is protected by SOMDOBJS, a client must have *read* or *update* authority, depending on the type of access being attempted. If a client program is using the method to update an attribute of an object, give the client *update* authorization for the method; if a client program is using the method to read an attribute of an object, give the client *read* authorization for the method. All names are folded into uppercase characters, regardless of how they are entered.

In addition to the SOMDOBJS definitions, specify method-level access checking through the WebSphere Administration application. Check the box for method-level access checking when defining the application's container.

15.8.5 Resource Managers

Resource managers such as DB2, IMS, and CICS have implemented their own resource controls, which control the ability of clients to access resources. When resource controls are used by DB2, use CA-ACF2 for DB2 or issue the relevant DB2 GRANT statements.

Access to OTMA for IMS access is through the FACility resource class IMSXCF.OTMACI.

Access to EXCI for CICS is through the SURROGAT class resource logonid DFHEXCI.

15.8.6 File Permissions and UNIX Permissions Under ACF2

1. The data set permissions for the HTTP server have already been specified in the *Web Server STIG*. WebSphere runs under the HTTP server logonid. The ACF2 rules defined in the *Web Server STIG* cover WebSphere. The only difference is that the HTTP server logonid needs *read* access to the following data set:

   SYS2.EJS.** and SYS2.OE.**

   For WebSphere V4.0.1

   SYS2.WAS401

2. The HTTP server logonid requires *read* authority for all structures subordinate to /usr/lpp/WebSphere.

15.9 WebSphere CA-TOP SECRET Implementation

Through individual accountability, access permissions, and a comprehensive audit trail, CA-TOP SECRET controls and monitors who can access and change data. CA-TOP SECRET permissions are issued to control how new data is shared. Additional advanced technology within CA-TOP SECRET provides further assurance of data integrity.

15.9.1 Classes and Special Records

The following table briefly describes the resource classes and special records that CA-TOP SECRET employs to control WebSphere:

CONTROL	*AUTHORIZATION*
Access control lists in LDAP	Controls access to WebSphere for z/OS naming and interface repository data
CBIND class	Access to a server
DATASET class	Access to data sets
DCEUUIDS and IBMFAC classes	Mapping DCE credentials to CA-TOP SECRET userids
DSNR class	Access to DB2
EJBROLE class	Access to methods in enterprise beans
IBMFAC (IRR.DIGTCERT.LIST) & (IRR.DIGICERT.LISTING)	SSL key rings certificates and mappings
IBMFAC (IMSXCF.OTMACI)	Access to OTMA for IMS access
IBMFAC (IRR.RUSERMAP)	Kerberos credentials
File permissions	Access to HFS files
GRANT (DB2)	DB2 access to plans and database
KERBLINK	Specifies a label-name to identify the foreign principal mapping record. Up to 8 alphanumeric characters are used. It must be a unique name within the KERBLINK SDT record type.
LOGSTRM class OPERCMDS class	Access to log streams Start and stop servers by Daemon
PTKTDATA class	PassTicket enabling in the Sysplex (This relates to the session keys in the NDT within CA-TOP SECRET.
REALM	Used to define the local and foreign realms. Required for Kerberos setup as defining the local realm to this class. This class is also used to define foreign realms.
SERVER class	Access to control region by server region.
SERVAUTH class	TCP/IP in OS/390 2.10 and above uses the SERVAUTH resource class to protect TCP/IP resources from unauthorized access. There are four functions protected by the SERVAUTH class: Stack Access, Net Access, Port and TN3270 Access.
SOMDOBJS class	Access to methods in CORBA objects
STC	Associate procname and userid in the STC table.
SURROGAT class (*.DFHEXCI)	Access to EXCI for CICS access

15.9.2 CBIND Class

The CBIND class is used to restrict a client's ability to access servers. There are two types of resources that WebSphere uses in the CBIND class:

The other resource controls whether a local or remote client can access servers. The name of the resource follows the following format:

CB.BIND.*server_name*

where *server_name* is the name of the server

NOTE: When adding a new server, all systems management userids (e.g., WebSphere administrator ID) must be authorized to have read access to the CB.server_name and CB.BIND.server_name resources.

- *(ZWAS0030: CAT II) The IAO will ensure that the CBBIND resource is defined to the ACP with an access of none.*

Example: The WebSphere administrator ID needs *read* authority to the CB.BBOASR1 and CB.BIND.BBOASR1 servers:

```
TSS ADD(cbowner) CBIND(CB)
TSS PERMIT(was_admin_acid) CBIND(CB.BBOASR1) ACCESS(READ)
TSS PERMIT(was_admin_acid) CBIND(CB.BIND.BBOASR1) ACCESS(READ)
```

GEJBROLE, EJBROLE, and SOMDOBJS classes use the EJBROLE (or GEJBROLE) class in CA-TOP SECRET to control a client's access to enterprise beans. There are two distinct sets of tasks that are required to protect an application using EJB roles"

1. The security administrator must define the roles and set up access rights in CA-TOP SECRET.

2. A profile name, with the same name as the EJBROLE classname, must be defined.

Example:

```
TSS ADD(DEPARTMENT) EJBROLE (ROLE_NAME)
```

Where department is a department already defined in the CA-TOP SECRET database and role_name matches the security role attribute specified either in the jar file or for the application. Create membership in the role by permitting CA-TOP SECRET userids or profiles permission to the defined EJBROLE resource.

Example:

```
TSS PERMIT(Userid/profile) EJBROLE(role_name) ACCESS(READ)
```

The application assembler must assign method permissions to the bean or method using the Application Assembly Tool. It is done in the following way:

1. Define the roles relevant to the application. These role names must match the resource names defined to CA-TOP SECRET.

2. Once defined, the role can be assigned to access an application (as a method permission).

3. After the application assembly is complete, the application must be reinstalled using the Administration application.

Use the SOMDOBJS class in CA-TOP SECRET to control a client's access to CORBA objects. Resource names in SOMDOBJS have the form:

server_name.home.method

where:

server_name - Is the server name.
home - Is the home name.
method - Is the method name.

If a method is protected by SOMDOBJS and:

1. A client program is using the method to *update* an attribute of an object; give the client update authorization for the method.

2. A client program is using the method to read an attribute of an object; give the client *read* authorization for the method.

All names are folded into uppercase characters, regardless of how they are entered. Thus, there is no difference between:

my_server_my_home.my_method; and,
my_SERVER.my_HOME.my_METHOD

In addition to the SOMDOBJS definitions, specify the method-level access checking through the WebSphere Administration application. Check the box for method-level access checking when defining the application's container.

15.9.3 Resource Managers

Resource managers such as DB2, IMS, and CICS have implemented their own resource controls, which control the ability of clients to access resources. When resource controls are used by DB2, use the DSNR CA-TOP SECRET class or issue the relevant DB2 GRANT statements.

Access to OTMA for IMS access is through the **IBMFAC** class (**IMSXCF.OTMACI**).

Access to EXCI for CICS is through the **SURROGAT** class (***.DFHEXCI**). Access to data sets is controlled through the DATASET class. Access to HFS files is controlled through file permissions or the HFSSEC class.

15.9.4 File Permissions and UNIX Permissions Under TSS

1. The data set permissions for the HTTP server have already been specified in the *Web Server STIG*. WebSphere runs under the HTTP server ACID. The TSS rules defined in the *Web Server STIG* cover WebSphere. The only difference is that the HTTP server ACID needs *read* access to the following data sets:

   SYS2.EJS. and SYS2.OE.****

   For WebSphere V4.0.1

   SYS2.WAS401

2. The HTTP server ACID requires ***read*** authority for all structures subordinate to **/usr/lpp/WebSphere**.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense Directive (DODD) 8500.1, “Information Assurance (IA),” 24 October 2002.

Department of Defense Instruction (DODI) 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003.

Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assurance (IA) and Computer Network Defense (CND)”, 15 March 2002.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AIS)," July 1996.

Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide, Version 4, Release 2, 15 October 2002.

Defense Information Systems Agency (DISA) S/390 Logical Partition Security Technical Implementation Guide, Version 1, Release 5, 13 May 2003.

Defense Information Systems Agency (DISA) VM Security Technical Implementation Guide, Version 1, Release 4, 13 May 2003.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 October 1991.

Army Regulation (AR) 25-2, "Information Assurance," 14 November 2003.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," August 1992.

Public Law 100-235, 100th Congress, an Act cited as the "Computer Security Act of 1987," 8 January 1988.

International Business Machines Corporation

- IBM Communications Server for OS/390 V2R10 TCP/IP Implementation Guide Volume 1: Configuration and Routing (SG24-5227)
- IBM Communications Server for OS/390 V2R10 TCP/IP Implementation Guide Volume 2: UNIX Applications (SG24-5228)
- OS/390 UNIX System Services Planning (SC28-1890)
- OS/390 UNIX System Services User's Guide (SC28-1891)
- OS/390 UNIX System Services Command Reference (SC28-1892)
- OS/390 Version 2 Release 6 UNIX System Services Implementation and Customization (SG24-5178)
- OS/390 MVS Initialization and Tuning Reference (SC28-1752)
- OS/390 MVS System Management Facilities (SMF) (GC28-1783)
- OS/390 MVS System Commands (GC28-1781)
- OS/390 SecureWay Communications Server IP Configuration (SC31-8513)
- OS/390 SecureWay Communications Server User's Guide (GC31-8514)
- OS/390 Security Server (RACF) Callable Services (GC28-1921)
- OS/390 IBM Communications Server IP User's Guide (GC31-8514)
- OS/390 IBM Communications Server IP Configuration Guide (SC31-8725)
- OS/390 IBM Communications Server IP Configuration Reference (SC31-8726)
- OS/390 IBM SDSF Customization and Security (SC28-1623-03)
- z/OS IBM SDSF Operation and Customization (SA22-7670-03)

Computer Associates International

- CA-ACF2 OS/390 Administrator Guide, Version 6.3
- CA-ACF2 OS/390 Security Cookbook, May 2000
- CA-TOP SECRET OS/390 Security Cookbook, April 2000
- CA-EXAMINE Product Manuals
- eTrust CA-ACF2 Security for OS/390 and z/OS – OS/390 and z/OS Security Cookbook, September 2001
- eTrust CA-TOP SECRET Security for OS/390 and z/OS –Security Cookbook, October 2001

Other

TMON for MVS Product Manuals
TMON for CICS Product Manuals
FDR Product Manuals
OMEGAMON/OMEGAMON II Product Manual

APPENDIX B. SAMPLE PROGRAM PROPERTIES TABLE (PPT)

The following table depicts the default values for the Program Properties Table (PPT), as provided by IBM in module **IEFSDPPT** for OS/390, Version 2 Release 10. Please refer to the IBM *OS/390 MVS Initialization and Tuning Reference* documentation for the version and release of OS/390 installed at the individual site for the actual contents of the default **IEFSDPPT** module.

PROGRAM NAME	*PROGRAM DESCRIPTION*	*NC*	*NS*	*PR*	*ST*	*ND*	*BP*	*KEY*	*PROC AFFINITY*	*2P*	*1P*	*NP*
AHLGTF	GTF	X	X		X			00	NONE			X
AKPCSIEP	ISP		X		X	X		01	NONE			X
ANFFIEP	IP Printway		X		X	X		01	NONE			
APSPPIEP	PSF		X		X	X		01	NONE			X
ASBSCHIN	APPC/MVS Scheduler Address Space (ASCH)		X		X			01	NONE	X	X	
ASBSCHWL	APPC/MVS Message Log Writer			X				01	NONE			
ATBINITM	APPC/MVS Address Space		X		X			01	NONE	X	X	
ATBSDFMU	APPC/MVS SDFM Utility			X				01	NONE			
AVFMNBLD	AVM	X	X		X			03	NONE			X
BPXINIT	OMVS	X	X		X			00	NONE			
BPXPINPR	OMVS	X			X			08	NONE	X	X	
BPXVCLNY	OMVS		X	X	X			08	NONE			
CBRIIAS	OTIS				X			05	NONE			
CBROAM	OAM		X		X			05	NONE			
CNLSSDT	MVS Message Service (MMS)		X		X			00	NONE	X	X	
COFMINIT	VLF		X		X	X	X	00	NONE			
COFMISDO	DLF	X	X		X	X	X	00	NONE			
CQSINIT0	IMS CQS		X		X			07	NONE			X
CSVLLCRE	LLA		X		X		X	00	NONE			
CSVVFRCE	Virtual Fetch		X		X			00	NONE			
DFSMVRC0	IMS Control Program		X		X			07	NONE			
DSNUTILB	DB2 Batch							07	NONE			

PROGRAM NAME	*PROGRAM DESCRIPTION*	*NC*	*NS*	*PR*	*ST*	*ND*	*BP*	*KEY*	*PROC AFFINITY*	*2P*	*1P*	*NP*
DSNYASCP	DB2		X		X			07	NONE			
DXRRLM00	IMS Manager		X		X			07	NONE			
EPWINIT	FFST	X	X			X	X	00				X
ERBMFMFC	RMF		X		X	X		08	NONE			
ERB3GMFC	RMF		X		X	X		08	NONE			
EZAPPAAA	NPF		X					08				
EZAPPFS	NPF		X					01				
EZBTCPIP	TCP/IP Address Space	X	X	X	X			06		X	X	
GDEICASB	DFP/DFM		X		X			05	NONE			X
GDEISASB	DFP/DFM				X			05	NONE			X
GDEISBOT	DFP/DFM		X		X			05	NONE			X
HASJES20	JES2	X	X		X	X		01	NONE			
HHLGTF	GTF	X	X		X			00	NONE			X
IASXWR00	External Writer	X			X			01	NONE			
IATCNDTK	JES3	X	X	X	X			01	NONE			
IATINTK	JES3	X	X		X	X		01	NONE			
IATINTKF	JES3 FSS		X		X	X		01	NONE			
IDAVSJST	SMSVSAM Address Space	X	X	X	X			05	NONE			
IEAVTDSV	Dumping Services			X	X		X	00	NONE	X	X	
IEDQTCAM	TCAM		X					06	NONE			X
IEEMB860	Master	X	X		X	X	X	00	NONE			
IEEVMNT2	Mount Command	X			X			00	NONE			
IEFIIC	Initiator	X		X	X			00	NONE			
IFASMF	SMF	X	X	X	X	X		00	NONE			
IFDOLT	OLTEP							08	NONE	X	X	
IGDSSI01	SMS	X	X		X		X	05	NONE			
IGG0CLX0	CAS	X	X	X	X	X		00	NONE	X		
IHLGTF	GTF	X	X		X			00	NONE			X
IKTCAS00	TCAS	X		X	X			06	NONE			

PROGRAM NAME	*PROGRAM DESCRIPTION*	*NC*	*NS*	*PR*	*ST*	*ND*	*BP*	*KEY*	*PROC AFFINITY*	*2P*	*1P*	*NP*
IOSVROUT	IOS	X	X		X		X	00	NONE			
IRRSSM00	RACF	X	X	X	X			02	NONE			
ISFHCTL	SDSF		X					01	NONE			
ISTINM01	VTAM	X	X		X		X	06	NONE			X
ITTTRCWR	CTRACE Writer Address Space	X	X	X	X		X	00	NONE	X	X	
IWMINJST	WLM	X	X		X			00	NONE			X
IXCINJST	XCF	X	X		X			00	NONE	X	X	
IXGBLF00	System Logger Address Space		X		X			00	NONE			
IXGBLF01	System Logger Address Space	X	X		X			00	NONE	X	X	
IXZIX00	JES Common Coupling Address Space	X	X	X	X			01	NONE			
MVPTNF	TNF Address Space	X	X	X	X			00	NONE			
MVPXVMCF	VMCF Address Space	X	X	X	X			00	NONE			
SNALINK	SNALINK Address Space		X		X			06	NONE			

The following table lists the known user-defined Program Properties Table (PPT) entries and values in effect at DISA sites. Vendor documentation has been verified to include both IBM and non-IBM programs:

PROGRAM NAME	VENDOR	PROGRAM DESCRIPTION	NC	NS	PR	ST	ND	BP	KEY	PROC AFFINITY	2P	1P	NP
CSQYASCP	IBM	MQSeries				X			07	NONE			X
CTOMTO7	New Dimension	Control-O							07				
FNMASMAN	IBM	NetView Synergy Interface (NSI)		X					06	NONE			
FNMMAIN	IBM	NetView Performance Monitor (NPM)		X					06	NONE			
HGLSSTC	Allegro Consultants	Y2K Processing	X	X	X	X			00	NONE			
SLSBINIT	StorageTek	Required for Tape Silo Systems				X			03	NONE			

SYNONYM	MEANING	SCHEDxx KEYWORD
NC	Non-cancelable	NOCANCEL
NS	Non-swappable	NOSWAP
PR	Privileged	PRIV
ST	System task	SYST
ND	No data set integrity	NODSI
BP	Bypass password protection	NOPASS
Key	PSW key for this program	KEY(x)
Proc Affinity	Processors eligible	AFF(y)
2P	Second-level preferred storage	SPREF
1P	First-level preferred storage	LPREF
NP	No preferred storage	NOPREF

APPENDIX C. IBM SMF RECORDS TO BE COLLECTED AT A MINIMUM

0 (00) – IPL
6 (06) – External Writer/ JES Output Writer/ Print Services Facility (PSF)
7 (07) – [SMF] Data Lost
14 (0E) – INPUT or RDBACK Data Set Activity
15 (0F) – OUTPUT, UPDAT, INOUT, or OUTIN Data Set Activity
17 (11) – Scratch Data Set Status
18 (12) – Rename Non-VSAM Data Set Status
24 (18) – JES2 Spool Offload
25 (19) – JES3 Device Allocation
26 (1A) – JES Job Purge
30 (1E) – Common Address Space Work
32 (20) – TSO/E User Work Accounting
43 (2B) – JES Start
45 (2D) – JES Withdrawal/Stop
47 (2F) – JES SIGNON/Start Line (BSC)/LOGON
48 (30) – JES SIGNOFF/Stop Line (BSC)/LOGOFF
49 (31) – JES Integrity
52 (34) – JES2 LOGON/Start Line (SNA)
53 (35) – JES2 LOGOFF/Stop Line (SNA)
54 (36) – JES2 Integrity (SNA)
55 (37) – JES2 Network SIGNON
56 (38) – JES2 Network Integrity
57 (39) – JES2 Network SYSOUT Transmission
58 (3A) – JES2 Network SIGNOFF
60 (3C) – VSAM Volume Data Set Updated
61 (3D) – Integrated Catalog Facility Define Activity
62 (3E) – VSAM Component or Cluster Opened
63 (3F) – VSAM Catalog Entry Defined
64 (40) – VSAM Component or Cluster Status
65 (41) – Integrated Catalog Facility Delete Activity
66 (42) – Integrated Catalog Facility Alter Activity
67 (43) – VSAM Catalog Entry Delete
68 (44) – VSAM Catalog Entry Renamed
69 (45) – VSAM Data Space Defined, Extended, or Deleted
80 (50) – RACF/TOP SECRET Processing
81 (51) – RACF Initialization
83 (53) – RACF Audit Record For Data Sets
90 (5A) – System Status
92 (5C) except subtypes 10, 11 – OpenMVS File System Activity
101 (65) – DATABASE 2 Accounting
103 (67) - IBM HTTP Server
110 (6E) – CICS/ESA Statistics
118 (76) – TCP/IP Statistics
230 – ACF2 or as specified in **ACFFDR** (vendor-supplied default is 230)

This page is intentionally left blank.

APPENDIX D. CA-SYSVIEW/E COMMANDS

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
ABENDX	X									
ACTIVITY	X	X								
AGENTS	X	X								
ALERTS	X	X								
ALLFILES	X	X								
ALLIST	X									
ALLOCAS	X	X								
ALLOCDS	X	X								
APFLIST	X									
APPCOUTQ	X	X								
APPLMON	X	X								
APPLMOND	X	X								
AR	X									
ASADMIN	X	X								
ASID	X									
ASVT	X									
ATLIST	X									
ATTNX	X									
AXATABLE	X									
BOTTOM	X	X	X	X	X	X	X	X	X	X
BROWSE	X	X	X	X	X	X	X	X	X	X
CA90LMP	X									
CA90RIM	X									
CA90SMF	X									
CACHECTL	X	X								
CACHEDEV	X	X								
CAIDS	X									
CARTM	X	X								
CATALOG	X									
CCONFIG	X			X						
CDBCTL	X			X	X					
CDB2CON	X	X		X	X					
CDB2ENTR	X				X					
CDB2PLAN	X				X					
CDB2RCT	X				X					
CDIR	X			X						
CDOMAINS	X			X						

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
CDSAS	X			X						
CDSAX	X			X						
CDUMPMGT	X			X						
CDUMPS	X			X						
CEDA	X			X						
CELEMENT	X			X						
CELLPOOL	X									
CEMT	X			X						
CENQPOOL	X	X		X						
CENQUEUE	X	X		X						
CFCACHE	X	X								
CFCONFIG	X	X								
CFILES	X									
CFLIST	X	X								
CFPATH	X	X								
CFPROC	X	X								
CFSTRUCT	X	X								
CFUSER	X	X								
CGBLEXIT	X			X						
CGROUPS	X	X		X						
CHANGES	X	X	X	X	X	X	X	X	X	X
CHANPATH	X	X								
CICE				X						
CICS	X	X		X						
CICSLOGR	X	X		X						
CIMS	X			X			X			
CIMSDMB	X			X			X			
CIMSPSB	X			X			X			
CIMSSTAT	X	X		X			X			
CIMSTASK	X	X		X			X			
CJMODEL	X	X		X						
CJOURNAL	X	X		X						
CKTCB	X			X						
CLIFE	X	X		X						
CLIST	X	X								
CLISTLIB	X	X								
CLOGS	X			X						
CLSRBUFF	X			X						
CLSRPOOL	X			X						

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
CMCT	X			X						
CMONITOR	X			X						
COLS	X	X	X	X	X	X	X	X	X	X
COMMENT	X	X	X	X	X	X	X	X	X	X
COMMON	X									
CONFLICT	X	X								
CONSOLE	X	X								
CONTROL	X	X								
COPYOUTP	X	X								
CPAS	X			X						
CPFTABLE	X	X								
CPROGRAM	X			X						
CPU	X	X								
CREMOTE	X	X		X						
CREVIEW	X	X		X						
CSFBUSY	X			X		X				
CSFCODES	X			X		X				
CSFIO	X			X		X				
CSFLOAD	X			X		X				
CSFTABLE	X			X		X				
CSFTASKS	X			X		X				
CSFTCBS	X			X		X				
CSFTRACE	X			X		X				
CSFREQS	X			X		X				
CSFURTS	X			X		X				
CSFUSERS	X			X		X				
CSIT	X			X						
CSRT	X			X						
CSTATUS	X			X						
CSUBPOOL	X			X						
CSUBSPAC	X			X						
CSYMBOLS	X			X						
CSYSDATA	X			X						
CTASKENT	X			X						
CTASKS	X	X		X						
CTCLASS	X			X						
CTDATA	X			X						
CTEMPSTG	X			X						
CTERMS	X	X		X						

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
CTHRESH	X	X		X						
CTIMERS	X	X		X						
CTRANLOG	X			X						
CTRANS	X			X						
CTRANSUM	X			X						
CTSQUEUE	X			X						
CUMBRELA	X			X						
CURSOR	X	X	X	X	X	X	X	X	X	X
CUSERS	X		X							
CVARLIST	X			X						
CVSAM	X	X		X						
CWAITS	X	X		X						
CXLOG	X	X		X						
DASD	X	X								
DAT	X									
DATACOM	X					X				
DATE	X	X	X	X	X	X	X	X	X	X
DCACCESS	X					X				
DCACNT	X					X				
DCAREAIO	X					X				
DCAREAS	X					X				
DCBUFFER	X					X				
DCCOLUMN	X					X				
DCDBASES	X					X				
DCDIR	X					X				
DCDSETS	X					X				
DCELEMEN	X					X				
DCKEYFLD	X					X				
DCKEYS	X					X				
DCLOG	X					X				
DCMRDF	X					X				
DCMUFS	X					X				
DCOPEN	X					X				
DCOPTION	X					X				
DCPRODS	X					X				
DCRATES	X					X				
DCREQS	X					X				
DCSMP	X					X				
DCSMPTSK	X					X				

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
DCSTATS	X					X				
DCSYSTEM	X					X				
DCTABLES	X					X				
DCTABREQ	X					X				
DCTASKS	X					X				
DCVOLUME	X					X				
DCXCF	X					X				
DDLIST	X									
DELMAPS	X									
DEST	X	X								
DESTID	X	X								
DEVPATH	X	X								
DISASSEM	X									
DOMAIN	X	X								
DOWN	X	X	X	X	X	X	X	X	X	X
DROP	X									
DSALLOC	X	X								
DSCAT	X	X	X	X	X	X	X	X	X	X
DSID	X	X								
DSINFO	X	X	X	X	X	X	X	X	X	X
DSLIST	X									
DUMP	X									
DUMPDS	X	X								
DUMPOPTS	X									
DUPLICAT	X									
DYNEXIT	X									
ECHO	X	X	X	X	X	X	X	X	X	X
EDIT	X	X	X	X	X	X	X	X	X	X
EDT	X	X								
EFRAMES	X									
END	X	X	X	X	X	X	X	X	X	X
ENFLIST	X									
ENQJOB	X	X								
ENQSUM	X	X								
ENQUEUE	X	X								
EQUATE	X									
ESRTABLE	X									
EST	X									
ETCON	X									

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
ETLIST	X									
ETRINFO	X									
EXTENTS	X	X								
FIND	X	X	X	X	X	X	X	X	X	X
FLUSH	X									
FRAMES	X									
FREEMAIN	X									
GETMAIN	X									
HELP	X	X	X	X	X	X	X	X	X	X
HEX	X									
HSMREQ	X	X								
IDCAMS	X									
IDENTIFY	X									
INDEX	X									
INIT	X	X								
INTRDR	X	X								
INVOKE	X									
IOCDATA	X									
IPLINFO	X	X								
ISERVE	X									
ISPFCMD	X	X	X	X	X	X	X	X	X	X
ISPTCM	X									
JINPRTY	X	X								
JLOGON	X	X								
JOBCLASS	X	X								
JOBSUM	X	X								
JPA	X									
JPATHS	X	X								
JREMOTES	X	X								
JRESOURC	X	X								
JSESSION	X	X								
KEYS	X	X	X	X	X	X	X	X	X	X
LABEL	X	X	X	X	X	X	X	X	X	X
LEFT	X	X	X	X	X	X	X	X	X	X
LINES	X	X								
LINK	X	X	X	X	X	X	X	X	X	X
LINKACT	X									
LINKDEF	X									
LINKDEL	X									

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
LINKJOBS	X									
LINKLIBS	X									
LINKLIST	X									
LINKOPT	X									
LINKSETS	X									
LINKUPD	X									
LISTCICS	X	X		X						
LISTCONS	X	X								
LISTDCOM	X	X				X				
LISTDIR	X	X	X	X	X	X	X	X	X	X
LISTFILE	X	X								
LISTHELD	X	X								
LISTINP	X	X								
LISTJOBS	X	X								
LISTLAB	X	X	X	X	X	X	X	X	X	X
LISTLOAD	X									
LISTMAPS	X									
LISTMODS	X									
LISTMVAR	X									
LISTOUT	X	X								
LISTSEL	X	X	X	X	X	X	X	X	X	X
LISTSYS	X	X								
LLAREFR	X									
LOADMAPS	X									
LOCATE	X	X	X	X	X	X	X	X	X	X
LOGREC	X	X								
LOOKUP	X	X	X	X	X	X	X	X	X	X
LPA	X									
LPALIST	X									
LXATABLE	X									
MAP	X									
MAPLIB	X									
MASTER		X								
MENU	X	X	X	X	X	X	X	X	X	X
MODIFY	X	X	X	X	X	X	X	X	X	X
MOREINFO	X	X								
MPFTABLE	X									
MQACTIVE	X	X							X	
MQALERTS	X	X							X	

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
MQBROWSE	X	X							X	
MQCHAN	X	X							X	
MQCHCCON	X	X							X	
MQCHRCVR	X	X							X	
MQCHRQSR	X	X							X	
MQCHSCON	X	X							X	
MQCHSNDR	X	X							X	
MQCHSRVR	X	X							X	
MQCHSTAT	X	X							X	
MQCLEAN	X	X							X	
MQCLEAR	X	X							X	
MQCMD	X	X							X	
MQCONN	X	X							X	
MQDEAD	X	X							X	
MQDISC	X	X							X	
MQDQMGR	X	X							X	
MQEVENT	X	X							X	
MQINDOUT	X	X							X	
MQLIST	X	X							X	
MQLOG	X	X							X	
MQMGR	X	X							X	
MQNAME	X	X							X	
MQPAGE	X	X							X	
MQPERF	X	X							X	
MQPROC	X	X							X	
MQQALIAS	X	X							X	
MQQLOCAL	X	X							X	
MQQMODEL	X	X							X	
MQQREMOT	X	X							X	
MQQUEUE	X	X							X	
MQRMGR	X	X							X	
MQSECUR	X	X	X						X	
MQSERIES	X	X							X	
MQSTGCL	X	X							X	
MQTHRESH	X	X							X	
MQTRACE	X								X	
MSGCOLOR	X	X								
MTT	X									
MVS		X								

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
NAMETOKN	X									
NODES	X	X								
NOOP	X	X	X	X	X	X	X	X	X	X
NUCLEUS	X									
OFFLOAD	X	X								
OUTCLASS	X	X								
OUTDES	X	X	X	X	X	X	X	X	X	X
OUTPUT	X	X	X	X	X	X	X	X	X	X
OWNER	X	X	X	X	X	X	X	X	X	X
PAGEDS	X									
PAGES	X									
PAGING	X									
PARMLIB	X									
PARMLIST	X									
PARTINFO	X	X								
PCLIST	X									
PFSHOW	X	X	X	X	X	X	X	X	X	X
PFT	X									
PLEXARM	X	X								
PLEXCPL	X	X								
PLEXGRPS	X	X								
PLEXMBRS	X	X								
PLEXPATH	X	X								
PLEXPEND	X	X								
PLEXSYS	X	X								
PLOT	X	X								
PLOTATTR	X	X								
PLOTLIB	X	X								
PLOTLIST	X	X								
PLOTLOG	X	X								
PPT	X									
PREFIX	X	X	X	X	X	X	X	X	X	X
PRINT	X	X	X	X	X	X	X	X	X	X
PRINTER	X	X								
PRISM	X	X								
PRIVATE	X									
PROCLIST	X									
PRODCODE	X									
PRODUCTS	X									

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
PROFILE	X	X	X	X	X	X	X	X	X	X
PROMPT	X	X	X	X	X	X	X		X	X
PUNCH	X	X								
QUERY	X	X	X	X	X	X	X	X	X	X
QUICKREF	X	X								
READER	X	X								
RECALL	X	X	X	X	X	X	X	X	X	X
REGION	X									
REGPRODS	X									
REPEAT	X	X	X	X	X	X	X	X	X	X
RESERVE	X	X								
RETURN	X	X	X	X	X	X	X	X	X	X
REVIEW	X	X	X	X	X	X	X	X	X	X
RIGHT	X	X	X	X	X	X	X	X	X	X
RNLIST	X	X								
ROSAWS	X	X						X		
ROSBUFF	X	X						X		
ROSCOE	X	X						X		
ROSLIBS	X	X						X		
ROSLIST	X	X						X		
ROSMON	X	X						X		
ROSMPL	X	X						X		
ROSRESP	X	X						X		
ROSUSER	X	X						X		
SCM	X	X						X		
SCREEN	X	X	X	X	X	X	X	X	X	X
SECURITY			X							
SEGMENTS	X									
SELECT	X	X	X	X	X	X	X	X	X	X
SESSIONS	X	X								
SET	X	X	X	X	X	X	X	X	X	X
SFTABLE	X									
SMF	X	X								
SMFEXIT	X									
SNAP	X									
SORT	X	X	X	X	X	X	X	X	X	X
SPACE	X	X								
SPLIT	X	X	X	X	X	X	X	X	X	X
SPOOLS	X	X								

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
STATUS	X									
STCK	X	X	X	X	X	X	X	X	X	X
STEPSUM	X	X	X	X	X	X	X	X	X	X
STORGRP	X	X								
STREXCL	X	X								
STRLIST	X	X								
STRPREF	X	X								
SUBCHAN	X	X								
SUBMIT	X	X	X							
SUBPOOL	X									
SUBSYS	X									
SVCTABLE	X									
SWAP	X	X	X	X	X	X	X	X	X	X
SWAPDS	X									
SWAPPING	X									
SYMBOLS	X									
SYMPTOMS	X									
SYSGROUP	X	X								
SYSLOG	X	X								
SYSSYM	X									
SYSVIEW	X	X	X	X	X	X	X	X	X	X
TAPE	X	X								
TASK	X									
TASKLIB	X									
TERMINAL	X	X	X	X	X	X	X	X	X	X
THRESH	X	X								
TIME	X	X	X	X	X	X	X	X	X	X
TIMERS	X									
TIMEZONE	X	X								
TOP	X	X	X	X	X	X	X	X	X	X
TOPICS	X	X	X	X	X	X	X	X	X	X
TOTAL	X	X	X	X	X	X	X	X	X	X
TRACE	X									
TSO	X	X	X	X	X	X	X	X	X	X
TSOTABLE	X									
TYPE	X	X	X	X	X	X	X	X	X	X
UNIT	X	X								
UP	X	X	X	X	X	X	X	X	X	X
UPDATE	X	X	X	X	X	X	X	X	X	X

	SYSPROG	OPER	ADMIN	CICS	DB2	DATACOM	IMS	ROSCOE	MQ	GLOBAL
USE	X									
USERS	X	X	X							
VALPATH	X	X								
VCHECK	X	X	X	X	X	X	X	X	X	X
VDEFAULT	X	X	X	X	X	X	X	X	X	X
VDEFINE	X	X	X	X	X	X	X	X	X	X
VDELETE	X	X	X	X	X	X	X	X	X	X
VIEW	X	X	X	X	X	X	X	X	X	X
VLFIELD	X	X	X	X	X	X	X	X	X	X
VLFLIST	X	X	X	X	X	X	X	X	X	X
VLIST	X	X	X	X	X	X	X	X	X	X
VM	X	X								
VRESET	X	X	X	X	X	X	X	X	X	X
VSET	X	X	X	X	X	X	X	X	X	X
VSMTRACK	X									
VTAM	X	X								
VTOC	X	X								
WAIT	X	X	X	X	X	X	X	X	X	X
WTOACTN	X	X								
WTOR		X								
XCFADMIN	X	X								
XCONSOLE		X								
XMVS		X								
ZAP	X									

APPENDIX E. FORMS

ACKNOWLEDGEMENT OF RISK LETTER FOR DATA TRANSFER INTERFACE USERIDS <date>

This document has been removed from this STIG and will be placed in a different manual to be shared by all technologies. Once the manual name is decided, the STIG will be updated to reference the new manual.

This page is intentionally left blank.

SAMPLE MEMORANDUM OF UNDERSTANDING (MOU)

1. **PURPOSE:** This MOU policy is to establish and assign responsibilities for the decentralized security functions, security maintenance and security training for the DISA Area Command Ogden decentralized security system. This decentralized security system is being developed for the Centralized Purchasing and Accounting System (CPAS) which will encompass both Ogden and Oklahoma City Area Commands. This agreement will define the roles and responsibilities of the CPAS Operating Locations (OPLOCs) decentralized administrators and the DISA Area Commands. AC Ogden will develop these decentralized CPAS security programs as requested by the OPLOC CPAS customers.

2. DAC's Ogden and Oklahoma City Software/Security Roles and Responsibilities:

   a. DAC's Ogden and Oklahoma City will:

      1) Maintain the Operating System software packages for IBM system, OS390, CA-TOP SECRET, etc.

      2) Provide security technical support and assistance as requested.

      3) Provide overall maintenance support for the IBM security system, CA-TOP SECRET.

      4) Monitor overall system security violations.

      5) Monitor CPAS userid activity. If the CPAS userid is inactive over the specified limit (currently 180 days) and the CPAS decentralized administrator has not taken action, DAC Ogden/Oklahoma City will delete the userid with no prior notification to the CPAS OPLOC. This action is required to maintain the security environment consistent with applicable security policy and guidelines.

      6) Serve as the backup Point of Contact for CPAS users with security problems. (CPAS users will contact AC help desks FIRST, prior to contacting DAC Security Administrators.)

      7) Develop and maintain CPAS security profiles, as required, granting access to the CPAS application. The Security Administrators located at the DISA Area Commands will maintain these profiles.

      8) Provide TSO access, on a limited basis, as required. Access request forms will be processed through the appropriate central Security Administrators.

   b. In addition, DAC Ogden will:

      1) Design, text, and implement the CPAS decentralized security programs.

      2) Isolate and resolve all decentralized security software technical problems.

      3) Provide decentralized security training for the CPAS OPLOC customers. (The CPAS customers will incur the TDY costs for DAC security trainers.)

   c. CPAS OPLOC decentralized Security Administrators will:

      1) Serve as Security Administrators for the CPAS application and abide by all DOD, DISA, and other applicable security regulations, policies, and guidelines.

      2) Serve as the main security Point of Contact for all CPAS users with security problems.

      3) Grant access to the CPAS application using security profiles provided and designated by the Area Commands.

4) Ensure System Authorization Access Requests (DISA Form 41s) are filled out in accordance with (IAW) DISA specifications and all other applicable regulatory guidelines.

5) Maintain CPAS access request form files at the OPLOC sites in accordance with DISA policy. Upon request, OPLOCs will provide Area Commands with user access request forms as needed for audits and/or investigations.

6) Add/modify/delete/suspend/unsuspend/maintain all CPAS decentralized application userids.

7) Be responsible for auditing security violations and deleting inactive CPAS user accounts in accordance with inactivity thresholds (currently 180 days).

8) Successfully complete all training requirements as specified by DISA.

Defense Financial and Accounting Systems (DFAS)

Michele Garneau
DFAS

Area Commands

AC Oklahoma City

Rod Sloan
(IAM) Security

Douglas Holland
Chief of Security

Rudy Vines
Deputy Commander
Area Command
Oklahoma City

AC Ogden

Stephen R. Fletcher
(Lead) System Software Programmer

Bruce Waltz
Branch Chief
Logistics Support Branch

Val Lofgreen
Deputy Commander

APPENDIX F. SECTIONS IN DEVELOPMENT

F.9.2 IMS/DB/DC

Vendor: IBM Corporation

IMS/DB/DC (Information Management System/Database/Data Communications) provides facilities to develop databases and to perform interactive access to the defined databases.

Internal Product Security Controls within IMS provide the capability to restrict access for the product's functions. User data is potentially accessible without appropriate approvals.

Use the ACP to ensure that authorization is managed by the IAO.

Apply the following recommendations for IMS security controls:

(1) Control access to an IMS system for a user using the ACP.

(2) At a minimum, implement transaction-level checking in all IMS regions.

(3) Several commands within IMS are sensitive in nature and will be restricted for the orderly execution of IMS. At a minimum, restrict the following commands to authorized personnel:

DELETE	START	MODIFY
ERESTART	STOP	MONITOR
EXCLUSIVE	TRACE	MSASSIGN
IDLE	MSVERIFY	MSVERIFY
LOOPTEST	NRESTART	NRESTART
MODIFY	ERESTART	OPNDST
MONITOR	EXCLUSIVE	QUIESCE
MSASSIGN	IDLE	RECOMPT
SWITCH	LOOPTEST	SMCOPY
SSR		

Coordinate authorization for command use between the IAO, Operations, and IMS support personnel.

F.9.2.1 ACF2

Secure every IMS control region using the ACF2/IMS sub-product. This allows I&A processing and the verification of resource access within IMS.

Assign every IMS region a unique @MUSASS and @MLID macro pair in the ACF2 ACFFDR. Assign every IMS region a unique set of the following:

(1) The seven IMS region logonids (STC or batch):

BMP region logonid
Control region logonid
DBRC region logonid
DLISAS region logonid
Fast path region logonid
IMSRDR region logonid
Message processing region logonid

(2) The three default logonids:

IMS control region default logonid
IMS Internal Product Security Control link default logonid
IMS MSC link default logonid

(3) IMS control region sign-on authorization flag

(4) IMS region enqueue major name

(5) A unique set of ACF2 Infostorage IMS control records, associated with the control region by each control record's DIVISION field (containing the MUSID from the control region's logonid record)

(6) A unique set of primary and secondary IMS transaction types (specified in ACF2 Infostorage IMS Control RESOURCE records), associated with the control region by each control record's DIVISION field (containing the MUSID from the control region's logonid record)

Every IMS control region will process in ABORT mode, as specified in the OPTS ACF2 Infostorage IMS control record.

The ability to update the ACF2 Infostorage IMS control records for an IMS region will be strictly controlled.

F.9.2.2 RACF

*** Information was not available at the time this document was prepared. ***
*** Recommendations for this product will be added in a future update to this document. ***

F.9.2.3 TOP SECRET

*** Information was not available at the time this document was prepared. ***
*** Recommendations for this product will be added in a future update to this document. ***

F.9.3 MICS

Vendor: Computer Associates

MICS is a comprehensive information systems management product. It uses an SAS-managed database to store information about the MVS operating system, subsystems, and applications. MICS employs a series of regularly scheduled batch jobs to load information into its database. It provides many reports that can be used to analyze the data. The MICS Workstation Facility (MWF), a powerful ISPF dialog application used by general users and MICS administrators, is included with the product.

MICS security management will be implemented by using a combination of ACP and Internal Product Security Controls. MICS internal security must be used within the MWF. MICS currently does not make use of the MVS SAF facility.

The MICS environment is comprised of numerous data sets classified in two distinct categories:

- Complex (or sharedprefix) level
- Unit (or prefix) level

Both the MICS administrator and the backup administrator must have complete access to both complex and unit-level data sets.

The integrity of the data within the MICS database is strictly based on the data set controls in effect for the SMF data and other data used as input into the MICS processes. Rigid data set controls are essential to ensure the integrity of the MICS environment. Refer to *Section 3.1.5.1, Data Set Controls*, for further information.

Use the following recommendations to control access to MICS:

(1) Complex-level (sharedprefix) data set considerations are as follows:

(a) MICS users will be restricted to *read* authority except the <sharedprefix>.MICS.LOAD library, which is restricted to *program execute only* authority.

(b) MICS production jobs will be restricted to *read* authority except the <sharedprefix>.MICS.LOAD library, which is restricted to *program execute only* authority.

(c) MICS System Administrators require, and will be granted, complete access to all complex-level data sets.

(d) The authorized exceptions to complex-level (sharedprefix) data set access *read-only* authority are as follows:

1) <sharedprefix>.MICS.CAPACITY

The MICS Capacity Planner uses this data set. Only MICS users responsible for capacity planning or production jobs that update this file will be granted *read* and *update* authority to this data set.

2) <sharedprefix>.MICS.TABLES

MICS Accounting and Charge-back uses this data set. The data entered in this file is done so manually or by monthly Accounting and Charge-back processing. Only the MICS Accounting and Charge-back administrator, the person(s) responsible for entering accounting data from MWF, and production jobs that update this file will be granted *read* and *update* authority to this data set.

3) <tsharedprefix>.MICS.ACCT.MONTHC

This data set is kept on tape as indicated by the different high-level qualifier. It contains all the debits and credits used to create the Financial Recap file. Only the MICS Accounting and Charge-back administrator and production jobs, such as CLOSETBL, INVOICE, and FINRECAP, will be granted *alter*, *read*, and *update* authority to this data set.

4) <sharedprefix>.MICS.MWFPDS.DATA

The MICF Shared Output Catalog feature uses this data set. Reports produced from MICS inquiries are stored in this file for later review. Only MICS users responsible for adding reports and deleting existing entries and for production jobs, such as DAILYRPT, WEEKRPT, and MONTHRPT, will be granted *read* and *update* authority to this data set.

5) <sharedprefix>.MICS.MWFSAS.DATA

The MICF Shared Output Catalog feature uses this data set. Color graphics produced from MICS inquiries are stored in this file for later review. Only MICS users responsible for adding reports and deleting existing entries and for production jobs, such as DAILYRPT, WEEKRPT, and MONTHRPT, will be granted *read* and *update* authority to this data set.

6) <sharedprefix>.MICS.DTF.INDEX

This data set is used by the EasyReach Data Manager (EDM) as a directory to all EDM files. Only MICS users responsible for creating EDM files and for production jobs, such as DAILYRPT, WEEKRPT, and MONTHRPT, will be granted *read* and *update* authority to this data set.

7) <sharedprefix>.MICS.ISPTLIB

Many different features within MWF use this data set. Only persons responsible for batch production reporting jobs, and for the following functions, will be granted *read* and *update* authority to this data set:

a) Updating the Shared Inquiry Catalog
b) Updating the Shared Inquiry Output Catalog
c) Updating the Shared MICF Options
d) Performing Production Reporting administration
e) Printing MICS documentation
f) Updating Accounting and Charge-back parameters
g) Updating the Shared Capacity Planning file

(2) Unit-level (prefix) data set considerations are as follows:

(a) Restrict MICS users to *read* authority.

(b) Restrict MICS production jobs to *read* and *update* authority.

(c) MICS System Administrators require, and will be granted, complete access to all unit-level (prefix) data sets.

(d) The ACP will log all *alter* and *update* access to the unit-level (prefix) data sets (except MICS production jobs).

The MICS complex contains multiple units, and each unit consists of one or more MICS components. The units are grouped together by informational area. For instance, one unit may contain OS/390 performance data and another unit may consist of DASD management data.

Each unit consists of a group of data sets specific to that unit, meaning they are not shared among other units. This group of files includes MICS application data sets and database files. To differentiate one set of MICS unit data sets from another, unique high-level data set qualifiers or prefixes are used.

Each MICS unit will be considered a separate entity and will be individually protected against unauthorized access. For example, MICS users responsible for accessing OS/390 performance data will not be given access to DASD management data. The unique prefixes between units will be used to facilitate security within each ACP.

(3) Another group of MICS unit data sets pertains to backup and archive processing. These data sets are indicated by a MICS tapeprefix.

Unit-level (tapeprefix) data set considerations are as follows:

(a) Restrict MICS users to *read* authority.

(b) Restrict MICS production jobs to *alter*, *read*, and *update* authority.

(c) MICS System Administrators require, and will be granted, complete access to all unit-level (tapeprefix) data sets.

(d) The ACP will log all *alter* and *update* access to the unit-level (tapeprefix) data sets (except MICS production jobs).

(e) An authorized exception to unit-level (tapeprefix) data set access authority exists for the MICS Accounting and Charge-back administrator. This administrator requires, and will be granted, complete access to the following data sets:

1) <tapeprefix>.MICS.ACCT.DAY1

This data set contains current month-to-date DETAIL-level data from all the journal files.

2) <tapeprefix>.MICS.ACCT.DAY2

This data set is a backup of the DAY1 file.

3) <tapeprefix>.MICS.ACCT.MONTH

This data set contains a complete month of data for a previous month at the DETAIL-level from all the journal files.

(4) The MICS MWF (MICS Workstation Facility) is a set of powerful ISPF dialog applications used to provide access to the MICS complex. The invocation of the MICS MWF driver application is through a clist. Limit the execution of this clist only to MICS users and administrators.

MWF does not interface with SAF at present. It has its own internal security application, Authorization Assignment, which will be used to limit access to each MWF application, and to restrict the use of options within those applications. Refer to the *MICS PIOM (Planning, Installation, Operation, and Maintenance) Guide, Section 4.4.3*, for details on how to set up MWF internal security.

NOTE: A possible security exposure exists within MWF regarding MICS internal security. The MICS Authorization Assignment facility uses the ISPF table format to store its security information. If a user creates a security table and allocates it before the MICS ISPTLIB data set, MWF will use the user-created table instead, thus bypassing MICS internal security.

(5) For batch production jobs, a unique batch logonid will be used for each distinct MICS unit when submitting any scheduled MICS production job, such as DAILY, WEEKLY, MONTHLY, YEARLY, BACKUP, etc. These batch logonids will be the only logonids with *update* authority to the MICS database files, except for the MICS System Administrator, as discussed in *Section H.9.3, MICS, Paragraph (2)(c)*.

The batch logonids and MICS System Administrator will be the only logonids with the authority to *alter* and *update* the audit, history, and backup tapes, as discussed in *Section H.9.3, MICS, Paragraph (3)(c)*.

Any *restore* processing of the MICS complex and unit data sets, along with the MICS database files, will be strictly handled by the MICS System Administrator. Any MICS Accounting and Charge-back files requiring *restore* processing may be alternatively handled by the MICS Accounting and Charge-back administrator.

F.9.3.1 ACF2

MICS external security utilizing ACF2 will be accomplished through data set resource controls. Refer to *Section H.9.3, MICS*, for information on MICS data set access authority requirements. For additional information on data set resource controls, refer to *Section 3.1.5.1, Data Set Controls*.

MICS internal security will be used to secure the MICS MWF environment. Refer to *Section H.9.3, MICS, Paragraph (4)* for further information.

For additional information about MICS data sets and MICS internal security, refer to the *MICS PIOM (Planning, Installation, Operation, and Maintenance) Guide*.

F.9.3.2 RACF

MICS external security utilizing RACF will be accomplished through data set resource controls. Refer to *Section H.9.3, MICS,* for information on MICS data set access authority requirements. For additional information on data set resource controls, refer to *Section 3.1.5.1, Data Set Controls*.

MICS internal security will be used to secure the MICS MWF environment. Refer to *Section H.9.3, MICS, Paragraph (4)*, for further information.

For additional information about MICS data sets and MICS internal security, refer to the *MICS PIOM (Planning, Installation, Operation, and Maintenance) Guide*.

F.9.3.3 TOP SECRET

MICS external security utilizing TOP SECRET will be accomplished through data set resource controls. Refer to *Section H.9.3, MICS*, for information on MICS data set access authority requirements. For additional information on data set resource controls, refer to *Section 3.1.5.1, Data Set Controls*.

MICS internal security will be used to secure the MICS MWF environment. Refer to *Section H.9.3, MICS, Paragraph (4)*, for further information.

For additional information about MICS data sets and MICS internal security, refer to the *MICS PIOM (Planning, Installation, Operation, and Maintenance) Guide*.

F.10.2 FDR (Fast Dump Restore)

Vendor: Innovation Data Processing

FDR (Fast Dump Restore) and its associated sub-products allow backup and restoration of data on DASD. Optional capabilities include optimization of data set placement, release of unused space, and extent management.

The product, as provided by the vendor, allows unlimited access to DASD resources. The product operates on a track level, versus a data set level, thus potentially bypassing security validation routines.

Interfaces are provided with the product that allows it to query the ACP for verification of the access request at the data set and/or volume level. Install this interface to support discretionary access controls.

The FDRZAPOP utility allows an installation to set up the security controls, as well as other installation options. The FDRZAPOP program will be protected. (Refer to *Section 3.1.5.3, Sensitive Utility Controls*, for further information.)

Control maintenance jobs that back up data for use in recovery situations with batch userid controls designed for such processes. (Refer to *Section 3.1.2.5, Special Storage Management Users*, for further information.)

F.10.2.1 ACF2

Access to the FDRZAPOP utility (used to modify FDR) will be protected using the Protected Program List facility, as discussed previously. (Refer to *Section 3.2.5.3, Sensitive Utility Controls*, for further information.) Standard data set access rules are required for the library containing the program.

FDR will be installed with full volume-level and data set-level validation enabled. Use the FDR exits, FDRYOPEN and FDRYPASS, supplied with ACF2 to accomplish this. This will ensure that data set *backup* and *restore* functions and full-volume *restore* functions are protected via data set rules.

F.10.2.2 RACF

Access to the FDRZAPOP utility (used to modify FDR) will be protected as a protected program, as discussed previously. (Refer to *Section 3.3.5.3, Sensitive Utility Controls* for further information.) Standard data set access protections are required for the library containing the program.

During the installation of FDR, generate the product with the ALLCALL option enabled. Protection of FDR processing is performed by SAF calls validated by RACF. Further documentation of the protection mechanisms can be found in the *Installation* section of the FDR product documentation.

F.10.2.3 TOP SECRET

Access to the FDRZAPOP utility (used to modify FDR) will be protected using appropriate TSS protection mechanisms. (Refer to *Section 3.3.5.3, Sensitive Utility Controls*, for further information.) Standard data set access rules are required for the library containing the program.

During the installation of FDR, generate the product with the ALLCALL option enabled. Protection of FDR processing is performed by SAF calls issued that TOP SECRET validates. Further documentation of the protection mechanisms can be found in the *Installation* section of the FDR product documentation.

F.10.4 ICKDSF

Vendor: IBM Corporation

ICKDSF is a tool used for the initialization, scanning, and debugging of DASD units. It is a stand-alone utility program provided by IBM to its customers as a courtesy. It also comes bundled as a standard component of OS/390. ICKDSF is known colloquially as DSF.

ICKDSF operates at the device level and does not interface with the ACP to verify individual data set access. Additionally, the utility can over-write selected tracks of data. Such capabilities pose a risk to data integrity.

Full volume-level access will be granted to authorized users through the volume protection capabilities of the ACP.

Access to ICKDSF will be protected using program protection controls. (Refer to *Section 3.1.5.3, Sensitive Utility Controls*, for further information.)

F.10.4.1 ACF2

Protect access to ICKDSF using the Protected Program List facility, as discussed in *Section 3.2.5.3, Sensitive Utility Controls*. Standard data set access rules are required and will be written for the library containing the utility.

F.10.4.2 RACF

Protect access to ICKDSF using the sensitive program protection mechanisms, as discussed in *Section 3.3.5.3, Sensitive Utility Controls*. Standard data set access rules are required and will be written for the library containing the utility.

F.10.4.3 TOP SECRET

Protect access to ICKDSF using the sensitive program protection mechanisms, as discussed in *Section 3.4.5.3, Sensitive Utility Controls*. Standard data set access rules are required and will be written for the library containing the utility.

F.12.3 NetView

Vendor: IBM Corporation

NetView is a powerful network management product. It provides facilities to monitor, control, interrogate, and analyze activities associated with network resources. It also allows an authorized user to execute VTAM and OS/390 commands from a terminal. The power of this application makes it dangerous in the hands of an unauthorized user. Therefore, access to NetView will be limited only to authorized persons. It is also necessary to distinguish between different users. Some users will require a large selection of the possibilities of NetView, while others will only need a small subset.

NetView Internal Product Security Controls can be used to limit access to NetView. This mechanism performs user identification, authentication, and validation based on security information stored in a NetView data set. However, all information (e.g., userids and passwords) is stored in clear text format, which makes this method of validation undesirable. A more secure approach is to use the services of an ACP.

Use the following recommendations to control access to NetView:

(1) Secure user access to NetView using the services of an ACP. Implementation details are documented in Section F.12.3.1, ACF2, Section F.12.3.2, RACF, and Section F.12.3.3, TOP SECRET.

(2) Define a span of control for each NetView user to limit the user control boundaries using the **ISPAN** and **SPAN** statements in the user's profile. The user cannot execute any command for a network resource that is outside that user's span of control. **SPAN** names are defined in member **DSISPN** of data set **DSIPARM** using the **SPANLIST** statement, and in **SYS1.VTAMLST** using the **SPAN** operand.

(3) Define the scope of commands for each NetView user using the **OPCLASS** statement in the profile data set to restrict users to the set of NetView commands that matches their roles, needs, and responsibilities.

(4) Define NetView as a started task with no special attribute.

(5) Restrict the ability to issue OS/390 commands only to NetView automation processes (e.g., **clist**). General users will not be given the authority to issue OS/390 commands.

(6) Use the services of an ACP to secure access to key NetView data sets. Restrict access to data sets having the following DD names in the NetView JCL start procedure only to the network systems programming staff and authorized users:

DSIPARM - NetView environment definitions
DSIPRF - NetView operator profiles
DSICLD - NetView **clist** libraries
STEPLIB - NetView load libraries
DSIVTAM - VTAM start options and definition statements

F.12.3.1 ACF2

Apply the following recommendations when using NetView with ACF2:

(1) Use ACF2 to perform authentication of userids, user passwords, and user terminal names by specifying **OPTIONS VERIFY=MAXIMUM** in member **DSIDMN** of the **DSIPARM** data set. When using this option with ACF2, the user passwords in member **DSIOPF** will no longer be used. ACF2 will perform password validation and pass a return code to NetView. If the return code is zero (**0**), NetView will allow the session. Otherwise, the logon request will be rejected. Under this same option, user profiles, scopes of command, and span of control authorities will remain in force and will continue to be controlled internally by NetView.

(2) Assign invalid values to all user passwords stored in member **DSIOPF** of the **DSIPARM** data set. They will not be used to authenticate any individual.

F.12.3.2 RACF

Use the following recommendations when using NetView with RACF:

(1) Use RACF to perform authentication of operator ID, operator password, and operator terminal name by specifying **OPTIONS VERIFY=MAXIMUM** in member **DSIDMN** of the **DSIPARM** data set. When using this option with RACF, the user passwords in member **DSIOPF** will no longer be used. RACF will perform password validation and pass a return code to NetView. If the return code is zero (**0**), NetView will allow the session. Otherwise, the logon request will be rejected. Under this same option, user profiles, scopes of command, and span of control authorities will remain in force and will continue to be controlled internally by NetView.

(2) Assign invalid values to all user passwords stored in member **DSIOPF** of the **DSIPARM** data set. They will not be used to authenticate any individual.

F.12.3.3 TOP SECRET

NetView will be defined as a TOP SECRET Facility (**FAC**). This **FAC** will be used to validate a user's authority to access NetView.

Apply the following recommendations when using NetView with TOP SECRET:

(1) Use TOP SECRET to perform authentication of userids, user passwords, and user terminal names by specifying **OPTIONS VERIFY=MAXIMUM** in member **DSIDMN** of the **DISPARM** data set. When using this option with TOP SECRET, the user passwords in member **DSIOPF** will no longer be used. TOP SECRET will perform password validation and pass a return code to NetView. If the return code is zero (**0**), NetView will allow the session. Otherwise, the logon request will be rejected. Under this same option, user profiles, scopes of command, and span of control authorities will remain in force and will continue to be controlled internally by NetView.

(2) Assign invalid values to all user passwords stored in member **DSIOPF** of the **DSIPARM** data set. They will not be used to authenticate any individual.

F.12.4 CA-EXAMINE

CA-EXAMINE is a software product that enables an organization to perform an analysis of its OS/390 hardware and software environment. CA-EXAMINE assists in monitoring the integrity of the OS/390 environment and determining the current system status.

CA-EXAMINE also provides the capability to maintain documentation related to the review of selected areas of MVS on-line. The status and results of a review can be stored within the EXAMINE product database itself and retained on an indefinite basis.

CA-EXAMINE runs as an ISPF application. It also can be run as a background (batch) job.

CA-EXAMINE requires *read* access to all load libraries that it will audit (e.g., libraries in the Linklist, APF list, etc.).

Section 2.1.4, Auditing, describes the requirements for using CA-EXAMINE as the repository for system documentation.

F.12.4.1 General Considerations

Use the following controls when installing CA-EXAMINE on each domain/system:

(1) The IAO will strictly control authorization to access the CA-EXAMINE environment. *Update* and *alter* access to the CA-EXAMINE product libraries will be restricted only to systems programming and security/audit personnel.

(2) All requests for access to CA-EXAMINE will be justified in writing and approved by the IAO.

(3) When installing CA-EXAMINE, create a **prefix.FSO.EXAMINE.CAIDBS1** file. This file will be the repository for system documentation, and will be retained permanently. The IAO will maintain on file the documented procedures for the maintenance and retention of this data set. Restrict *update* access to the following personnel:

DISA FSO/DOD SRR Personnel
Systems Programming Personnel
Local Audit Personnel

(4) Grant external audit personnel *update* access to **prefix.FSO.EXAMINE.CAIDBS1** for the duration of performing a review.

(5) The IAO will review and audit *update* and *alter* access to the **prefix.FSO.EXAMINE.CAIDBS1** file on a daily basis.

(6) In addition to the **FSO** file, the site may allocate multiple **prefix.EXAMINE.CAIDBS1** files. Access to these files also will be strictly controlled and audited.

For more detailed procedures about auditing, refer to *Section 2.1.4, Auditing*.

F.12.4.2 ACF2

Use standard ACF2 data set controls to control access to the CA-EXAMINE product libraries. No additional ACF2 controls are required.

F.12.4.3 RACF

Use standard RACF data set controls to control access to the CA-EXAMINE product libraries. No additional RACF controls are required.

F.12.4.4 TOP SECRET

Use standard TOP SECRET data set controls to control access to the CA-EXAMINE product libraries. No additional TOP SECRET controls are required.

F.12.5 CA-SYSVIEW/E

Vendor: Computer Associates International

F.12.5.1 Overview

CA-SYSVIEW/E is a product that is designed to assist the OS/390 systems programmer, operations specialist, or automation analyst in dealing with OS/390, JES2, and CICS environments. CA-SYSVIEW/E allows you to issue OS/390 and JES2 commands and to display information about system activities via easy-to-use panels. In addition, the product incorporates OS/390 and CICS data collection agents that provide comprehensive solutions in the field of performance management.

CA-SYSVIEW/E provides data center operators with an efficient full screen front-end to many OS/390, CICS, and JES2 commands. It provides easy-to-use utilities to perform system tasks such as dynamically changing the LINKLIST, adding or deleting Link Pack Area (LPA) modules, and adding entries to the Program Properties Table (PPT). CA-SYSVIEW/E a1so provides extensive resource displays such as cross memory connectivity between system components and the task structure of address spaces.

F.12.5.2 General Considerations

CA-SYSVIEW/E can be accessed on-line, in local 3270 mode, through the application interface (API), through the CICS Monitor Exit Interface (MEI), or through the batch interface. Access to this product must be restricted to systems programmers, Security Administrators, and only those operation specialists that have a unique requirement. The program product data sets must be secured, thereby giving access to only authorized personnel. All commands that have the capability to alter operating system control blocks or display sensitive data must also be secured.

F.12.5.2.1 On-line Access

On-line access is available from VTAM (as a VTAM application), TSO, ISPF, CICS, and from CMS if OS/390 is running in a VM (virtual machine) environment. The local 3270 device interface of CA-SYSVIEW/E can be used to run the product in a dedicated mode from any locally attached 3270 device. This interface can be used to start a session with CA-SYSVIEW/E when TSO and VTAM are not active. It can even be used when JES2 is not active.

F.12.5.2.1.1 Dedicated Mode

Dedicated mode execution of CA-SYSVIEW/E is by design independent of individual users, as it executes using a dedicated local 3270 console. Enforce the following controls for dedicated mode execution:

(2) Ensure that the system consoles and/or terminals dedicated to CA-SYSVIEW/E are in a controlled area accessible only to operations and systems programming personnel.

(3) Ensure that access to the consoles and/or terminals dedicated to CA-SYSVIEW/E are further restricted to those personnel authorized to use the product.

F.12.5.2.1.2 VTAM Mode

In VTAM mode, CA-SYSVIEW/E can be accessed directly from VTAM or via CL/SUPERSESSION. CA-SYSVIEW/E should only appear as a CL/SUPERSESSION selection option for authorized personnel only. Define the APPLID to the **APL** resource class for only authorized users of CA-SYSVIEW/E.

F.12.5.2.1.3 ISPF and TSO Modes

ISPF and TSO Mode execution of CA-SYSVIEW/E occurs within the user's TSO address space. Authorized access to CA-SYSVIEW/E from ISPF and TSO will be controlled using the following mechanisms:

(1) The libraries (i.e., **SYS2.SYSVIEW.LOADLIB** and **SYS2.SYSVIEW.ISPFLIB**) necessary for ISPF execution of CA-SYSVIEW/E will only be available in the TSO environment of those individuals authorized access.

(2) CA-SYSVIEW/E will only appear as ISPF panel selection options for those individuals authorized access.

F.12.5.2.1.4 CICS Mode

The following CICS transactions must be secured allowing access to only authorized personnel:

XPFS – To manually start the CICS Data Collector
XPFT – To manually terminate the CICS Data Collector
XPFI – The internal transaction to function requests (cannot be executed directly)
SYSV – CA-SYSVIEW/E on-line interface

F.12.5.2.2 Using the CICS Monitor Exit Interface

The CICS MEI allows you to customize your applications to pass information to CA-SYSVIEW/E. Adding interface calls to existing packages running in CICS provides more data collection information about the transaction. Information passed to CA-SYSVIEW/E is collected for individual transactions. The MEI provides support for umbrella-type transactions. **XPFCMEI**, a macro used as the interface to the monitor exit, is provided with CA-SYSVIEW/E. Since this is a one-directional access to CA-SYSVIEW/E (i.e., the CICS transaction is sending information to CA-SYSVIEW/E for collection), there is no requirement to enforce security to use this interface.

F.12.5.2.3 Batch Interface

The batch interface provides the capability to supply CA-SYSVIEW/E display commands as input, and to receive simulated screen output to SYSOUT or a data set. The userid for the batch session is controlled by the userid field on the JOB card. Access to the program **GSVXBAT** or **SYS2.SYSVIEW.LOADLIB** should be restricted to only those userids that are associated with the personnel authorized to use CA-SYSVIEW/E.

F.12.5.2.4 Application Program Interface

The application-programming interface (API) for CA-SYSVIEW/E can be used to obtain information from CA-SYSVIEW/E displays for use in other programs. The API is accessed by using TSO/E REXX. Commands are passed to the API by using the REXX ADDRESS function. The information from the display is passed back to the caller in a line-oriented format. Using the API can also change information passed back.

In order to use the API from TSO/E REXX, the REXX host command environment table must include the entry **SYSVIEWE**. This can be done in one of two ways:

(2) The **SYSVIEWE** entry can be added to the REXX modules IRXPARMS, IRXTSPRM, and/or IRXISPRM,

OR

(3) It can be added dynamically by coding the statement **ADDRESS 'LINK' GSVXRXAA** at the beginning of the REXX routine that invokes the API.

With the latter method, the module **GSVXRXAA** will add the **SYSVIEWE** entry to the REXX host command environment table if it does not exist. For that reason, the latter method must be the only method for avoiding security risks. Since the **GSVXRXAA** module must be invoked from the user's TSO address space, normal controls can be enforced as specified in *Section H.12.5.2.1.3, ISPF and TSO Modes*. The first method provides no mechanism to enforce security controls.

F.12.5.3 Security Controls

CA-SYSVIEW/E provides comprehensive security. Any operator can be allowed or restricted in the ability to see or manipulate any individual field on any CA-SYSVIEW/E display. You can provide a wide range of access capabilities to specific subsets of the user community. CA-SYSVIEW/E supports ACF2, RACF, or TOP SECRET to make these decisions, or the Security Administrator can use CA-SYSVIEW/E's internal security.

CA-SYSVIEW/E provides the ability to define security in the following ways:

- Who can use CA-SYSVIEW/E
- Which of the product's commands can be used
- Which capabilities of the commands can be used
- What a user sees on a command's display

Personnel that should be authorized to access CA-SYSVIEW/E are Security Administrators, systems programmers, operational specialists, and developers for CICS, DB2, DATACOM, IMS, and MQ Series applications. All authorized users will have access to scrolling and functional commands (i.e., **BOTTOM**, **LOCATE**, **FIND**, **HELP**, **MENU**, etc.). These commands, along with any other non-restricted command, will be assigned to the GLOBAL security group; thereby being enabled to all authorized users. The table in *Appendix E, CA-SYSVIEW/E Commands,* identifies the commands that each of the groups should be authorized to use.

F.12.5.3.1 Internal Security

F.12.5.3.1.1 Security Groups

Security groups (which are defined by CA-SYSVIEW/E administrators and sub-administrators) contain the security definitions for lists of users with similar security requirements for the product. CA-SYSVIEW/E checks these groups to determine what security privileges a user can exercise. Any number of security groups can be defined. The following chart describes the different types of CA-SYSVIEW/E internal security groups:

SECURITY GROUP	***SECURITY DEFINITIONS CONTAINED IN THE GROUP***
GLOBAL	Definitions that apply to every user
ADMIN	Definitions that apply to the CA-SYSVIEW/E administrators
Sub-administrator	Definitions that apply to the sub-administrators
User-defined	Definitions that apply to users defined by administrators or sub-administrators. The definitions for these security groups reflect the restricted use of the SECURITY command.
DEFAULT	Definitions for users who are not specifically defined in any security group. Userids do not have to be defined for this group. If a userid is not found in any other security group, CA-SYSVIEW/E uses the DEFAULT security group.

When a user issues a command, CA-SYSVIEW/E checks the definitions in the GLOBAL security group first. The user-defined security groups are also checked. If a userid is found in any of these groups, the more specific definition in the user-defined group will override the GLOBAL group definition. If a userid is not found in any other security group, use the DEFAULT security group.

F.12.5.3.1.2 Security Categories

The chart below lists the security categories that can be available for a security group. These categories are options on the Group Access Display.

SECURITY CATEGORY	*WHAT IS DEFINED*	*WHO CAN UPDATE THIS*
Userid	Members belonging to security group	Administrator and sub-administrator
Commands	The commands that the group can use	Administrator and sub-administrator
Command Fields	The fields on the display that the group can see and change	Administrator
Jobnames	The jobs that the group can access or the ones for which definitions apply	Administrator
Resources	The resources that the group can access	Administrator

F.12.5.3.1.3 Administrators and Sub-administrators

Administrators and sub-administrators define security groups. An administrator is a user who has the authority to create and modify all security groups and perform all security functions. A sub-administrator is a user who can create security groups, but is restricted in what security functions can be performed. The first CA-SYSVIEW/E administrator is created during the installation of the product. That administrator creates additional CA-SYSVIEW/E administrators. Administrators can create sub-administrator security groups, whose members called sub-administrators, can themselves create security groups. In this way, maintenance of user groups can be delegated. The security privileges of sub-administrators have the following restrictions:

- Sub-administrators cannot change security definitions in the ADMIN, GLOBAL, or DEFAULT groups.

- Security definitions that apply to sub-administrators are transferred to the users in the security groups that the sub-administrators create. Also, sub-administrators can change only the capabilities of the security groups they create, not their own.

- The only security definitions that sub-administrators can change for their security groups are definitions affecting userids and commands.

- Sub-administrators in the same security group, or co-sub-administrators, can change security for any of the groups that they and their fellow co-sub-administrators create.

F.12.5.3.2 Interface to an Access Control Program

F.12.5.3.2.1 User and Password Validation

Userid and password validation is performed by either the Access Control Product (ACP) or the internal security facility. Coding **SAF=USER** in the **GSVXGEN** module will enable CA-SYSVIEW/E to call the ACP to validate the userid and password when accessing the product through either the VTAM or the local 3270 interface. The USER setting has no effect on the TSO, ISPF, and ROSCOE interfaces.

F.12.5.3.2.2 Security Exit

CA-SYSVIEW/E provides an exit that can be used to control the product's security with any Access Control Product. The security exit can be used to control access through the ACP instead of, or in addition to, CA-SYSVIEW/E's internal security tables. It is DOD's direction to use the ACP whenever possible. If the security exit is not going to be used, code **SECEXIT=** in the **GSVXGEN** module; or code **SECEXIT=AUTH**.

Ensure that CA-SYSVIEW/E internal security allows access to all entities that are to be controlled by the ACP. If internal security does not allow access to an entity, the security exit will **not** be able to grant access. In the security exit source **SYS2.SYSVIEW.SAMPLIB (SAFSECX)**, set the global variable (i.e., **GRCLASS**) for the name of the General Resource Class that the exit will use for an entity class according to the ACP:

ACF2:	**SYSVIEW**
RACF:	**#SYSVIEW**
TOP SECRET:	**CAGSVX**

Sections F.12.5.3.3, ACF2, F.12.5.3.4, RACF, and F.12.5.3.5, TOP SECRET, describe the necessary steps required to define the General Resource Class for ACF2, RACF, and TOP SECRET respectively.

Calls made to the security exit by CA-SYSVIEW/E are as follows:

User Validation Call

This call is made when the user first enters CA-SYSVIEW/E. The purpose of the user validation call is to determine if the user is authorized to use CA-SYSVIEW/E from the particular environment (i.e., VTAM, TSO, CICS, etc.) that was used to log on, if the user is allowed multiple sessions, and if display field checking is required.

Each environment that will provide access to CA-SYSVIEW/E will require an entity in the ACP's General Resource Class, along with an access list to identify those users that can access CA-SYSVIEW/E resources. The following entities with an access list should be defined as needed:

SV.ENV.VTAM
SV.ENV.TSO
SV.ENV.ISPF
SV.ENV.CICS
SV.ENV.BATCH

Initialization Call

The purpose of the initialization call is to determine the commands for CA-SYSVIEW/E for which the user is authorized. Only authorized commands will be displayed when the **MENU** command is used. The initialization call is made when the user first enters CA-SYSVIEW/E and is made only during CA-SYSVIEW/E's session initialization. Only commands that are authorized through CA-SYSVIEW/E internal security are checked with an initialization call. Scrolling commands and function commands (e.g., **FIND**, **HELP**, **MENU**, etc.) are not checked.

Command Validation Call

The purpose of the command validation call is to provide the security exit with the command and parameters entered by the user on the command line of CA-SYSVIEW/E. In order to grant access to the CA-SYSVIEW/E commands using the ACP, define the generic entity **SV.CMND.*** in the SYSVIEW resource class (i.e., **#SYSVIEW**) that permit universal access. Using the table in *Appendix E, CA-SYSVIEW/E Commands,* as a guide, grant access to the sensitive commands based on the users' roles. For each command that requires controlled access, define an entity (i.e., **SV.CMND.command**) in the CA-SYSVIEW/E resource class with no universal access, defining only those users in the access list that are permitted to use the command.

Jobname Validation Call

The jobname validation call provides the security exit with the job information that the user might access. Jobname validation calls are made when a command displays job-related information.

Resource Validation Call

The purpose of the resource validation call is to validate access to a resource name. Resource validation calls are made when a user enters a line command that affects the resource.

Termination Call

The purpose of the termination call is to allow the security exit to free any storage it has acquired. The termination call is made after the user issues the **END** command.

F.12.5.3.2.3 Data Sets

All CA-SYSVIEW/E data sets need to be protected by the ACP. The level of access for each data set by group is defined in the table that follows.

Table B-64. CA-SYSVIEW/E DATA SETS (G.12.5.3.2.3)

DATA SET OR LIBRARY	*ADMIN*	*SYSPROG*	*OPERATIONS*
SYS2.SYSVIEW.LOADLIB	READ	ALTER	READ
SYS2.SYSVIEW.ISPFLIB	READ	ALTER	READ
SYS2.SYSVIEW.SECURITY	UPDATE	READ	READ
SYS2.SYSVIEW.SAMPLIB		ALTER	
SYS2.SYSVIEW.MACLIB		ALTER	
SYS2.SYSVIEW.PARMLIB	READ	ALTER	READ
SYS2.SYSVIEW.CLISTLIB	READ	ALTER	READ
SYS2.SYSVIEW.PANELLIB	READ	ALTER	READ
SYS2.SYSVIEW.HELPLIB	READ	ALTER	READ
SYS2.SYSVIEW.BOOKS	READ	ALTER	READ
SYS2.SYSVIEW.PLOTLIB		ALTER	READ
SYS2.SYSVIEW.PROFILE	UPDATE	READ	READ

F.12.5.3.2.4 CICS Transactions

The following CICS transactions must be secured allowing access to only authorized personnel:

XPFS
XPFT
XPFI
SYSV

Please refer to *Section 8.2, CICS*, for guidance on using an ACP to restrict access to these transactions.

F.12.5.3.3 ACF2

F.12.5.3.3.1 Define the SAF Resource Classes to the ACF2 Database

Associate the STIG recommended resource type **SVW** with the resource class CA-SYSVIEW/E.

```
CLASMAP.SYSVIEW RESOURCE(SYSVIEW) RSRCTYPE(SVW)
```

NOTE: When coding entity rules in ACF2, use an entity rule TYPE of **SVW** and a mode of **RESOURCE**.

F.12.5.3.3.2 Define Resource Entities and Enable Access

Define resource entities as required for controlling access to CA-SYSVIEW/E environments and commands. Unless there is a unique restriction (see *Table B-28* below for CA-SYSVIEW/E resource entities), access is granted for all CA-SYSVIEW/E resources that are not explicitly controlled. The following example grants access to all CA-SYSVIEW/E resources and then establishes an entity and access control to the TSO environment and the **DUMP** command:

```
$KEY(SV.*) TYPE(SVW) (UID(userid) ALLOW)
$KEY(SV.ENV.TSO) TYPE(SVW) (UID(userid) ALLOW)
$KEY(SV.CMND.DUMP) TYPE(SVW) (UID(userid) ALLOW)
```

Table B-65. CA-SYSVIEW/E RESOURCE ENTITIES (G.12.5.3.3.2)

SV.CHKA	Include action codes on SV.USER calls.
SV.CHKF	Check user access to display fields.
SV.CHKU	Generically grant access to jobnames when USER=, NOTIFY= or jobname matches the userid (or the user has access to rule granting access to **NOTIFY=** or jobname).
SV.JOBN	Checked when a command accesses data related to a specific job; user must have access to jobname.
SV.JQUE	When a user accesses a jobname, check to see if the user has access to the queue (input, converter, execution, output, etc.) the job is in.
SV.JTYP.*type*	Checks to see if the user has access to specific job types where the type is STC, SYS, JOB, or TSU.
SV.SUSP.JTYP	Disable checking on the entity type for job types.
SV.NQDQ	Restrict some users to one session.
SV.NTFY	When a user accesses a jobname that had a **NOTIFY=** on the Job card, a check is done to validate the user's access to the resource specified in the NOTIFY parameter.
SV.RESN.*resourcename*	Where *resourcename* is a device unit, JES2 resources (spool, classes, destinations, etc.), and system IDs.
SV.USER	When a user accesses a jobname that has a **USER=** on the Job card, a check is done to validate the user's access to the resource specified in the USER parameter.
SV.WTRN	When a jobname is accessed, each writer name referenced by the job is individually checked for access using the writer's name.

F.12.5.3.3.3 Enable VTAM Access

Define the APPLID to the **APL** resource class for only authorized users of CA-SYSVIEW/E in VTAM mode:

$KEY(*sysview_applid*) TYPE(APL) (UID(*userid*) ALLOW)

F.12.5.3.4 RACF

F.12.5.3.4.1 Update the RACF Class Descriptor Table

(1) Define the **#SYSVIEW** resource class to the RACF Class Descriptor Table (ICHRRCDE). The following is an example of an ICHRRCDE table source update using the ICHERCDE macro:

```
ICHERCDE CLASS=#SYSVIEW,
         ID=nnn,          <== This number must be a unique numeric.
         FIRST=ANY,
         OTHER=ANY,
         POSIT=nnn
```

NOTE: The values specified for ID and POSIT are site-specific. Refer to the IBM RACF Macros and Interfaces manual for more information.

(2) Assemble and link-edit ICHRRCDE into **SYS1.LINKLIB**. In accordance with *Section 2.1.2, Software Integrity*, the RACF Class Descriptor Table must be installed and maintained using SMP/E.

F.12.5.3.4.2 Update RACF Router Table

(1) Add the **#SYSVIEW** resource class to the RACF Router Table (ICHRFR01). Update the RACF Router Table source with the following entry:

```
ICHRFRTB CLASS=#SYSVIEW,
         ACTION=RACF
```

(2) Assemble and link-edit ICHRFR01 into SYS1.LINKLIB. In accordance with *Section 2.1.2, Software Integrity*, the RACF Class Descriptor Table must be installed and maintained using SMP/E.

NOTE: An IPL of the operating system is required for these changes to take effect.

(3) Activate the RACF resource classes by using the RACF **SETROPTS** command using the following examples to perform the activation:

```
SETROPTS CLASSACT(#SYSVIEW)
```

F.12.5.3.4.3 Define Resource Entities and Enable Access

Define resource entities as required for controlling access to CA-SYSVIEW/E environments and commands. Unless there is a unique restriction (see *Table B-28* for CA-SYSVIEW/E resource entities), access is granted for all CA-SYSVIEW/E resources that are not explicitly controlled. The following example grants access to all CA-SYSVIEW/E resources and then establishes an entity and access control to the TSO environment and the **DUMP** command:

```
RDEFINE #SYSVIEW SV.* AUDIT(ALL) UACC(READ)

RDEFINE #SYSVIEW SV.ENV.TSO AUDIT(ALL) UACC(NONE)
PERMIT SV.ENV.TSO CLASS(#SYSVIEW) ID(userid) ACCESS(READ)

RDEFINE #SYSVIEW SV.CMND.DUMP AUDIT(ALL) UACC(NONE)
PERMIT SV.CMND.DUMP CLASS(#SYSVIEW) ID(userid) ACCESS(READ)
```

F.12.5.3.4.4 Enable VTAM Access

Define the APPLID to the **APPL** resource class for only authorized users of CA-SYSVIEW/E in VTAM mode. Examples of the commands to control access are shown below:

```
RDEFINE APPL sysview_applid UACC(NONE)
PERMIT sysview_applid CLASS(APPL) ID(userid) ACCESS(READ)
```

F.12.5.3.5 TOP SECRET

F.12.5.3.5.1 Define SYSVIEW Facility and STC

(1) Define a FACILITY. Add these statements to TOP SECRET's startup parameters:

```
FAC(USERnn=NAME=GSVX)
FAC(GSVX=PGM=GSV,MULTIUSER,SHRPRF,KEY=8,NOLUMSG,NOSTMSG)
FAC(GSVX=MODE=FAIL,LOG(NONE),ACTIVE,TENV,NOABEND)
FAC(GSVX=SIGN(M),NOTRACE,AUTHINIT)
FAC(GSVX=NOAUDIT,ASUBM,DEFACID(*NONE*))
FAC(GSVX=UIDACID=8)
```

NOTE: USERnn can be any available Facility Matrix Table entry.

(2) Create an ACID called **GSVX** for the started task:

```
TSS CREATE(GSVX) NAME('SYSVIEW') FAC(STC)
    MASTFAC(GSVX) PASS(password,0) DEPT(owning_dept)
    NOLCFCHK NORESCHK SOURCE(INTRDR)
```

(3) Add the ACID to the Started Task Table:

TSS ADD(STC) PROCNAME(*sysview_procname*) ACID(GSVX)

(4) Allow all users associated to the ACID **GSVX** to have access to the Facility **GSVX**:

TSS ADD(GSVX) FAC(GSVX)

F.12.5.3.5.2 Define Resource Entities and Enable Access

(1) Define a new Entity Class Name in the Resource Definition Table (RDT), using the command:

TSS ADD(RDT) RESCLASS(CAGSVX) RESCODE(*xxxx*) DEFACC(NONE)
ACLST(UPDATE,READ,NONE) ATTR(LONG,DEFPROT)

NOTE: RESCODE value **xxxx** may be any unused hex value

(2) Define resource entities as required for controlling access to CA-SYSVIEW/E environments and commands. Unless there is a unique restriction (see *Table B-28* for CA-SYSVIEW/E resource entities), access is granted for all CA-SYSVIEW/E resources that are not explicitly controlled.

The following example grants access to all CA-SYSVIEW/E resources and then establishes an entity and access control to the TSO environment and the **DUMP** command:

TSS ADD(*owning_acid*) CAGSVX(SV)

TSS ADD(*owning_acid*) CAGSVX(SV.ENV.TSO)
TSS PERMIT(*user_acid*) CAGSVX(SV.ENV.TSO)

TSS ADD(*owning_acid*) CAGSVX(SV.CMND.DUMP)
TSS PERMIT(*user_acid*) CAGSVX(SV. CMND.DUMP)

NOTE: When adding generic entity names to TOP SECRET, do NOT include the "**.***".

F.12.5.3.5.3 Enable VTAM Access

Define the APPLID to the **KLS** resource class for only authorized users of CA-SYSVIEW/E in VTAM mode:

TSS PERMIT(GSVX) KLS(*sysview_applid*) ACCESS(READ)

F.13. SYSTEM MAINTENANCE SOFTWARE

F.13.1 General Considerations

System maintenance software products facilitate one or more of the following tasks regarding program products and executable code:

- Installation
- Maintenance
- Customization
- Debugging

The products typically provide programmers with a comprehensive set of tools, which includes commands, utilities, and reports, to perform these tasks in either interactive on-line mode or a batch environment.

Consideration will be given to securing the data sets that contain the system maintenance software products. Access to these data sets will not be permitted to the general user community, but will only be granted to authorized personnel.

Use of sensitive utility controls will be considered. Evaluate all programs to determine if they pose possible data or system integrity problems and/or potential security exposures. For example, the SMP/E program, **GIMSMP**, should be considered sensitive and therefore be restricted.

Interactive execution of the system maintenance software products will be available under the appropriate TMP. Prohibit access to these on-line applications from general use. Only grant access to authorized personnel.

Some system maintenance software products provide ACP resource interfaces for various functions and options. Review and evaluate these interfaces for potential security exposures and possible implementation. If it is determined that an enhanced level of protection is gained, an interface may be installed. However, base-level ACP security controls will never be compromised.

Use the following recommendations when securing access to system maintenance software:

(1) Control access to the software product's data sets, and restrict access only to authorized personnel.

(2) Implement program protection for especially sensitive utilities (e.g., SMP/E).

(3) Control access to the interactive on-line applications, and restrict access only to authorized users.

(4) Review and evaluate resource interfaces for potential implementation to ensure they do not pose a security risk or compromise base-level ACP controls.

F.13.2 SMP/E

Vendor: IBM Corporation

SMP/E (System Modification Program/Extended) is used to perform the installation and customization of other IBM products. The product provides extensive tracking capabilities so that maintenance applied to components of the operating system (e.g., programs, macros) can be analyzed during problem determination. Many vendors distribute their products using SMP/E for installation and customization.

SMP/E is the primary tool used to perform maintenance on the OS/390 operating system. If adequate controls are not in place, the possibility exists that someone could alter the operating system and product code. Additionally, problem diagnosis with IBM and other vendors becomes difficult because the current maintenance level of a product can become questionable.

Use the following recommendations with SMP/E:

(1) Protect all SMP/E data sets (i.e., **SMPLOG**, the **CSI** (Consolidated Software Inventory), **SMPMTS**, and **SMPPTS**) with data set-level controls. Access to these data sets will not be permitted to the general user community. Only grant access to authorized personnel.

(2) Restrict access to the SMP/E program, **GIMSMP**, only to authorized personnel. Refer to *Section 3.1.5.3, Sensitive Utility Controls*, for further information.

(3) Protect access to the libraries that SMP/E controls with data set-level controls. This includes target libraries and distribution libraries.

F.13.2.1 ACF2

Standard data set access rules are required and will be written for the library containing the SMP/E utility, and for all files used and maintained by the product. Protect access to the **GIMSMP** (SMP/E) program using the Protected Program List (**PPGM**) facility, as discussed previously. Only grant program access to authorized users.

Refer to *Section 3.2.5.3, Sensitive Utility Controls*, for further information.

F.13.2.2 RACF

Protect SMP/E by using standard data set controls to protect the SMP/E product data sets. Also, protect the **GIMSMP** program using the **PROGRAM** resource class. Only grant program access to authorized users. Protect all SMP/E libraries using normal data set protection.

Refer to *Section 3.3.5.3, Sensitive Utility Controls*, for further information.

F.13.2.3 TOP SECRET

Protect SMP/E by using standard data set controls to protect the SMP/E product data sets. Also, protect the **GIMSMP** program using the **PROGRAM** resource class. Only grant program access to authorized users. Protect all SMP/E libraries using normal data set protection. Refer to *Section 3.4.5.3, Sensitive Utility Controls*, for further information.

APPENDIX G. LIST OF ACRONYMS AND DEFINITIONS

Abend	Abnormal End. Abnormal termination of a job or task.
Abort Mode	Term used in ACF2 to indicate that the system is in full protection mode.
ACF2	Access Control Facility 2. Access Control Product marketed by Computer Associates.
ACF2/CICS	Sub-product of ACF2 designed to provide protection of CICS resources.
ACID	Accessor ID. Unique character-string identifier by which TOP SECRET identifies a user and the user's associated security record.
ACP	Access Control Product. Industry term that designates an add-on system component/product that performs system-wide security validation (e.g., ACF2, RACF, and TOP SECRET).
ADP	Automated Data Processing.
AIS	Automated Information System.
AOR	Application Owning Region.
APF	Authorized Program Facility. MVS component that allows programs to access protected facilities of the operating system.
ASIMS	Army Standard Information Management Systems.
ATCF	Automated Technical Control Facility.
AUTOLOGON	Facility to automatically log on a user without a password.
AUTOMATE	Product marketed by Legent Corporation (now Computer Associates) to provide automated response to Master Console Messages.
AUTOTRAN	Product marketed by Universal Software Inc. to provide support for transferring files from a local host computer to a remote computer.
Batch	Concept of taking work that needs to be accomplished and allowing MVS to process it in background mode.
BLP	Bypass Label Processing. Feature provided by MVS that allows bypassing of the labels written on tapes that identify the actual data set name.
CA	Computer Associates Inc. Corporation that markets the ACF2 and TOP SECRET Access Control Products.
CA	Certificate Authority. A component of a Public Key Infrastructure, a CA is responsible for issuing and revoking digital certificates.

CA-1	Tape Management System marketed by Computer Associates. Often referred to as TMS.
CA-7	On-line, real-time, interactive Automated Production Control system that automatically controls, schedules, and initiates work according to time-driven and/or event-driven activities.
CA-11	Automated Rerun and Tracking System. Performs as a rerun handler, as a job analysis and tracking system, or as a combination of both.
CA-LOOK	Product marketed by Computer Associates that displays MVS internals and system information.
CA-TOP SECRET	Access Control Product marketed by Computer Associates. Also referred to as *CA-TSS*.
CA-TSS	CA-TOP SECRET.
CCTV	Closed Circuit Television.
CDA	Central Design Activity.
CICS	Customer Information Control System. Interactive system marketed by IBM for processing interactive, transaction-based applications.
COMPUSEC	Computer Security.
COMSEC	Communications Security.
COOP	Continuity of Operations Plan. A process to ensure availability in the event of a system or component failure.
CPU	Central Processing Unit. Computer hardware that processes computer software instructions.
CRYPTO	Cryptographic. A marking or designator identifying all COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive unclassified information.
CSI	Consolidated Software Inventory. A database used by SMP/E to manage, maintain, and update system software.
CSPE	Computing Services Processing Element.
Daemon	A background process that operates continuously or periodically to provide a system service. Daemons usually have special security privileges that allow them to assume the security context of a user.
DASD	Direct Storage Device. A hardware device used for temporary or permanent storage of data and software.

Data Integrity	Concept of ensuring that data is not manipulated or accessed in any way other than what was originally intended.
Data Labels	Labels that identify the classification level of data. Normally associated with B1 security processing.
Data Owner	Organization or individual that owns the data on a system and is responsible for the contents and integrity of that data.
DCA	Department Control ACID. Individual(s) who controls users, profiles, departments, and resources within their own department.
DDN	Defense Data Network.
DFDSS	Data Facility Data Set Services. Product marketed by IBM that is designed to perform data set management.
DFHSM	Data Facility Hierarchical Storage Manager. Product marketed by IBM that is designed to perform hierarchical storage management.
DFP	Data Facility Product.
DFSMS	Data Facility Storage Management Subsystem. An integrated product marketed by IBM that is designed to encompass DFDSS and DFHSM and to introduce systems-managed storage to facilitate the effective management of DASD space.
DISA	Defense Information Systems Agency.
DISAI	Defense Information Systems Agency Instruction.
DISN	Defense Information Systems Network.
DOD-CERT	Department of Defense Computer Emergency Response Team (*formerly ASSIST*).
DSC	Data Services Center.
DSF	Device Support Facilities. Product marketed by IBM that is designed to perform DASD maintenance and DASD error identification.
EPO	Emergency Power-Off. A mechanism to disconnect power to a device or devices in the event of a malfunction or an emergency.
ESSD	Executive Software Support Division.
EXCP	Execute Channel Program. MVS macro instruction used to execute channel commands to perform I/O processing to an auxiliary device.
Fail Mode	Term used in RACF and TOP SECRET processing to indicate that the security system is in full protection mode.

FDC	Fire Department Connection.
FDR	Fast Dump Restore. Product marketed by Innovation that is used to perform DASD management.
FEP	Front End Processor.
FFS	Fee-for-Service. Concept of charging users for resource consumption.
FLASHER	Product marketed by Tone Software to provide interactive viewing of the JES3 spool queue and consoles.
Fork	The act of creating and starting a child process.
FSP	File Security Packet. A data structure containing security-related information about a file. The FSP is stored in the file system with its related file.
GID	Group Identifier. Defined in OS/390 UNIX as the numeric ID that identifies a group to which users belong for the purpose of file security.
GNOSC	Global Network Operations and Security Center (formerly *GOSC*).
GSO	Global System Options. Type of ACF2 records that specifies overall processing options for the ACF2 Access Control Product.
HFS	Hierarchical File System. The collection of mountable file systems, organized in a tree structure with the root file system as the highest member.
HVAC	Heat, Ventilation, and Air Conditioning.
I&A	Identification and Authentication.
IAM	Information Assurance Manager. The individual responsible for the information assurance program of a DOD information system or organization.
IANA	Internet Assigned Numbers Authority. The IANA defines standards for various protocol implementations commonly used on the Internet.
IAO	Information Assurance Officer. An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DOD information system or organization.
IBM	International Business Machines. Corporation that markets the MVS operating system and the RACF security product.
IDMS	Integrated Database Management System.
IDNX	Integrated Digital Network Exchange.
IDS	Intrusion Detection System.

IMS	Information Management System. Product marketed by IBM designed to allow interactive access to databases.
IOA	Integrated Operations Architecture. A fully integrated family of products marketed by New Dimension Software that is designed to streamline and automate mainframe operations.
I/O Appendage	Input/Output Appendage. Routine designed to provide additional controls for system I/O operations.
IPL	Initial Program Load. Initial load of the operating system into the CPU.
IPSC	Internal Product Security Controls are security mechanisms internal to COTS products and GOTS applications.
ISC	Inter-Systems Communication. Concept used to allow a CICS region to communicate with another CICS region or an IMS region.
ISPF	Interactive Systems Productivity. Product marketed by IBM that runs under TSO to provide menu-driven capabilities for programmer functions.
ISSM	Information Systems Security Manager. Now referred to as the Information Assurance Manager (IAM).
ISSO	Information Systems Security Officer. Individual responsible for security administration on the platform. Now referred to as the Information Assurance Officer (IAO).
JCL	Job Control Language. Language provided by MVS to define input, output, and processing parameters to job streams.
JES2/JES3	Job Entry Subsystem. Subsystem designed to process job streams in the MVS environment.
JSIDS	Joint Service Intrusion Detection System.
JWT	Job Wait Time.
LAN	Local Area Network.
LCF	Limited Command Function. TOP SECRET method for authorizing access to system resources.
Legacy Site	DOD facility scheduled for eventual migration into a site, but still functioning as a separate entity.
LID	Logon ID. Term used by ACF2 to uniquely identify a user of resources (i.e., userid).
LOOK	Product marketed by Computer Associates that allows MVS diagnostic functions.

LPA	Link Pack Area. Area of storage used for re-entrant programs. Loaded during IPL.
LSCA	Limited Central Security Control ACID. Has authority of an SCA, but has a limited scope of control that is customized by the MSCA.
MAINVIEW	Product marketed by Boole and Babbage used to monitor MVS system performance and analyze system problems.
MICOM	Missile Command.
MICS	Product marketed by Legent Corporation (now Computer Associates). Used by DISA to maintain a database of system utilization information.
MRO	Multiple Region Option. Concept to link multiple CICS regions together and make it look like one region to the system user.
MSCA	Master Security Control ACID. Highest level Security Administrator who controls the master password for updating the security database. Scope includes the entire installation. Has authority to designate and authorize SCAs, LSCAs, ZCAs, VCAs, and DCAs.
MUSASS	Multiple User Single Address Space System. Term used to identify an address space that multiple users can access at one time.
MVS	Multiple Virtual Storage. Operating system designed by IBM to allow multiple processes to concurrently use mainframe computing resources.
NCTS	Naval Computer and Telecommunications Station.
NetView	Product marketed by IBM to aid in management of network resources.
NFPA	National Fire Protection Association.
NFS	Network File System. A protocol that allows users to directly access files that reside on other network-connected systems.
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network.
NISC	Naval Information Systems Center.
NJE	Network Job Entry. Concept of allowing work to be transmitted between multiple MVS systems connected in an SNA network.
NSA	National Security Agency.
OI	Operating Instructions.
OMEGAMON	A product marketed by the Candle Corporation to perform analysis of operating system problems.

OSI	Office of Special Investigations.
OTRAN	Method within TOP SECRET to perform transaction verification.
PD	Position Description.
PDS	Protected Distribution System.
PIN	Personal Identification Number.
PKCS	Public Key Cryptography Standards. The set of standards for elements used in the deployment of public key cryptography.
PMS	Problem Management System.
PPT	Program Properties Table. Facility provided by IBM to identify programs that require special designation when invoked in an OS/390 environment.
RACF	Resource Access Control Facility. Access Control Product marketed by IBM to protect OS/390 operating system resources.
RACROUTE	Macro provided by the OS/390 operating system to interface with SAF.
RCC	Regional Control Center (now referred to as the Regional Operations Service Center [ROSC]).
RESOLVE	Product marketed by Boole and Babbage that is designed to perform MVS diagnostics.
RJE	Remote Job Entry. Workstations used to submit background work to the MVS system.
RNOSC	Regional Network Operations and Security Center (formerly *ROSC*).
ROSC	Regional Operations Service Center (formerly referred to as the Regional Control Center [RCC]).
RPC	Remote Processing Center.
SAF	System Authorization Facility. Mechanism designed within the OS/390 operating system that provides a common interface to the installed Access Control Product.
SCA	Central Security Control. Security Administrator ACID whose scope of authority includes the entire installation. SCAs can designate and authorize VCAs and DCAs.
SCPLIST	Scope List. ACF2 feature used to identify and limit the level of administration authorized for a delegated Security Administrator.
SDS	Standard Depot Systems.

SETROPTS	Set RACF Options. Mechanism by which security control defaults are established for RACF.
SIPRNet	Secret Internet Protocol Router Network.
SISOCS	Streamlining Information Service Operations Consolidation Study.
SLA	Service Level Agreement.
SM	Security Manager.
SMC	Systems Management Center.
SMF	System Management Facility. MVS-provided facility that provides for the tracking of system activity (used by Access Control Products to store security-related information).
SMP/E	System Modification Program/Extended. Product provided by IBM to perform installation and maintenance of products.
SNIFFER	Network interface that is designed to interrogate data passed through the network communication links.
SNT	Sign-on Table. Facility provided in CICS to allow CICS internal security functions.
Software Support	Local Executive Software group at the site.
SOP	Standard Operating Procedures.
Spawn	The act of creating and starting a child process running a named program.
SPS	Security Police Squadron.
SSBI	Single Scope Background Investigation.
SSO	Software Support Organization (local Executive Software group at the site).
SSO	Systems Support Office (SSO-Mechanicsburg and SSO-Dayton).
STC	Started Task Control. Facility provided by MVS to submit work to run in the background mode (generally used for operations-controlled software).
Sticky bit	Defined in OS/390 UNIX as an FSP permission bit that can be applied to directories or executable files.
STROBE	Product marketed by Programart designed to analyze the performance of application code.

Super IDs	Userids defined to be used in emergency situations to correct problems when the systems programmer access is insufficient to do so.
Superuser	Defined in OS/390 UNIX as a user who passes all security checks with respect to privileged commands and file accesses. Users assigned a UID of 0 (zero) have superuser status.
SVC	Supervisor Call. Code executed by the OS/390 operating system on behalf of a user to perform system-level functions.
SYSLOG	System Log. JES spool file of all system messages issued to, or by, the OS/390 operating system and its components.
SYSOUT	System Output. Generally refers to hard-copy output.
TASO	Terminal Area Security Officer.
TEMPEST	Transient Electromagnetic Pulse Emanation Standard.
TMON	The Monitor. Series of products marketed by Landmark Corp. that allows diagnosis and analysis of operating system components.
TNF	Termination Notification Facility. TNF provides inter-address space communication services for some TCP/IP applications.
TOP SECRET	Refer to *CA-TOP SECRET*.
TOR	Terminal Owning Region.
TSO	Time Sharing Option. Product marketed by IBM that is designed to allow flexibility to programmers in modifying the operating environment.
TSS	TOP SECRET Services. TOP SECRET security interface facility.
UACC	Universal. Definition within RACF software that can be established for profiles to give all users a particular level.
UID	UNIX User Identifier. Defined in OS/390 UNIX as the numeric ID that identifies a user for the purpose of file and process management security. Although highly discouraged, it is possible to assign the same UID to multiple users. See also *superuser*.
UPS	Uninterruptible Power Supply.
Userid	User ID. Mechanism used to uniquely identify a user of system resources.
Usermods	User Modifications. Term used to identify a modification designed and implemented by customers, versus one distributed by a vendor.

VCA	Divisional Control ACID. Has capability to define user ACIDs with ability to create authorization profiles. Scope of authority is limited to the ACID's assigned division.
VMCF	Virtual Machine Communication Facility. VMCF provides inter-address space communication services for some TCP/IP applications.
VPN	Virtual Private Network. A network connection utilizing tunneling, authentication, optional encryption, and other security controls to create a secure link that appears to be dedicated.
VTAM	Virtual Telecommunications Access Method. Access method marketed by IBM to allow terminal to application communications.
ZCA	Zone Control ACID. Administrative ACID whose scope of authority includes an entire zone. Controls all VCAs, DCAs, divisions, departments, profiles, users, and resources owned within the ACID's zone.