Office of Information Services
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, Maryland 21244-1850

CMS Security Whitepaper:

Mainframe OS/390 and z/OS RACF Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS RACF* WHITEPAPER, VERSION 2.0

1) Converted baseline version dated March 7, 2007 to updated CMS style format.
2) Moved Section 1, Introduction, from before Table of Contents to after.
3) Updated Section 2, Background, to add BPSSM section reference concerning the use of STIGs.
4) Added titles to the following tables:
   a) Table 1 in Section 3.1.1.1,
   b) Table 2 in Section 3.1.3,
   c) Table 3 in Section 3.2.2,
   d) Table 4 in Section 3.2.6, and
   e) Table 5 and 6 in Section 3.3.1.
5) Moved Section 3.2.2, Interactive Users and Parameters, subsection “Started Task Control (STC) User” to new Section 3.2.3
6) Removed former Appendix A CSRs and added pointer to new CMSRs.
7) Changed CSR glossary term in Appendix B to CMSR.
8) Updated Table 3 and Section 3.2.5, and updated the Appendix A CMSR reference.

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS RACF* WHITEPAPER, VERSION 1.0

1) Baseline Version 1.0.

(This Page Intentionally Blank)

TABLE OF CONTENTS

LIST OF TABLES

(This Page Intentionally Blank)

1 INTRODUCTION

This white paper was developed by PricewaterhouseCoopers LLP (PwC) for the Centers for Medicare and Medicaid Services (CMS). This document is one of a number of white papers issued by CMS management to assist with the proper understanding and implementation of key security controls around CMS' data and information systems environment.

The intended audience of this paper however, extends beyond CMS management and staff to include all CMS business partners. In this context, a CMS business partner is any private or public sector organization which provides services to this agency. These business partners include, but are not limited to; Medicare Carriers, Fiscal Intermediaries (FI), Common Working File (CWF) Host Sites, Durable Medical Equipment Regional Carriers (DMERCs), standard claims processing system maintainers, Regional Laboratory Carriers, claims processing data centers, Medicare Administrative Contractors (MAC), and Enterprise Data Centers (EDC).

This document is designed to provide guidance and information to CMS & CMS business partners in implementing and configuring a secure operating system (O/S) and computing environment through the use of the access control product RACF As computers and technology advanced they became capable of running several programs at once. This created a need to control resources and programs. The O/S addressed these issues by controlling the resources and functions that programs could use as well as keeping them from interfering with one another and the O/S itself. With the advent on online applications and transaction processing, it became possible for multiple end users to connect to a computer simultaneously, submitting and manipulating data from remote locations. Access control products (ACP) were developed to prevent users from affecting resources or processes outside of their responsibility. The O/S and ACP work in tandem to ensure the integrity of mainframe

O/S deployed by most CMS Contractor's mainframes use the International Business Machines (IBM) OS/390 or z/OS operating system package which includes the MVS O/S. The Defense Information Systems Agency (DISA), an agency of the Department of Defense (DOD), has developed an OS/390 & z/OS Security Technical Implementation Guide (STIG). The STIG, Version 5, Release 2, provides guidance on implementation of controls, configurations, and design of the OS/390,z/OS, and ACPs. References within this document to OS/390 also relate to z/OS; all references to OS/390 can also be applied to z/OS.

The purpose of this document is to relay pertinent information within the STIG to CMS and applicable CMS contractors which process information on behalf of CMS utilizing OS/390 or z/OS. Information within this document does not cover all controls and guidance provided within the STIG nor should a contractor using just this information have comfort in the overall security and integrity of their O/S. Rather, this document should be used as an introduction to the STIG and information contained within used as a starting point in developing a secure and controlled environment. This document will focus on and the access control product known as RACF, or Resource Access Control Facility, from IBM.

2 BACKGROUND

Federal agencies, such as CMS and CMS Contractors processing claims on their behalf, have become increasingly reliant on computerized information systems to process, maintain, and report essential information. This dependency on systems will continue to increase as technology advances and with this reliance also comes inherent vulnerabilities. To mitigate the risks associated with computerized information processing security and controls over the systems are paramount.

A key aspect of any computerized environment is the O/S. The O/S is used to control programs and resources, allowing multiple programs to run on the mainframe without interfering with one another or the O/S. Most federal agencies process many significant transactions through the use of a mainframe and use IBM OS/390 or z/OS. Additionally, agencies secure these environments with ACPs such as RACF. Access control products (ACP) were developed to prevent users from affecting resources or processes outside of their responsibility. The O/S and the ACPs must be properly installed and configured to maintain the integrity of the site.

Secure configurations and controls of RACF are essential to the integrity of a processing environment and they are subject to review as part of financial statement audits. Federal audit requirements applicable to the audit of CMS' financial statements include assessing the general and application controls over the processing of Medicare information and concluding on whether the controls are operating effectively.

To assist in the appropriate configuration of RACF, the DoD released the OS/390 & z/OS STIG, Version 5, Volume 2 on September 11, 2006. The STIG was developed by DISA for the DoD and provides guidance for the implementation and configuration of OS/390, ACF2, RACF, and TSS. This document was developed with regards to the STIG and key aspects of audit work programs in order to introduce concepts provided by the STIG. The STIGs provide very useful information on establishing a control framework for the mainframe operating system. This document will relay pertinent information from the STIG to readers, however, is not a substitute for the STIG, and will not alone provide a completely secure environment. Refer to section 3.10.2 in the BPSSM concerning the use of STIGs in the business partner environment.

3 RACF SECURITY IN THE OS/390 ENVIRONMENT

Multiple Virtual System (MVS) is an operating system which is part of the OS/390 and z/OS software packages. MVS controls programs and users and prevents them from interfering with one another and the O/S itself. When a user logs on to a terminal, when a batch job starts or a task, the System Authorization Facility (SAF), a component of MVS, makes a call an Access Control Product (ACP). ACPs are security mechanisms that provide security controls for the OS/390 environment. ACPs, such as ACF2, RACF, and Top Secret, receive controls from SAF by means of the RACROUTE macro. The ACP will create a control block in memory called the ACEE (Access Control Environment Element). The ACEE will contain information in regards to the accesses allowed for a user, started task, batch job, etc. For example, when the user attempts to access a dataset or resource the ACP can get control to determine whether they

should be permitted to access it. This is accomplished by comparing the information in the ACEE to either a dataset rule or a resource rule.

The ACP uses records, dataset rules, and resource rules to secure access to data and resources. The ACP provides security by answering the following two questions:

1) Is the user who they say they are?

2) What resources, datasets, transactions, etc. do they have access to?

By authenticating a user and controlling their access the tool maintains the integrity of the O/S, hence, configuration and controls surrounding ACP are paramount to ensure this integrity.

RACF is one of the three ACPs; RACF has several unique concepts for managing users and system resources not found in the other ACP packages. Unlike ACF2, RACF does not group users together through the use of a UID string. Instead each defined user belongs to at least one group, known as a default group. A group is a collection of RACF users who share common access requirements to protect resources or who have similar attributes within the system. RACF users can be members of one or more groups. In RACF terminology, when a user is associated with a group we can say that this user is "connected" to that group.

Another concept unique to RACF is the use of resource classes. For each type of resource protected by the system, a new class is created. The class documents the syntax rules, auditing, and statistical control for the resource, telling RACF how the resource is to be protected. These classes are tracked by RACF in the Class Descriptors Table (CDT). A number of classes are included with RACF; sites can also create classes to meet the needs of their environment.

3.1 RACF SYSTEM CONFIGURATION

3.1.1 SYSTEM CONFIGURATION STANDARDS

RACF offers many options with a variety of settings which can have a dramatic affect o the level of control that the ACP can provide. On such means of defining system options within RACF is by way of the Global Settings via RACF SETEROPTS command. SETROPTS is used to set system-wide options to protect resources.

3.1.1.1 SETROPTS SETTINGS

SETROPTS changes can be issued from TSO, ISPF menus, a console using an operator command, or via a parameter library. System users must have sufficient authority to the proper resource in the OPERCMDS class before the SETROPTS can be updated. Users with the RACF profile attribute SPECIAL can make changes to any SETROPTS settings, except the following which require the AUDITOR attribute:

APPLAUDIT | NOAPPLAUDIT

AUDIT | NOAUDIT

CMDVIOL | NOCMDVIOL

LOGOPTIONS

OPERAUDIT | NOOPERAUDIT

SAUDIT | NOSAUDIT

SECLABELAUDIT | NOSECLABELAUDIT

SECLEVELAUDIT | NOSECLEVELAUDIT

Users with the SPECIAL or the AUDITOR output can use the LIST command, which displays current SETROPTS settings.

The DISA STIG recommends the following RACF Standard Global Options (SETROPTS) and controls as specified below which will ensure the appropriate oversight and control of global options; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

The options specified are STIG requirements and each site can choose to be more restrictive. The values listed below are deviations from product default settings. Values not listed are to be the default values for the product.

Table 1 Recommended Standard Global Options Settings

Option	Description	Required Value
ADSP	Automatic data set protection	NOADSP The IAO will ensure that ADSP SETROPTS value is set to NOADSP. ADSP indicates that RACF automatically creates discrete data set profiles to protect data sets created by users having this attribute.
AUDIT	Logging RACF command and RACDEF SVC activity	AUDIT(*) The IAO will ensure that AUDIT SETROPTS value is set to AUDIT(*) indicating that RACF sets all classes to do auditing of uses of the RACDEF SVC and all changes made to profiles by RACF commands.
CLASSACT	General resource protection	The following classes will be activated on all systems: DATASET USER GROUP The following class will be activated only if no tape management system is installed on the system: TAPEVOL The IAO will ensure that CLASSACT SETROPTS value is set to values defined in the above table. See above table for the values.

Option	Description	Required Value
X`CMDVIOL	Logging of RACF command violations	CMDVIOL The IAO will ensure that CMDVIOL SETROPTS value is set to CMDVIOL to log violations to RACF commands.
EGN	Enhanced generic naming	EGN The IAO will ensure that EGN SETROPTS value is set to EGN this allows the generic character ** when you define dataset profiles.
ERASE	Erasure of scratched or released DASD data set space. CAUTION: Use of the ERASE feature can cause considerable system overhead affecting system performance. ERASE may be enabled in DATASET profiles which would afford more granular control.	Unclassified Systems: ERASE() Classified Systems: ERASE(ALL) The IAO will ensure that ERASE SETROPTS value is set to ERASE() on unclassified systems. On classified systems it is set to ERASE(ALL) this allows DASD datasets to be erased when deleted. See above table for additional information.
GENCMD	Generic profile creation	GENCMD(*) This option does not apply to the following resource classes: CCICSCMD GLOBAL KERBLINK PROGRAM REALM All group resource classes (e.g., GCICSTRN, GDASDVOL, etc.) The IAO will ensure that GENCMD SETROPTS value is set to GENCMD(*) this activates generic profile command processing for the dataset class and all classes defined in the CDT.
GENERIC	Generic profile checking	GENERIC(*) This option does not apply to the following resource classes: CCICSCMD GLOBAL KERBLINK PROGRAM REALM All group resource classes (e.g., GCICSTRN, GDASDVOL, etc.) The IAO will ensure that GENERIC SETROPTS value is set to GENERIC(*) this activates generic profile checking for the dataset class and all classes defined in the CDT.
GRPLIST	List-of-Groups authority checking	GRPLIST The IAO will ensure that GRPLIST SETROPTS value is set to GRPLIST. This sets a user's access based on the highest authority in any group to whom the IAO belongs.

Option	Description	Required Value
INACTIVE	Unused userid interval	35 days The IAO will ensure that INACTIVE SETROPTS value is set to 35 days this specifies the number of days that a user is inactive and still remain valid.
INITSTATS	Records RACINIT statistics	INITSTATS The IAO will ensure that INITSTATS SETROPTS value is set to INITSTATS this specifies that statistics available during RACINIT SVC processing are recorded.
JES(BATCHALLRACF)	Forces batch users to identify themselves to RACF	JES(BATCHALLRACF) The IAO will ensure that JES(BATCHALLRACF) SETROPTS value is set to JES(BATCHALLRACF). This specifies that JES is to test for a userid and password on the job statement or for propagated RACF identification information for all batch jobs.
JES(EARLYVERIFY)	JES userid early verification	JES(EARLYVERIFY) The IAO will ensure that JES(EARLYVERIFY) SETROPTS value is set to JES(EARLYVERIFY). This specifies that JES is to invoke the system authorization facility (SAF) for jobs that do not qualify for user identification propagation.
JES(XBMALLRACF)	Support for execution batch monitor	JES(XBMALLRACF) The IAO will ensure that JES(XBMALLRACF) SETROPTS value is set to JES(XBMALLRACF). This specifies that JES is set to test for a userid and password on the job statement or for propagated RACF identification information for all jobs run under the execution batch monitor.
OPERAUDIT	Logging activities of users with the OPERATIONS attribute	OPERAUDIT The IAO will ensure that OPERAUDIT SETROPTS value is set to OPERAUDIT. This specifies that RACF logs all actions such as accesses to resources and commands for a user who has operations or group operations attribute.
PASSWORD (HISTORY)	Number of previous passwords	10 The IAO will ensure that PASSWORD(HISTORY) SETROPTS value is set to 10. This specifies the number of previous passwords that RACF saves for each USERID and compares with an intended new password. If there is a match with one of the previous passwords, or with the current password, RACF rejects the intended new password.

Option	Description	Required Value
PASSWORD (INTERVAL)	Maximum password change interval	90 days The IAO will ensure that PASSWORD(INTERVAL) SETROPTS value is set to 90 days. This specifies the maximum number of days that each user's password is valid.
PASSWORD (REVOKE)	Consecutive password verification attempts	3 The IAO will ensure that PASSWORD(REVOKE) SETROPTS value is set to 3. This specifies the number of consecutive incorrect password attempts RACF allows before it revokes the USERID on the next incorrect attempt. If you specify REVOKE, ensure INITSTATS are in effect.
PASSWORD (RULEn)	Password syntax rules	LENGTH(8) ALPHANUM(1:8) The IAO will ensure that PASSWORD(RULEn0) SETROPTS value is set to LENGTH(8) ALPHANUM(1:8). RULEn specifies an individual syntax rule for new passwords that users specify at logon, on the job cards, or on the PASSWORD command.
PASSWORD (WARNING)	When password expiration message is issued	10 The IAO will ensure that PASSWORD(WARNING) SETROPTS value is set to 10. WARNING specifies the number of days before a password expires when RACF is to issue a warning message to the user.
PROTECTALL	RACF-protect all data sets	PROTECTALL The IAO will ensure that PROTECTALL SETROPTS value is set to PROTECTALL. PROTECTALL activates protect all processing. When protect all processing is active, the system automatically rejects any request to create or access a data set that is not RACF protected.
REALDSN	Places actual data set names in messages and SMF records	REALDSN The IAO will ensure that REALDSN SETROPTS value is set to REALDSN. REALDSN specifies that RACF is to record in any SMF log records and operator messages, the real data set name used on the data set commands, and in the RACHECK and RACDEF macros.
RETPD	Selects security retention period for tape data sets	99999 The IAO will ensure that RETPD SETROPTS value is set to 99999. RETPD specifies the default RACF security retention period for tape data sets. The security retention period is the number of days that RACF protection is to remain in effect for the tape data set.

Option	Description	Required Value
RVARYPW	Sets the RVARY passwords	Site defined. Must change default value. To be set in accordance with standard password guidelines. The IAO will ensure that RVARYPW SETROPTS value is set to a non default value. RVARYPW specifies passwords that an operator is to use to respond with requests to approve RVARY command processing.
SAUDIT	Logging of activity of users with SPECIAL attribute	SAUDIT The IAO will ensure that SAUDIT SETROPTS value is set to SAUDIT. SAUDIT specifies whether RACF is to log all RACF commands issued by users with the SPECIAL or group SPECIAL attribute.
SECLEVELAUDIT	Auditing for security levels	NOSECLEVELAUDIT The IAO will ensure that SECLEVELAUDIT SETROPTS value is set to NOSECLEVELAUDIT. SECLEVELAUDIT specifies the SECLABEL profiles auditing options are used in addition to the auditing options specified for the resource profile. This additional auditing occurs whenever an attempt is made to access a resource protected by a profile that has a security label specified.
TAPEDSN	Activates tape data set protection	TAPEDSN The IAO will ensure that TAPEDSN SETROPTS value is set to TAPEDSN. TAPEDSN activates tape data set protection. When tape data set protection is in effect, RACF can protect individual tape data sets as well as tape volumes.
TERMINAL	Universal access authority for terminals	READ The IAO will ensure that the TERMINAL SETROPTS value is set to READ; this sets the universal access authority (UACC) associated with undefined terminals.
WHEN(PROGRAM)	Program control	WHEN(PROGRAM) The IAO will ensure that WHEN(PROGRAM) SETROPTS value is set to WHEN(PROGRAM). WHEN(PROGRAM) activates RACF program control, which includes both access control to load modules and program access to data sets.

Option	Description	Required Value
Note: Global Access Table Information: The use of the RACF Global Access Table option (GLOBAL in SETROPTS) is optional for each site and may improve system performance. When access is requested, the Required Global Access Table is checked first because it resides in memory. By placing resources that are frequently accessed and have a UACC of read in this table, no further checking is made if the requested access is granted. If no entry exists in the Global Access Table, or the desired access is greater than specified in the table, a search is then made of the RACF database. While the use of the Global Access Table is a site option, the decision to use it should be carefully made and will consider the following: Only frequently accessed resources should be considered. No RACLISTed resources will be included because these requests bypass the table. Only widely available resources will be included (e.g., SYS1.BRODCAST, SYS1.HELP, etc.). Any resources that require logging and/or audit trails will not be included in the Global Access Table.		

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Section 3.3.1; Table A-. REQUIRED GLOBAL OPTIONS (SETROPTS) - RACF (3.3.1).

3.1.1 PROTECTALL MODE

The PROTECTALL value will display the mode that the RACF system is in. There is only one acceptable DISA setting to ensure that any access attempts not specified by the system will not be allowed and will be logged. The PROTECTALL SETROPTS value must be set to PROTECTALL which ensure that they system will automatically reject any request to create or access a data set that is not RACF protected.

3.1.1 PASSWORD GUIDELINES

Passwords are used to validate a user to their logonid. Users should create their own passwords, which encourages them to not write them down. However, guidelines must be enforced over the composition of passwords to ensure that user created passwords impose security and cannot be easily guessed.

Weak password setting could allow unauthorized access to system resources or data by a user. By increases the strength of passwords the probability that passwords can be ‘cracked’ decreases significantly.

The DISA STIG recommends following the password guidelines specified below which will ensure the appropriate oversight and control of passwords; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) After three consecutive password failures, the userid is to be suspended until reset by the IAO or authorized personnel.

2) Passwords are to be eight (8) characters in length.

3) Passwords are to be a mix of alphabetic, numeric, and special characters, including at least one of each. Special characters include the national characters (i.e., @, #, and $) and other non-alphabetic and non-numeric characters typically found on a keyboard. However at this

time the three ACPs only support the national characters. The following set represents the complete list of characters currently supported by the three ACPs:

ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789@#$

Note: Lower case alphabetic characters are not supported by the three ACPs.

4) Each character of the password is to be unique, prohibiting the use of repeating characters.
5) Passwords are to contain no consecutive characters (e.g., 12, AB).
6) Passwords are not to include the user's name, telephone number, userid, or any standard dictionary word.
7) Users are to be required to change their password every 90 days at a minimum. Users are permitted to manage and change their own passwords.
8) Passwords are not to be changed more than once every 24 hours without the intervention of the IAO or authorized personnel.
9) Users are not to be permitted to reuse a password assigned within the last ten password changes.
10) The password files are to be stored in encrypted form.
11) Password requirements are to be enforced by standard security product controls where possible.
12) Exits are only to be used where the requirements cannot be enforced by standard security product controls. (Refer to the DISA STIG Section 3.1.3.2, Password EXIT Processing (volume 1), for further information.)

Note: Adherence is required when the software has the capability to enforce. Otherwise the password policies not enforced by the software are to be documented in the site Security Features Users Guide.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.3.1 Password Guidelines.

The above password requirements should be enforced by RACF by use of the RACF SETROPTS settings and (optionally) the password validation exit (Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.2.3.2, Password EXIT Processing).

Most of the passwords requirements can be enforced by RACF, however as noted with the STIG, the below list cannot.

Table 2 Password Requirements Not Enforced by RACF

Password Requirements not Enforced by RACF
No words found in standard dictionaries are to be used.
At least one alphabetic, numeric, and special character is to be used.
Each character of the password is to be unique.
Passwords are to contain no consecutive characters (e.g., 12, AB).
Are not to contain the user's name, userid, or telephone number.

Password Requirements not Enforced by RACF
Passwords cannot be changed more than once every 24 hours without IAO intervention.

Where password standards cannot be enforced by RACF the STIG recommends use of EXITS. If this method is used, the following exit should be used to implement these controls:

RACF Exit: ICHPWX01

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.3.2, Password EXIT Processing.

3.1.1 TSO PARAMETERS

RACF intercepts some operating system requests made by programs like TSO, taking control and deciding if the request should be allowed, allowed but logged to SMF, or denied and logged to SMF. RACF will make this choice based on the total environment and rules that specify under conditions access should be allowed. Total environment considers components such as the user who made the request, the data set name, and the program making the request. TSO is one such component; TSO allows users to establish a session where they can issue commands.

The PARMLIB command is an authorized TSO command processor that provides users the ability to display and dynamically change, without an IPL, the active IKJTSOxx member of SYS1.PARMLIB. A user with the ability to add or alter programs within IKJTSOxx could give a program APF-authorization which could then execute privileged instructions, interfering with production applications and data.

The DISA STIG recommends the following in regards to TSO controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

- Control authority to execute this command by permitting user access to the RACF PARMLIB resource of the RACF TSOAUTH resource class. Only systems programmers responsible for supporting TSO/E should be authorized to access the PARMLIB command.
- The following steps provide examples of RACF commands necessary to control the PARMLIB command:

  a) Activate the TSOAUTH resource class:

     SETROPTS CLASSACT(TSOAUTH)

  b) Define the PARMLIB resource to the TSOAUTH resource class allowing no user access:

     RDEFINE TSOAUTH PARMLIB UACC(NONE)

  c) Permit a user access to the PARMLIB command to display specifications in the active IKJTSOxx member:

     PERMIT PARMLIB CLASS(TSOAUTH) ID(user1) ACCESS(READ)

  d) Permit a user access to the PARMLIB command to display and dynamically change the active IKJTSOxx member:

PERMIT PARMLIB CLASS(TSOAUTH) ID(user1) ACCESS(UPDATE)

RACF controls a number of other privileges in the TSOAUTH general resource class. The DISA STIG states that TSOAUTH privileges such as OPER and ACCT, as well as access to the TSO/E CONSOLE facility, will be strictly controlled.

Attributes for most TSO-level controls can be found in the RACF TSO segment of a user's profile. If a user logs on to TSO and does not have a defined TSO segment, TSO checks the SYS1.UADS data set for the user's information. If TSO does not find an entry for the user in SYS1.UADS, the logon attempt is terminated.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that access to TSO logon procedures is controlled and that access to multiple logon procedures are limited to authorized personnel.
- The organization will not grant the Device Mount privilege to on-line TSO users. It may be granted to STC userids that execute TSO in batch on an as-needed basis.
- The IAO will strictly control and limit access to TSOAUTH privileges. Authorization is restricted to authorized personnel and justification for access is documented.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 7.2 TSO, 7.2.2 RACF.

3.2 USER MANAGEMENT

3.2.1 USER CONTROLS

Each RACF user is uniquely identified by a RACF userid. To RACF, a user can be an individual, a started task, or a batch job. When a new userid is created in RACF, the system automatically creates a user record with the following information:

NAME	User's Name
DFLTGRP	Default Group
OWNER	User's profile owner
PASSWORD	Password

It is possible for the security administrator to specify a password when creating a new user. If a password is not specified, the default group specified in the SETROPS will be used as the new user's password. The DISA STIG states that the organization should assign a unique password to every userid to prevent unauthorized access by a person who knows the default group for a new userid.

Within RACF each userid is associated with certain privileges so it is imperative that individuals have unique ids. Without unique userids users will be assigned access which may not enforce

the concept of least privileged. Appropriate controls over access cannot be enforced with shared ids. In addition, logging will not be affective because the organization will not be able to appropriately determine which user performed the invalid function or violation. Thus there is no accountability.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that every USERID is uniquely identified to the system. Within the USERID record, the users name, default group, the owner, and the users' password fields are completed.
- The IAO will ensure that every user is uniquely identified to the system. Userids are not shared among multiple users.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.2 Userid Controls.

3.2.1 INTERACTIVE USERS AND PARAMETERS

As discussed above userids are established for users, started tasks, and batch jobs. For all users the STIG outlines requirements within RACF as follows:

1) Apply the principle of least privilege in the granting of all user privileges. Grant individual users the minimum resource authorizations necessary to accomplish their assigned functions. Only grant access to system resources as required.
2) Generate group profiles for all groups of users (e.g., general users, started tasks). These group profiles will identify the minimum privileges necessary for each group of users to accomplish its assigned functions. Associate every user's userid with at least one group profile.
3) Alternatively, if a user requires additional authority not granted to that user's default group, the user may be connected to one or more additional RACF groups on a permanent or a temporary basis. Because the installation is employing List-of-Groups checking, the user is given the highest level of authority allowed by any associated RACF group.
4) When a RACF userid initially is added, the Last Access Date (LAST-ACCESS) is set to UNKNOWN. Hence, an unused userid never expires due to inactivity. This results in non-expired, unused userids in the RACF database. Therefore the site should ensure that the local procedures for adding an interactive user include issuing the ALTUSER <userid> RESUME command. This sets the LAST-ACCESS from UNKNOWN to the current date and time and thus enforce the expiration of the userid after 35 days of inactivity, even if the userid is never used.

In addition, userids contain fields which values should be controlled. The DISA STIG recommends the following values that should be specified for certain selected fields as user privileges and access are granted:

Table 3 Recommended UserID Field Settings

Field	Short Description	Required Value
ACCTNUM	Specifies the user's default TSO logon account. Used for all billing.	May be required for Fee-for-Service support.
DATA	Installation data field. Note: Field may be used for validation by other products (e.g., Netmaster).	Optional
DFLTGRP	User's default group	Will be completed for all users.
NAME(username)	Specifies the 1- to 20-character name of the use.	Will be completed for all users.
OWNER	User's profile owner	Will be completed for all users.
PASSWORD	Logon password for the user	Will be completed for all users.
PROC	Specifies the user's default TSO logon procedure	Will be completed for all TSO users.
SECLABEL	User's current security label	Optional for MAC II Sensitive
USERDATA	Optional user data	Site defined

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Interactive userids have the values specified in the above table completed.
- The IAO will ensure that ALL RACF users are assigned a group profile.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.2.1 Interactive Users.

3.2.1 STARTED TASK CONTROL (STC) USERS

Started tasks are procedures started from the operating system console with the MVS START command. Like batch jobs, it is possible to assign a RACF userid to started tasks to control the activities performed by a resources available to the started task. By default started tasks do not run under a specific userid, allowing the task to operate without being identified to RACF. Without controls over this process, started tasks have the authority to access any information in the O/S.

Every started task should be uniquely identified to the ACP by the IAO. This will ensure that the resources available to the task are limited to only those resources deemed necessary. Additionally, it uniquely identifies the actions of the task in log data which can be used to trace system problems. Software Support personnel should notify the IAO so that a unique userid can be assigned to any new started task added to the system. No default userids are to be assigned to started tasks otherwise not identified.

Started tasks are stored as members in program libraries. It is possible for both started tasks and non-started tasks to exist in the concatenated libraries. These typically are procedures intended for general use as batch processes or for use by TSO users. To prevent their improper execution, these members should not be defined to RACF as started tasks.

The DISA STIG recommends the following in regards to STC; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) All started tasks will be assigned a unique userid. The Started Task Control (STC) should be granted the minimum access authorities necessary to perform its function.

2) All STC userids will be defined as PROTECTED userids. Protected user IDs cannot be used to enter the system by any means that requires a password, such as logging on to TSO, signing on to CICS, or running a batch job that specifies a password on the JOB card.The following command shows the ALTUSER command used to assign the PROTECTED attribute to an existing userid:

   ALTUSER stc-userid NOPASSWORD

3) Connect all started task userids to a valid STC Group ID. Only connect STC userids to STC Group IDs.

4) All STCs not defined to RACF are run as an undefined user.

5) All STCs will have a matching profile defined to the STARTED resource class. The STARTED resource class allows profiles to be defined in this class for each job, or group of jobs, that needs to run under a unique userid. A profile can be created for a specific STC, or a more generic profile can be created for a grouping of STCs with the same access requirements. There is also a generic "catch-all" profile of '**'. The STDATA segment of these profiles is to specify a valid RACF userid and Group ID. A value of '=MEMBER' may be used to substitute the program library member name of the JCL procedure as the userid. For example:

   - The following RACF command defines a CICS profile:

     RDEFINE STARTED CICS*.* UACC(NONE) OWNER(admin)

     STDATA(USER(=MEMBER) GROUP(STCCICS) TRUSTED(NO))

   - The following RACF command defines a TCP/IP profile:

     RDEFINE STARTED TCPIP.* UACC(NONE) OWNER(admin)

     STDATA(USER(TCPIP) GROUP(STCTCPX) TRUSTED(NO))

6) Certain started tasks performing critical operating system related functions may be considered trusted for the purpose of data set and resource access requests. For these STCs, all access requests will be honored. The STIG standard for identifying trusted procedures is to define a specific, discrete profile for the STC to the STARTED resource class and to enable the TRUSTED flag within the profile. For example:

   RDEFINE STARTED JES2.* UACC(NONE) OWNER(admin)

STDATA(USER(JES2) GROUP(STCTRUST) TRUSTED(YES))

This will ensure that other STCs are not unintentionally added to the same profile as a trusted started task, thereby granting privileges access. Note: STCs identified as trusted are not to be granted the OPERATIONS attribute. Granting the OPERATIONS attribute would allow the started task referenced in the profile to bypass dataset security rules.

7) In addition to using the STARTED resource class to define started task profiles, a built-in RACF table can also be used, however this method is not recommended. To ensure RACF uses the STARTED resource class and not the ICHRIN03 started procedures table, define a matching generic catch all profile of '**' to the STARTED resource class. For example:

   RDEFINE STARTED ** UACC(NONE) OWNER(admin)

   STDATA(USER(=MEMBER) GROUP(STC) TRUSTED(NO))

   The STC GROUP identified with the generic profile of '**' is not to be granted any explicit data set or resource access authorizations. All access authorizations are to be dependent on the userid.

8) The ICHRIN03 started procedures table is to be maintained to support recovery efforts in the event the STARTED resource class is deactivated or critical STC profiles are deleted from the STARTED resource class. Ensure that STCs critical to support this recovery effort (e.g., JES2, VTAM, and any appropriate site specific tasks) are maintained in ICHRIN03 to reflect current STARTED resource class profiles.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that all started tasks are assigned a unique userid
- The IAO will ensure that all started tasks are assigned to a group ID
- The IAO will ensure that only trusted STCs have the TRUSTED flag enabled within the profile

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.2.3 STC Users.

3.2.1 EMERGENCY ACCESS USERS

Any processing environment will have situations that arise that are required to be immediately resolved so that data processing can occur. During these emergencies personnel may need elevated levels of access with additional privileges. To handle these situations emergency ids, also referred to as super ids or firecall ids, may need to be enacted.

Since these logonids generally have access which will bypass system security they must be secured so that individuals do not have general access to them, if used they must be logged and reviewed, and access should be automatically revoked after a period of time.

The DISA STIG recommends the following in regards to emergency access controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) One class of userids are to exist to perform all operating system functions except ACP administration. These super IDs may be released according to STIG recommended policy to effect repairs of the operating system in emergencies.

2) A second class of super IDs is to be maintained to allow the functions associated only with ACP administration. These IDs are to only be released at the direction of the IAO.

3) Normally both super IDs are not to be released to the same individual concurrently, although approved exceptions to this rule can be made. This constraint effects a check and balance process for recovery situations requiring both forms of authorization.

4) The super IDs are to be implemented with logging to provide an audit trail of their activities.

5) Both classes of super IDs are to be maintained in both the ACP and SYS1.UADS to ensure they are available in the event that the ACP is not functional.

6) Each super ID is to have distinct, different passwords in SYS1.UADS [user attribute data set] and in the ACP, and the site is to establish procedures to ensure that the passwords differ. The password for any ID in SYS1.UADS is never to match the password for the same ID in the ACP.

7) Documented procedures are to be established to provide a mechanism for the use of the IDs. Their release for use is to be logged, and the log is to be maintained by the IAO. When a super ID is released for use, its password is to be reset by the IAO within 12 hours after it is no longer needed for problem resolution.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.2.6 Emergency Userids.

3.2.2 EMERGENCY PRIVILEGED ACCESS IN RACF

As discussed above the STIG recommends emergency userids be defined in both the ACP and in the SYS1.UADS dataset, in case the ACP is not functional when then system needs to be restored.

The DISA STIG recommends the following in regards to emergency access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Emergency userids should be defined with the GROUP(NONE) specification and the OPERATIONS attribute. Full TSO access will be allowed. Also define the user with full access to all DASDVOL resource classes.

2) The emergency userid for security administration should also be assigned the SYSTEM SPECIAL attribute.

3) Implement each of these userids with logging enabled to track all activity performed by the userids.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Emergency USERIDs are defined with the GROUP(NONE) specification and the OPERATIONS attribute having full access to all DASDVOL resource classes with logging enabled. The userid established for security administration has the SYSTEM-SPECIAL attribute.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.2.6 Emergency Userids.

3.2.3 PRIVILEGED ACCESS USERS

Every ACP provides attributes (types of privileges) that can allow a user to modify the security environments, perform auditing tasks, and circumvent security.

Within RACF, a number of privilege levels have been defined to provide different levels of authority over the system. The three powerful and commonly assigned privileges are discussed below along with Tape Bypass Label Processing (BLP).

Table 4 Privilege Levels

Privilege	Description
SPECIAL	Permits the user full control over all resource profiles and RACF options in the RACF database. It does not allow the user to access all resources, but will allow the user to authorize themselves so they can have access.
AUDIT	Permits the user to control audit (logging) activities for all RACF profiles. It does not give the user any additional authority to access resources, such as data sets, or to alter other details of RACF profiles.
OPERATIONS	Permits a user full access to all resources where allowed in the Class Descriptor Table, CDT. The dataset CLASS will honor the OPERATIONS attribute. If a user is specifically identified either via USERID or a connected GROUP, then that level of access is taken in precedence of OPERATIONS. The OPERATIONS attribute does not allow the user to modify or delete the RACF profile covering the resource.
Note: Users can be granted access to these attributes if they are part of a group which is granted access. Users who have the group-SPECIAL, group-AUDITOR, or group-OPERATIONS attributes are restricted to only profiles that are within the scope of their groups.	
TAPE BLP	In addition to being used for system backups, magnetic tapes are often used as the source for data input and output for system processing. Organizations may receive tapes from other systems that are used as data input. To avoid the hassle of creating access rules every time a tape is received and loaded on the mainframe, an organization can enable the use of Bypass Label Processing (BLP). The ability to bypass the tape label is a privilege assigned to an individual through RACF. If BLP is specified in a submitted mainframe job, security validation for datasets on that job will be bypassed because the internal tape label with the dataset name will not be read. Tape BLP is thus a very powerful privilege, and although it is clearly useful in day-to-day processing, the risk of misuse or abuse presents a serious vulnerability.

The DISA STIG recommends the following general recommendations in regards to privileged access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Only the IAO is to be given any privileges that can modify the security environment, such as changing system-wide options.

2) Note that while the DISA STIG recommends that only the IAO should have privileges to modify the security environment it is understandable that other authorized users may require such functionality. However, all access should be granted based on least privilege, authorized, logged, and monitored.

3) Users allowed to perform security administration for application-related data are to be limited by the ACP to only change properties for which the user is responsible.

4) Privileges to view the contents of the security database may be granted to individuals by the IAO, provided a valid need exists. In many data centers, this access may be required for interactive system programmers to work with the user community to resolve problems.

5) Access to privileges to perform tape bypass label processing (BLP) is to be tightly controlled and only given to those authorized data center individuals (e.g., the tape librarian, Operations staff, or user) who require such access. Tape label bypass privileges allow a user to access data on a tape, using BLP processing, and, as such, to bypass any security-related controls. Therefore, authorization to perform BLP processing by the user community is to be tightly controlled. This is because a severe exposure exists in that any data on any tape can be accessed. Reasons for granting such access should be documented and available for inspection.

6) In addition to the special privileges specifically noted above, many other special privileges pose the danger of compromising the operational environment when misused or improperly applied. Each ACP provides the ability to control these privileges and to restrict them only to those personnel with valid requirements for their use. These special privileges include, but are not limited to, the ability to do the following tasks:

    - Mount tape volumes to a TSO session
    - Access system console information
    - Issue console commands
    - Execute restricted programs
    - Access data and resources despite rule restrictions

7) Restrict access to special privileges only to those individuals with an authorized need. Grant access to the minimum level necessary for the performance of job requirements. Reasons for granting such access should be documented and available for inspection.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.1.4.1 Access Control Product Modification Privileges, 3.1.4.2 Audit Privileges, 3.1.4.3 Tape Label Bypass Privileges, 3.1.4.4 Other Sensitive Privileges.

The DISA STIG recommends the following in regards to privileged access attributes within RACF; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) The special privileges discussed in this section are all of an extremely sensitive nature and will be rigidly controlled. The number of authorized users granted these privileges will be kept to an absolute minimum. Their use will be fully documented. The IAO will maintain the written request, justification, and authorization.

2) Limit the number of userids granted SPECIAL and GROUP-SPECIAL privileges to the minimum number necessary. Delegation of GROUP-SPECIAL processing to other personnel by site-defined Group Administrators is forbidden.

3) Limit the number of userids granted the AUDITOR privilege to the minimum number necessary. Specifics regarding the use of the AUDITOR privilege can be found in the RACF Security Administrators Guide.

4) Restrict the bypass label processing (BLP) privilege at the userid level, and grant access to the minimum number of necessary users. Implement the following controls:

    - If a tape management system (e.g., CA-1) is installed on the system, use the facilities of the resident tape management system to control BLP. In this case, activation of the TAPEVOL class is not required.

    - If no tape management system (e.g., CA-1) is installed on the system, use the RACF ICHBLP controls to control BLP access. In this case, activation of the TAPEVOL class is required. Grant authorized users of BLP the following authorities:

        i) The appropriate authority to profile ICHBLP in the FACILITY class

        ii) The appropriate access authority to the requested tape volume(s)

5) Limit the number of userids granted OPERATIONS and GROUP-OPERATIONS privileges to the minimum number necessary. Delegation of GROUP-OPERATIONS processing to other personnel by site-defined Group Administrators is forbidden.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that users granted SPECIAL privileges are limited to security group and administrators, except those requiring AUDITORS attributes. Documentation providing justification for any additional users are filed.

- The IAO will ensure that users granted AUDITOR privileges are limited to a minimum. Documentation providing justification for any additional are filed.

- The IAO will ensure that users granted TAPE BYPASS LABEL PROCESSING (BLP) privileges are limited to a minimum. Documentation providing justification for this privilege are filed.

- The IAO will ensure that the number of users granted OPERATIONS privileges are limited and documentation for justification for users outside of operators and system programmers are maintained.
- The IAO will strictly control and limit access to TSOAUTH privileges. Authorization is restricted to authorized personnel and justification for access is documented.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, 3.3.4 Special Privilege Access, 3.3.4.1 Access Control Product Modification Privileges, 3.3.4.2 Audit Privileges, 3.3.4.3 Tape Label Bypass Privileges.

3.3 RESOURCE CONTROLS

ACF2, RACF, and TSS provide capabilities to control access to system resources. System resources include data sets, volumes, spool volumes, sensitive utilities, and other programs, for example. Control of access to these resources is critical to ensure the integrity of the operating environment. For example, inappropriate access to PARMLIB could allow an individual to place an unauthorized program into an APF authorized library thus allowing the program to gain supervisor state. By gaining this access the program would have privileges usually reserved for the O/S. The user could have full access to data sets and make alterations to payroll data.

The DISA STIG provides information relating to data set controls, volume controls, sensitive utility controls, dynamic list controls, console controls, and system command controls. The following will focus on ACP controls for sensitive utilities, dynamic control lists, console access, system commands and transaction control.

3.3.1 CONTROLLING SENSITIVE UTILITIES

Sensitive utilities such as OMEGAMON, CICS, DASD, ICKDSF, etc. are required in most data centers to support various operations and processing. These products must be appropriately controlled as they are allowed to operate with privileges normally reserved for the OS. If a user could abuse the privileges of these programs they could potentially gain access to operate in supervisor state or with a protect key of 0-7. This could result in system failure, data manipulation, and bypassing of security in place. Therefore access to these programs should be very restricted. ACPs can be used to protect the utilities from unauthorized access at the program level. Each utility installed on the system should be evaluated to determine appropriate access.

The DISA STIG provides the following table of sensitive utility types and the type of user that should be granted access.

Table 5 Sensitive Utility Type/User

Sensitive Utility Controls	
UTILITY TYPE	**LEGITIMATE USERS**
Tape Management	Tape Librarian

Sensitive Utility Controls	
DASD Management	DASD Management staff
Job Scheduling	Production Control
Storage Alteration	Systems Programming
System Modification	Systems Programming

The DISA STIG provides the following table which displays a sample list of the minimal entries to be controlled:

Table 6 Sensitive Utility Controls

Sensitive Utility Controls		
PROGRAM	**PRODUCT**	**FUNCTION**
***GTF**	OS/390	System Activity Tracing
***IOCP	OS/390	System Configuration
*MASPZAP	OS/390	Data Management
AMAZAP	OS/390	Data Management
BLSROPTR	OS/390	Data Management
DEBE	OS/DEBE	Data Management
DITTO	OS/DITTO	Data Management
FDRZAPOP	FDR	Product Internal Modification
GIMSMP	SMP/E	Change Management Product
ICKDSF	OS/390	DASD Management
IDCSC01	OS/390	IDCAMS Set Cache Module
IEHATLAS	OS/390/DFP	Data Management
IEHD****	OS/390/DFP	DASD Management
IEHINITT	OS/390	Tape Management
IFASMFDP	OS/390	SMF Data Dump Utility
IGWSPZAP	OS/390	Data Management
IND$FILE	OS/390	PC to Mainframe File Transfer (Applicable only for classified systems)
*****SCP	OS/390	System Configuration
WHOIS	OS/390	Share MOD to identify user name from USERID. Restricted to data center personnel only.

The DISA STIG recommends the following in regards to controlling sensitive utilities by use of RACF; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Access to sensitive utilities will be strictly controlled. Utility program controls are provided via the PROGRAM resource class. Control access to the data sets in which the utilities reside through the use of data set access permission.

2) Control maintenance utilities as previously described within Section 3.1.2.5, Special Storage Management Users. The ability to execute privileged programs will be strictly controlled, and will be permitted to the minimum number of users.

3) Audit access to protected programs considered sensitive in nature. These programs will include, at a minimum, those specified within the section above.

4) The libraries in which sensitive programs and utilities can reside either are part of the system Linklist (they are publicly available), or they reside in libraries that are not in the Linklist (they are considered private libraries for the purpose of program protection). The methods used to protect these programs vary based on whether they are public or private.

    a) Use RACF program controls to control programs and utilities that reside in public (Linklist) libraries:

        i) Define a profile for each program name and alias in the PROFILE general resource class. Each profile will identify the library that contains the program, and the volume on which the library resides. The profile will also include the AUDIT option to ensure auditing of the use of the program.

        ii) Limit user access to each library that contains sensitive programs and utilities to read access in the associated DATASET class profile. This protects the programs from being copied, renamed, and then executed.

    b) Programs and utilities that reside in private (non-Linklist) libraries can only be controlled as execute-controlled libraries. This is done by using DATASET class profiles, if RACF, Version 1, Release 8.1, and DFP, Version 3, Release 1.0 or later, are installed. For these libraries, grant only execute access to users. Read access will not be granted.

        Do not confuse RACF program controls with the RACF Program Access to Data Sets (PADS) feature. PADS is a data set control feature, not a program control feature.

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that Access to sensitive utilities are limited and logged. A letter justifying any additional access is filed.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.5.3 Sensitive Utility Controls.

3.3.1 DYNAMIC CONTROL LIST

MVS provides capabilities to perform dynamic changes within the OS. Specifically, inherent to MVS, dynamic maintenance can be performed on EXITS and APF Libraries. The capability to perform dynamic EXIT maintenance is controlled by the CSVDYNEX macro, the SYS1.PARMLIB(PROGxx) member, the SET PROG=xx command, and the SETPROG EXITS command. The command SET PROG=xx dynamically changes the EXIT definitions based on the information in the specified PROGxx member. The SETPROG EXITS command provides the capability to selectively add and delete EXIT routines from EXIT definitions.

Without appropriate controls in place users could dynamically update libraries to be APF authorized, which could provide a means to obtain supervisor state. In addition, users could update EXITS and insert code that would allow them to obtain special privileges. Without appropriate control the organization cannot ensure the integrity of the OS. These facilities, if made available to operators are to be controlled.

The DISA STIG recommends the following in regards to controlling dynamic control listings; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Define the following resources in the FACILITY class with a default access of none:

   CSVAPF.**

   CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC

   CSVAPF.MVS.SETPROG.FORMAT.STATIC

   CSVDYNEX.**

   CSVDYNL.**

   CSVDYNL.UPDATE.LNKLST

2) Limit authority to those resources to Systems personnel. Restrict this access to the absolutely minimum number of personnel, and log all accesses.

3) Limit authority to the SET PROG=, SETLOAD, and SETPROG commands to Systems personnel. Restrict this access to the absolutely minimum number of personnel, and log all accesses. For additional information refer to the DISA STIG section 3.1.5.6, OS/390 System Command Controls [volume 1].

Within RACF dynamic list controls are provided via resources in the FACILITY resource class. This class should already be active and use generic masking, but the sample commands shown below include the relevant SETROPTS commands for the sake of completeness. When protecting the facilities for dynamic lists via the FACILITY class, the DISA STIG recommends the following:

1) Prevent access to these resources by default, and log all access. Create generic and specific profiles as follows:

   SETROPTS GENERIC(FACILITY)

RDEFINE FACILITY CSVAPF.** AUDIT(ALL) UACC(NONE)

RDEFINE FACILITY CSVAPF.MVS.SETPROG.FORMAT.DYNAMIC

AUDIT(ALL) UACC(NONE)

RDEFINE FACILITY CSVAPF.MVS.SETPROG.FORMAT.STATIC

AUDIT(ALL) UACC(NONE)

RDEFINE FACILITY CSVDYNEX.** AUDIT(ALL) UACC(NONE)

RDEFINE FACILITY CSVDYNL.** AUDIT(ALL) UACC(NONE)

RDEFINE FACILITY CSVDYNL.UPDATE.LNKLST

AUDIT(ALL) UACC(NONE)

SETROPTS CLASSACT(FACILITY)

SETROPTS RACLIST(FACILITY) REFRESH

2) The required access to specific resources is to be discretely granted to specific systems users. Restrict this access to the absolutely minimum number of personnel, and log all access. Sample commands are as follows:

RDEFINE FACILITY CSVAPF.SYS1.NEWLIB AUDIT(ALL) UACC(NONE)

PERMIT CSVAPF.SYS1.NEWLIB CLASS(FACILITY) ID(sysprog)

ACCESS(READ)

The DISA STIG provides the following technique related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that FACILITY resource class is active.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.5.4 Dynamic List Controls.

3.3.1 CONTROLLING CONSOLE ACCESS

Consoles allow a user to directly enter operator commands without being validated by a unique user name or password. Any actions taken cannot be logged to a specific user but rather the console from which the commands were entered. Therefore, with consoles, there is limited accountability. Console commands are very powerful and can be used for a variety of functions, such as updating APF authorized libraries, system parameters within PARMLIB, or EXITS. Therefore access to consoles must be stringently controlled as any user with physical access to a console can enter such commands.

Normally consoles are located within a physically secured area such as the computer room within a data center. However, just securing consoles within a restricted area may not be

adequate because of remote console access. This access allows authorized personnel the ability to log into a console session and issue commands outside of the secured area. The ability to log the remote access is available, however, any actions completed after logging into the console cannot be traced back to the user. These commands will be attributed to the console being used at the time. The SYS1.PARMLIB(CONSOLxx) member is used to control consoles; a very limited number of operators should be provided this access.

The DISA STIG recommends the following in regards to controlling console access; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Give every console an explicit console ID, and define that ID to the ACP as a user with only those access rights required for use of the console. Define every console, including extended MCS [multiple console support] consoles, with AUTH(INFO).

2) In SYS1.PARMLIB(CONSOLxx), specify the parameter LOGON(REQUIRED) on the DEFAULTS statement so that all operators are required to log on prior to entering OS/390 system commands. At the discretion of the IAO, LOGON(AUTO) may be used, provided the console userids are only authorized to use the CONTROL, DISPLAY, MONITOR, STOPMN, STOPTR, and TRACK commands, and their access is limited to read level.

3) The IAO will implement and document controls as described in the DISA STIG, Section 3.1.5, Resource Controls (volume 1).

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 2.1.2.12 MCS Consoles.

Within RACF MCS (multiple console support) console controls are provided via resources in the CONSOLE, OPERCMDS, and TSOAUTH resource classes. These classes should already be active, and OPERCMDS should already use generic masking, but the sample commands shown below include the relevant SETROPTS commands for the sake of completeness.

The DISA STIG recommends the following in regards to controlling console access within RACF; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Prevent access to these resources by default, and log all access. Create generic and specific profiles as follows:

```
RDEFINE CONSOLE * AUDIT(ALL) UACC(NONE)

RDEFINE CONSOLE consname AUDIT(ALL) UACC(NONE)

PERMIT consname CLASS(CONSOLE) ID(opergrp) ACCESS(READ)

SETROPTS CLASSACT(CONSOLE)

SETROPTS RACLIST(CONSOLE) REFRESH

SETROPTS GENERIC(OPERCMDS)

RDEFINE OPERCMDS MVS.** AUDIT(ALL) UACC(NONE)

SETROPTS CLASSACT(OPERCMDS)
```

SETROPTS RACLIST(OPERCMDS) REFRESH

RDEFINE TSOAUTH CONSOLE AUDIT(ALL) UACC(NONE)

SETROPTS CLASSACT(TSOAUTH)

SETROPTS RACLIST(TSOAUTH) REFRESH

2) The user profile for each real MCS console is to be granted read access to the corresponding console resource:

   PERMIT consname CLASS(CONSOLE) ID(consname) ACCESS(READ)

3) The group and user profiles for operators and systems programmers allowed to use each real MCS console are to be granted read access to the corresponding console resource:

   PERMIT consname CLASS(CONSOLE) ID(opergrp) ACCESS(READ)

4) At the discretion of the IAO, users may be allowed to use the TSO CONSOLE command, subject to the restrictions in Section 3.1.5.5, MCS Console Controls, Section 3.1.5.6, OS/390 System Command Controls, and Section 3.3.5.6, OS/390 System Command Controls.

   ALTUSER userid OPERPARM(AUTH(INFO))

   PERMIT MVS.MCSOPER.userid CLASS(OPERCMDS) ID(userid)

   ACCESS(READ)

   PERMIT CONSOLE CLASS(TSOAUTH) ID(opergrp) ACCESS(READ)

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The system programmer will ensure that the CONSOLxx members are properly configured.
- The IAO will ensure that all consoles identified in the CONSOLxx members are defined to the ACP.
- The IAO will ensure that OS/390 Sensitive System Commands are defined to the OPERCMDS resource class. Only a limited number of authorized people are able to issue these commands. All access is logged.
- The IAO will ensure that CONSOLE resource class is active.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.5.5 MCS Console Controls.

3.3.1 CONTROLLING SYSTEM COMMANDS

This document has discussed various system commands, also referred to as operator commands, and the risks and controls associated with them. OS/390 system command controls are provided via resources in the OPERCMDS resource class. This class should already be active and use

generic masking. Further system commands can be controlled by the ACP, the sample commands shown below include the relevant ACP commands for the sake of completeness.

The DISA STIG recommends the following in regards to controlling system commands within RACF; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Prevent access to the OS/390 resources by default, and log all access. Create generic and specific profiles with logging as required using the resources defined in Table A-29, Controls on OS/390 System Commands. For example:

   SETROPTS GENERIC(OPERCMDS)

   RDEFINE OPERCMDS MVS.** AUDIT(ALL) UACC(NONE)

   RDEFINE OPERCMDS MVS.ACTIVATE AUDIT(ALL) UACC(NONE)

   RDEFINE OPERCMDS MVS.CANCEL.JOB.** AUDIT(ALL) UACC(NONE)

   RDEFINE OPERCMDS MVS.CONTROL.** AUDIT(ALL(UPDATE))

   UACC(NONE)

   RDEFINE OPERCMDS MVS.DISPLAY.** UACC(NONE)

   RDEFINE OPERCMDS MVS.MONITOR UACC(NONE)

   RDEFINE OPERCMDS MVS.STOPMN UACC(NONE)

   SETROPTS CLASSACT(OPERCMDS)

   SETROPTS RACLIST(OPERCMDS) REFRESH

2) Only grant access to OS/390 system commands to the extent documented in the installation SOP. Define additional profiles similarly to those in Paragraph (1) above if the existing resource names are too specific or too generic for the controls in the SOP. The RDEFINE statements are to include the AUDIT and UACC values specified in the SOP, or AUDIT(ALL) UACC(NONE) if not specified.

   The following is an example of granting a user permission to issue commands against jobs with names beginning pfx, after obtaining permission from the IAO:

   PERMIT MVS.CANCEL.JOB.pfx* CLASS(OPERCMDS) ID(userid) ACCESS(UPDATE)

   PERMIT MVS.MODIFY.JOB.pfx* CLASS(OPERCMDS) ID(userid) ACCESS(UPDATE)

   PERMIT MVS.STOP.JOB.pfx* CLASS(OPERCMDS) ID(userid) ACCESS(UPDATE)

   SETROPTS RACLIST(OPERCMDS) REFRESH

   The following is an example of granting group opergrp permission to issue ROUTE commands to sysid from consid, after obtaining permission from the IAO:

PERMIT MVS.ROUTE.CMD.sysid CLASS(OPERCMDS) ID(opergrp)
ACCESS(READ) WHEN(CONSOLE(consid))

SETROPTS RACLIST(OPERCMDS) REFRESH

The DISA STIG provides the following techniques related to the above recommendations which further expand on the controls and the responsibilities of individuals within the organization. For additional information for each "policy bullet" including the short description identifier and the severity codes refer to the DISA STIG.

- The IAO will ensure that OPERCMDS resource class is active.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 1, Section 3.3.5.6 OS/390 System Command Controls.

3.3.2 CICS TRANSACTION CONTROL

Customer Information Control System (CICS) is a system utility that allows an authorized user the ability to connect from their terminal to run transactions and application processing on the mainframe. CICS invokes application programs in response to transactions entered at terminals.

The DISA STIG, volume 2, discusses controls for CICS transaction control within RACF. The following sections should be reviewed. In addition, the organization should ensure that controls are in place for any utility that allows connections to the mainframe, such as TSO.

- RACF/CICS Security Related System Initialization Parameters
- Propagation Control
- Surrogate Job Submission Controls
- CICS User Controls
- CICS Terminal Controls
- CICS Transaction Controls

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Volume 2.

4 CONCLUSION

This document is meant to relay pertinent information within the STIG to CMS and applicable CMS Contractors. This document does not cover all topics discussed in the DISA STIG and is not intended to be used as a substitute to the STIG. In addition, access privileges denoted within this document and DISA STIG may not be suitable for every organization, meaning that each organization may choose to be more restrictive. Because every organization is unique not all aspects of this document or the DISA STIG may be applicable.

This document is to be used as a guide to securing organization environments, and by following the recommendations and techniques within organizations will be able to secure the confidentiality and integrity of their data and resources.

Appendix A – CMS Minimum Security Requirements (CMSRs)

Refer to *CMS Information Security Acceptable Risk Safeguards (ARS) Including CMS Minimum Security Requirements*, Appendix A, *CMS Minimum Security Requirements for High Impact Level Data*, for the applicable CMSRs.

Appendix B - Glossary and Acronym Listing

ACEE	Access Control Environment Element
ACF2	Access Control Facility 2
ACID	Accessor ID
ACPs	Access Control Products
APF	Authorized Program Facility
BLP	Bypass Label Processing
CA	Computer Associates or Certificate Authority
CAISSF	CA's International Standard Security Facility
CDT	Class Descriptors Table
CICS	Customer Information Control System
CMP	Change Management Process
CMS	Centers for Medicare and Medicaid Services
CPU	Central Processing Unit
CMSRs	CMS Minimum Security Requirements
CWF	Common Working File
DAA	Designated Approval Authority
DAT	Dynamic Access Translation
DCA	Departmental Control Acid
DD	Data Definition
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information System Agency
DMERCs	Durable Medical Equipment Regional Carriers
DoD	Department of Defense
EDC	Enterprise Data Centers
ETMS	External Tape Management System
FI	Fiscal Intermediary
FTP	File Transfer Protocol
FTPD	File Transfer Protocol daemon program

FTPDNS	File Transfer Protocol server program
GSO	Global Systems Options
HFS	Hierarchical File System
HHS	Health and Human Services
HLQ	High Level Qualifier
IAC	Installation Account Code
IANA	Internet Assigned Numbers Authority
IAO	Information Assurance Officer
IBM	International Business Machines
ICS	Internet Connection Sharing
IMS	Information Management System
IP	Internet Protocol
IPL	Initial Program Load
ISPF	Interactive System Productivity Facility
IT	Information Technology
I/O	Input/Output
JCL	Job Control Language
JWT	Job Wait Time
LAN	Local Area Network
LID	Logonid
LSCA	Limit Control ACID
LU	Logical Unit
MAC	Medicare Administrative Contractors
MCS	Multiple Console Support
MSCA	Master Security Control ACID
MUSASS	Multi-User Single Address Space System
MVS	Multi-Processing Virtual Storage or Multiple Virtual System
NCP	Network Control Program
OIG	Office of the Inspector General
O/S	Operating System

PADS	Program Access to Data Sets
PPGM	Protected Program List
PPT	Program Properties Tables
PROC	JCL procedure
RACF	Resource Access Control Facility
SAF	System Authorization Facility
SCA	Security Control ACID
SDLC	Synchronous Data Link Control
SDSF	System Display and Search Facility
SID	SMF System ID
SMF	System Management Facilities
SNA	System Network Architecture
SPECLU	Specified Logical Unit
SSL	Secure Sockets Layer
STC	Started Task Control
STIG	Security Technical Implementation Guide
SVC	Supervisor Calls
TLS	Transport Layer Security
TSO	Time Sharing Option
TSS	TOP SECRET
USS	Unformatted System Services
VCA	Divisional Control ACID
VTAM	Virtual Telecommunication Access Method
ZCA	Zone Control ACID

References

- IBM International Technical Support Information. (May, 1996). *Planning for a CA-ACF2 Migration to OS/390 Security Sever (RACF)* Redbook.
- OS/390-Z/OS Security. (2004). *Audit and Control Features*. Peter Thingsted
- IBM Poughkeepsie Services Center. (September, 1999). *Security Server (RACF) Introduction.*
- IBM International Technical Support Information. (October, 2002). *Communications Server for z/OS V1R2 TCP/IP Implementation Guide Volume 2: UNIX Applications* Redbook.
- The Henderson Group. (February, 2006). *How to Audit MVS, RACF, ACF2, CICS, and DB2 Security.*
- IBM. (April 2006). *Introduction to New Mainframe: Networking*. Mike Ebbers, Wayne O'Brien, Bill Ogden.
- IBM (July 2006). *Introduction to New Mainframe: z/OS Basics.* Mike Ebbers, Chris Hastings.
- http://www.sdsusa.com/dictionary/
- http://www-03.ibm.com/systems/z/
- http://publib.boulder.ibm.com/infocenter/zoslnctr/v1r7/index.jsp

(This Page Intentionally Blank)