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 Top Secret Whitepaper

FINAL
Version 2.0
March 08, 2009

(This Page Intentionally Blank)

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS TOP* SECRET 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.,
   b) Table 2 in Section 3.2.1.1,
   c) Table 3 in Section 3.2.1.2,
   d) Table 4 in Section 3.2.2,
   e) Table 5 in Section 3.3.2,
   f) Table 6 and 7 in Section 3.3.6, and
   g) Table 8 and 9 in Section 3.4.1.
5) Removed former Appendix A CSRs and added pointer to new CMSRs.
6) Changed CSR glossary term in Appendix B to CMSR.
7) Updated Table 1 and Appendix A CMSR reference.

SUMMARY OF CHANGES IN *MAINFRAME OS/390 AND Z/OS TOP* SECRET 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 TSS 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 TSS, or Top Secret Security, from Computer Associates (CA).

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 TSS. 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 TSS 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 TSS, 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 TSS 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.

3.1 TSS BACKGROUND INFORMATION

eTrust CA Top Secret (TSS) is one of the three ACPs. Individual security records in TSS are identified by their Accessor ID, or ACID. An ACID can be up to eight alphanumeric characters long, and for individual users normally corresponds with the user's system userid. Administrators have the option of granting users one ACID for all facilities or a different ACID for each facility, for example, Time Sharing Option (TSO), Customer Information Control System (CICS), etc.

TSS provides an identification of userids through ACIDs. There are several different types of ACIDs, ranging from a user to an entire zone, to comprise a hierarchical structure. Each of these ACID types is then associated with a set of resource access authorizations. Following are examples of ACID types:

Table 1 ACID Types

ACID Type	Explanation
User ACIDs	Accessor ID - This is similar to a "User-ID". It is used to logon to the system. Security rules can be written at the level of a User ACID.
Department ACIDs	Used to identify the logical location of a person; for example, Accounting Department. Each User ACID belongs to one Department ACID. Inclusion within a particular department does not imply any system authorities.
Division ACIDs	Used to identify the location of a particular department. Each Department ACID belongs to one Division ACID. Users are associated to divisions only indirectly, as members of a department within that division. Inclusion within a particular division does not imply any system authorities.
Profile ACIDs	Used to logically place people into groups with identical security requirements. Security rules are normally written at this level, with many people associated with a particular profile.
Zone ACIDs	A Zone ACID is another optional organizational level in the hierarchical structure. A zone can be used to group two or more divisions. Every Zone is assigned a unique Zone ACID and resources can be assigned to a zone as well (as with Users, Profiles, Departments, and Divisions).
Control ACIDs	Control ACIDs are used for administrative purposes and are usually associated with security administrators. Examples of control ACIDs are: MSCA, SCA and LSCA.

Two categories of ACIDs are created in TSS: functional and organizational. Functional ACIDs refer to User, Profile, Group, and Control ACIDs, and are used to perform specific tasks. Organizational ACIDs are Department, Division, and Zone ACIDs, and are used to construct the upper levels of the security hierarchy.

3.1 TSS SYSTEM CONFIGURATION

3.1.1 SYSTEM CONFIGURATION STANDARDS

TSS offers many options with a variety of settings which can have a dramatic affect on the level of control that the ACP can provide. One such means of defining system options within TSS is by way of the Top Secret Control Options. These options are used to set system-wide options to protect resources.

3.1.1.1 CONTROL OPTIONS SETTINGS

Control Options changes can be issued from TSO using the TSS MODIFY command, the PARM field of a started-task procedure, or the TSS parameter file. Security administrators can use control options to perform several useful activities such as:

- Reset the security MODE. FAIL is the delivered default.
- Determine how eTrust CA-Top Secret will process normally and how it will process under specific security MODES and circumstances.
- Indicate what features, facilities, or products are on the operating system, and how individual facilities are handled by eTrust CA-Top Secret.
- Specify password selection rules and violation thresholds.
- Issue commands that force eTrust CA-Top Secret to reset after shutdown or reinitialize after installation of new eTrust CA-Top Secret maintenance.

The DISA STIG recommends the following TSS Control Options records as specified below which will ensure the appropriate oversight and control of TSS Control Options records. For additional information for each “policy bullet” including the short description identifier and the severity codes refer to the DISA STIG. Functions assigned to the Information Assurance Officer (IAO) should be performed by an individual with appropriate authority and knowledge.

Table 2 Recommended Control Options Settings

Option	Description	Required Value
ADMINBY	Enables administration information to be recorded for security changes.	ADMINBY The IAO will ensure ADMINBY control option is set to Adminby to record who when and where information in the ACID security record for administrative changes.

Option	Description	Required Value
ADSP	Controls global automatic data set protection.	ALL (default) (Pre-always call) YES (MVS, Version 1.x NO (MVS, Version 2.x and above) Note: Setting is also dependent on the type(s) of catalogs in use on the system. The IAO will ensure ADSP control option is set to (NO) indication that the RACF bit in the DSCB will is not set.
AUTH	Controls authorization checking.	OVERRIDE, ALLOVER The IAO will ensure AUTH control option is set to (OVERIDE, ALLOVER) TSS merges the user, profile, and all records for its access authorization search.
AUTOERASE	Controls auto-erase feature necessary to meet NCSC requirements.	Unclassified Systems: Optional Classified Systems: YES CAUTION: Usage will affect perfor. The IAO will ensure AUTOERASE control option is set to (YES) for Classified systems and is at the sites discretion for Unclassified systems to erase all residual information on DASD.
BACKUP	Controls automatic Security File backup.	Site defined Note: a time must be specified unless the database is shared and backed up on another system. The IAO will ensure the BACKUP control option specifies a time and BACKUP(OFF) is not specified unless the database is shared and backed up on another system.
BYPASS	Specifies jobs and started tasks that bypass security in an emergency.	As applies to a specific System Note: Local changes will be justified in writing with supporting documentation.
CANCEL	Allows TOP SECRET to be canceled via the operating system CANCEL command.	The CANCEL option will not be specified. Note: To maintain the integrity of the TOPSECRET environment, the MVS FORCE command will also not be used to terminate the TSS started task. The IAO will ensure CANCEL control option is not set to CANCEL. Security administrators do not have the ability to do an O/S CANCEL command to terminate the TSS address space.
CPFRCVUND	Identifies whether or not the local node can receive commands transmitted from remote nodes that have not been defined to the CPFNODES list.	NO The IAO will ensure CPFRCVUND control option is set to (NO). The CPFRCVUND Control Option indicates whether or not the local node can receive commands propagated from nodes which are not defined to the CPFNODES list.
DATE	Sets date display format.	MM/DD/YY The IAO will ensure the DATE control option is set to MM/DD/YY. The DATE Control Option specifies the format for dates displayed in listing.

Option	Description	Required Value
DEBUG	Controls debugging feature. Use as directed by CA support.	OFF The IAO will ensure DEBUG control option is set to (NO). The DEBUG Control Option controls the production of debugging dumps used to determine the cause of abnormal error conditions. Use as directed by CA Support.
DIAGTRAP	Controls diagnostic traps. Use as directed by CA support.	OFF (Ver 5.1 and below) ALL,DEL (Ver 5.2 and above) The IAO will ensure DIAGTRAP control option is set to (Off) for TSS ver 5.1 and earlier or it is set to (ALL,DEL) for TSS ver 5.2 or greater. DIAGTRAP creates a diagnostic dump. Use as directed by CA Support.
DL1B	Controls protection of DBD and PSB for DL/1 batch programs.	NO The IAO will ensure DL1B control option is set to (NO). The DL1B Control Option is used to implement PSB and DBD security for IMS batch regions, and to provide access to the TSS application interface program.
DOWN	Controls action taken when TSS address space is inactive.	SB, BW, OW, and either: TW (if users are still defined in SYS1.UADS) - or - TN (if only systems personnel remain defined in SYS1.UADS) The IAO will ensure that DOWN control option is set to(BW,SB,OW) and TW if users are still defined in SYS1.UADS, TN if only systems personnel are defined in SYS1.UADS.
DRC	Modifies or lists particular DRC attributes.	As applies to a specific system
DUFPGM	Identifies programs allowing for extraction or upgrade of INSTDATA.	As applies to a specific system
DUMP	Takes formatted dumps of TSS address space.	As applies to a specific system
EXIT	Installation user exit.	ON Note: The Post-Initiation exit point is supplied by IAO Mechanicsburg to support the control of privileged users by NC-PASS. Refer to Section 6.3.3, NC-PASS for TOP SECRET, for further information. Note: For non DISA sites this is site defined. Note: A review by DISA FSO is required for each exit point activated. The IAO will ensure that EXIT control option is set to (ON) for DISA sites. Note: The Post-Initiation exit point is supplied by SSO Mechanicsburg to support the control of privileged users by NC-PASS. Refer to Section 6.3.3, NC-PASS for TOP SECRET, for further information. For non DISA sites this value is site defined.

Option	Description	Required Value
FACILITY	Controls facility processing.	As applies to a specific system. All defined FACILITIES will specify MODE=FAIL. The IAO will ensure FACILITY control option specify the sub option of MODE=FAIL. The MODE sub option specifies the security mode for the FACILITY.
HPBPW	Days to honor previous batch password.	1-3 days The IAO will ensure HPBPW control option is set to 3 days maximum. HPBPW Control Option selects the maximum number of days that TSS honors an expired or previous password for batch jobs.
INACTIVE	Controls users who have been inactive for a specific period.	35 days maximum The IAO will ensure INACTIVE control option is set to 35 days maximum. The INACTIVE Control Option selects the number of days before TSS denies an unused ACID access to the system after the ACIDs password has expired.
IOTRACE	Controls TSS I/O trace.	OFF The IAO will ensure IOTRACE control option is set to (OFF)). The IOTRACE Control Option controls a diagnostic trace for use by technical support. The trace is produced on the TRACE/LOG data set.
INSTDATA	Alters global installation data field.	0 The IAO will ensure INSTDATA control option is set to 0. The INSTDATA Control Option controls the value of the 4-byte global data installation data area. This value is passed to the security exit developed at a particular site.
JCT	Identifies JES2 JCT offsets.	As applies to a specific System
JES	Identifies JES2/JES3 subsystems.	NOVERIFY The IAO will ensure JES control option is set to (NOVERIFY)). The JES Control Option indicates whether or not support for the JES Early Verify feature is desired.
JOBACID	Controls ACID identification for batch jobs.	Site defined Note: To be defined by the IAO.
LOG	Controls incident recording for all facilities.	MSG, SEC9, INIT, SMF The IAO will ensure LOG control option is set to (MSG, SEC9, INIT, SMF). The LOG Control Option identifies the types of events that TSS logs, and specifies whether the events are logged onto the audit tracking file and into the SMF files.
LOGBUF	Allows the maximum number of in-core logging buffers to be used.	32 The IAO will ensure LOGBUF control option is set to 32. The LOGBUF Control Option allows the maximum number of in-core logging buffers used by TSS.

Option	Description	Required Value
MODE	Controls processing mode for all facilities.	FAIL The IAO will ensure that MODE control option is set to (FAIL). The MODE Control Option selects the security mode in which TSS operates for all facilities.
MSG	Alters characteristics of TSS violation messages.	As applies to a specific system Note: Local changes will be justified in writing with supporting documentation.
MSUSPEND	Allows Master Security Control ACID (MSCA) to be suspended if password violation occurs.	YES The IAO will ensure that MSUSPEND control option is set to (YES). The MSUSPEND Control Option allows the MSCA ACID to be suspended automatically if the password violation threshold is set via the PTHRESH option and that limit is exceeded.
NEWPW	Selects new password specification rules.	MIN=8, WARN=10, MINDAYS=1, NR=0, ID, TS, SW, RS FA, FN for (Ver 5.3 and above) The IAO will ensure that NEWPW control option is set to (MIN=8, WARN=10, MINDAYS=1, NR=0, ID, TS, SW, RS) for 5.2 and below (FA, FN) is appended for Ver 5.3 and above. The NEWPW Control Option specifies the rules that TSS l applies when a user selects a new password.
NJEUSR	Defines a default ACID for NJE Store-and-Forward nodes. Has no significance on a job's execution node.	NJEUSER(NJESTORE) The IAO will ensure that NJEUSER control option is set to (NJESTORE). The NJEUSER Control Option is used to define a default ACID used for NJE store and forward nodes where no other ACID are identified.
NPWRTHRESH	Sets maximum threshold, from 0 to 99, for new passwords to be verified before the complete logon sequence needs restarting.	2 The IAO will ensure that NPWRTHRESH control option is set to 2. The NPWRTHRESH Control Option sets the threshold value for the number of attempts allowed for new password verification before complete logon sequence needs restarting.
OPTIONS	This parameter replaces optional APARs that have been applied prior to Release 5.1.	4, 33, 34 (Ver 5.2) 4 (Ver 5.3 and above) Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure that OPTIONS control option is set in accordance to the STIG, additional OPTIONS entries are justified in writing with supporting documentation.

Option	Description	Required Value
PRODUCTS	Specifies special products installed.	TSO/E As applicable to the individual sites Note: Local changes will be justified in writing with supporting documentation. The IAO will ensure PRODUCTS control option is set to (TSO/E). The site can list any other products at their own discretion. The PRODUCTS Control Option allows the site to list special products that are installed on the system.
PTHRESH	Specifies password violation threshold.	2 The IAO will ensure the PTHRESH control option is set to 2. The PTHRESH Control Option selects a maximum password violation threshold.
PWEXP	Specifies password expiration interval.	90 The IAO will ensure the PWEXP control option is set to 90. The PWEXP Control Option allows the site to specify a password expiration interval.
PWHIST	Specifies number of previous passwords to be maintained in history file.	10 The IAO will ensure the PWHIST control option is set to 10. The PWHIST Control Option specifies the number of previous passwords maintained as part of an ACIDs password history file.
PWVIEW	Controls display of passwords by administrators.	NO The IAO will ensure the PWVIEW control option is set to (NO). The PWVIEW Control Option allows the site to suppress the viewing of a users password.
RECOVER	Controls change recovery. Note: Requires the RECFILE DD statement in the TSS STC.	ON The IAO will ensure the RECOVER control option is set to (ON). The RECOVER Control Option indicates whether TSS records changes made to the security database onto the recovery file.
SECTRACE	Controls security diagnostic trace.	OFF Note: May be activated on an as-needed basis, only for diagnostic purposes. The IAO will ensure that SECTRACE control option is set to (OFF). The SECTRACE Control Option activates a diagnostic security trace on the activities of all defined users.
SUBACID	Controls on-line job submission.	U, 8 The IAO will ensure that SUBACID control option is set to (U,8). The SUBACID Control Option indicates how TSS derives an ACID for batch jobs that are submitted through an online terminal, from another batch job, or from a started task.
SWAP	Controls TSS address space swapping.	NO The IAO will ensure that SWAP control option is set to (NO). The SWAP Control Option controls the swapping of the TSS address space by the OS/390 operating system.

Option	Description	Required Value
SYSOUT	Spins off TSS activity log; specifies class and destination.	x, LOCAL Class as specified in the Computing Services's Naming Convention Recommendations. Class specified is at the sites discretion.
TAPE	Controls tape processing. Note: OFF indicates that an External Tape Management System (ETMS) is in use.	OFF The IAO will ensure that TAPE control option is set to (OFF). The TAPE Control Option specifies the type of tape protection in effect at the installation.
TEMPDS	Controls temporary data set protection.	YES (TSS0640: CAT II) The IAO will ensure that TEMPDS control option is set to (YES). The TEMPDS Control Option allows an installation to determine whether or not temporary data sets are protected.
TIMER	Interval at which data is written from TSS buffers to AUDIT/TRACKING file.	30 The IAO will ensure that TIMER control option is set to 30. The TIMER Control Option controls the interval at which data is written from TSS buffers to the audit tracking file.
VTHRESH	Selects violation threshold and action.	10, NOT, CAN The IAO will ensure the VTHRESH control option is set to (10, NOT, CAN). The VTHRESH Control Option selects an access violation threshold for users, batch jobs and started tasks, and selects the action that TSS takes when the threshold is reached.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.1 Standard Global Options (Control Options); Table A - REQUIRED GLOBAL OPTIONS (CONTROL OPTIONS).

3.1.1.1 FAIL MODE

The MODE control option selects the security mode in which TSS operates for all facilities. An improperly set MODE options could cause TSS rules to be ignored when determining if users are able to access system resources. There are four TSS MODE(s) which include:

Table 3 MODE Control Options

Mode	Description
DORMANT	eTrust CA-Top Secret will not perform security validation for normal users (everyone except security administrators). Normal users will enter their current signon and password, not an eTrust CA-Top Secret password. eTrust CA-Top Secret will always perform password validation for Security Control ACIDS (security administrators). Security administrators who sign on with their security control ACID, is prompted for their eTrust CA-Top Secret password. eTrust CA-Top Secret will also always perform password validation for those users whose UADS data fields are being managed by eTrust CA-Top Secret. Exceptions can be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.

Mode	Description
WARN	eTrust CA-Top Secret will perform security validations for all access attempts. Users who are guilty of security violations will receive a message indicating that they have violated security, but is not denied access to the resource unless exceptions have been specified. All specified LOG options are in effect. Exceptions can be specified via the DRC control option, or via the TSS PERMIT ACTION(FAIL) command.
IMPL	This mode is referred to as a gradual implementation mode since it will fully protect defined resources, and monitor all access requests made by defined users. Defined resources are protected and violations result in denied access. This mode will, however, allow undefined users uninhibited access to undefined resources. Thus, security can be gradually applied to selected users and resources with little or no impact.
FAIL	eTrust CA-Top Secret will deny all unauthorized facility or resource access unconditionally. All users must be defined.

Fail MODE is the only acceptable DISA setting. While running in this MODE any access attempts not specified by the system will not be allowed and will be logged.

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 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, Volume 1, Section 3.1.3.1 Password Guidelines.

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

Most of the passwords requirements can be enforced by TSS, however, as noted within the DISA STIG, the below list cannot.

Table 4 Password Requirements Not Enforced by TSS

Password Requirements not enforced by Top Secret
No words found in standard dictionaries will be used.
At least one alphabetic, numeric, and special character will be used.
Each character of the password will be unique.
Passwords will contain no consecutive characters (e.g., 12, AB).
Will not contain the user's name, userid (ACID), or telephone number.

Where password standards cannot be enforced by Top Secret the STIG recommends use of EXITS. If this method is used, the following EXIT entry point should be used to implement these controls:

- TSSINSTX Entry Point: PASSWORD

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.3.2 Password Exit Processing.

3.1.2 TSO PARAMETERS

TSS intercepts some OS/390 components and essentially gains control to decide if the request should be processed in one of three ways; allow, allow but log to SMF, and deny and log to SMF. TSS will make this choice based on the total environment and rules that specify access under certain conditions. Total environment considers components such as the user who made the request, the data set name, the program making the request, etc. Time Sharing Option (TSO) is one such component; TSO allows users to establish a session where they can issue commands.

To sign on to TSO, a user's ACID must be authorized to access the TSO facility. The TSO facility controls access to TSO. The DISA STIG notes to authorize each user type ACID requiring access to TSO with the appropriate ADD command.

- TSS ADD(acid) FACILITY(TSO)

All TSO attributes are taken from TSS, versus the IBM supplied default of SYS1.UADS. The DISA STIG recommends the following in regards to TSO controls:

1) As users are granted the facility of TSO, the organization will specify a default logon procedure (TSOLPROC) and a default account code (TSOLACCT) for each user. The specifications for these fields ensure that only TSS is analyzed for TSO profile options.

2) Authorize access to account codes, if applicable, via the TSOACCT resource class with specific authorizations to use an account code being granted.

3) Access to a TSO procedure name is controlled via the TSOPROC resource class. Most users should only be capable of executing one standard logon procedure. Limit the ability to specify an alternate logon procedure to those users who have a justified need.

TSO initially runs as an APF-authorized program, which is turned off prior to invoking external commands and programs. However, TSO provides a way to allow APF-authorized programs to be executed in a TSO user's address space. The process is controlled by the presence of the program name in one of two MVS load modules; SYS1.LINKLIB(IKJEFTE2) (for callable programs) and SYS1.LINKLIB(IKJEFTE8) (for TSO commands). The programs which are authorized are found in SYS1.PARMLIB(IKJTSOxx) and in load modules IKJTABLS and IKJEFTAP, which are located in SYS1.LPALIB.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 2.1.2.2 TSO APF Authorization.

The DISA STIG stresses control over a TSO command processor called PARMLIB. This command gives a user the ability to display and dynamically change 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 execute as an authorized program within their address space. This could possibly give the program supervisor state, e.g. excessive privileges. The user would have access to the TSS PARMLIB resource of the TSS TSOAUTH resource class. This essentially bypasses security and gives a user privileges reserved to the OS.

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.

1) Only systems programmers responsible for supporting TSO/E should be authorized to access the PARMLIB command. The IAO is assigned ownership of the PARMLIB entity.

2) The following steps provide examples of TSS commands necessary to control the PARMLIB command:

   a) Assign ownership of the PARMLIB entity:

      TSS ADD(acid) TSOAUTH(PARMLIB)

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

      TSS PERMIT(acid) TSOAUTH(PARMLIB) ACCESS(READ)

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

      TSS PERMIT(acid) TSOAUTH(PARMLIB) ACCESS(UPDATE)

Users who have been given access to TSO are permitted to all TSO commands by default. TSS provides a utility that allows security administrators to monitor security-related events for one or more systems in a real-time manner. This utility can be executed under TSO and is called TSSTRACK. For additional information on TSSTRACK, see the TSS Report and Tracking Guide.

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 access to TSO logon procedures is controlled and that access to multiple logon procedures are limited to authorized personnel.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 7.2.3 TOP SECRET.

3.2 USER MANAGEMENT

3.2.1 USER CONTROLS

TSS provides many venues for controlling user access. The security product must be used to answer the question, who is this user and what do they have access to. TSS is used to determine if a user is allowed access to a resource or data set so it must be able to associate a user with each resource or data set they wish to access. Within TSS all users are identified by an accessor id, referred to as ACID. TSS users, batch jobs, and started tasks will all have an ACID. ACIDs contain records which store information on the user which allows TSS to make decisions regarding what resources the user can access and what data they can read or update. Because

each logonid is associated with certain privileges it is imperative that individuals have unique ids.

Without unique ACIDs users will be assigned access which may not enforce the concept of least privilege. 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 recommends the following in regards to ACID controls; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Every user will be identified to TSS via a TYPE=USER Accessor ID (ACID) record. To TSS, a TYPE=USER ACID definition is used to identify an individual, a started task, or a batch job. Every user type ACID will be fully identified within TSS with the following completed fields:

   NAME User's name

2) IAOs will ensure that the values for these fields are maintained and current. They will update these fields as needed to reflect such changes as personnel actions, office relations, etc.

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 TYPE=USER ACID is uniquely identified to the system. Within the ACID record, the users NAME field is completed.
- The IAO will ensure that every user is uniquely identified to the system. Userids are not shared among multiple users.

3.2.1 INTERACTIVE USERS AND PARAMETERS

As discussed above an ACID is made up of records which contain fields. Many fields are reserved for use by TSS and contain specific values for settings defined within TSS for each user. Default values are specified for all users when they are added to the system. These default settings can give a user privileges which would allow them to bypass security controls in place within TSS.

Since ACIDs can override the global settings the default values must be appropriately controlled when a user is created within TSS.

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

1) Three facilities in particular are especially sensitive, batch processing, TSO, and similar online systems. Only grant access to these facilities if needed.

2) Shared profile ACIDs can be created to allow resources to be shared between multiple interactive users. All departments shall, at a minimum, have one shared profile to define the basic access authorizations for their personnel, and all departmental personnel should be assigned that profile at a minimum. Additional shared profiles should be defined as needed to grant access to other departmental resources (such as departmental shared files and CICS regions) to selected groups of users. As new requirements for resources develop, the resources should be added to existing shared profiles whenever possible. The use of shared profiles will ensure the granting of consistent privileges to new system users.

3) New shared profiles should be created only when the access requirements do not fit into the existing structure of shared profiles.

4) The following table provides values that will be specified for certain selected fields as user privileges and access are granted:

Table 5 ACID Field Settings

Field	Description	Required Value
FAC	Facilities the user is validated to use.	BATCH - For batch users TSO - For TSO users NC-PASS - For highly privileged users controlled by NC-PASS. Refer to Section 6.3.3, NC-PASS for TOP SECRET, for further information. Other: As necessary
NAME(username)	Specifies the 1–32-character name of the user.	Will be completed for all users
PASSWORD	The logon password for the user.	Will be completed for all users
INSTDATA	Installation-defined data.	Optional
PROF	Profile(s) defining the user's attributes.	Will be completed for all users
TSOACCT	Specifies the user's TSO logon account. Used for all billing.	May be required for Fee-for-Service support
TSOLACCT	Specifies the user's default TSO logon account. Used for all billing.	May be required for Fee-for-Service support
TSOAUTH	Used to secure TSO user attributes.	Will be completed for all TSO users
TSOLPROC	Specifies the user's default TSO logon procedure.	Will be completed for all TSO users
TSOPROC	Specifies the user's TSO logon procedure.	Will be completed for all TSO users

Note: All highly privileged users controlled by NC-PASS will be granted access to the SECURID ABStract. Refer to Section 6.3.3, NC-PASS for TOP SECRET, for further information.

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 all interactive ACIDS have the fields specified in the above table completed.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.2.1 Interactive Users.

3.2.1 STC (STARTED TASK CONTROL) USERS

Started tasks are procedures started from the operating system console with the MVS START command. It is possible to assign a TSS ACID 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 TSS. 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 that both started tasks and non-started tasks 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 TSS 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 STC ACIDs will have the STC facility. An STC also may be granted the FAC(BATCH) if it requires the capability to submit batch jobs to the internal reader. It should be noted, however, that this also will allow the STC itself to be executed as a batch job.

2) Each STC ACID will be defined with a password following the requirements as specified in Section 3.1.3.1, Password Guidelines. The only exception is that these passwords will be defined as non-expiring. In addition, each STC will have its own unique password. Defining a password for started tasks prevents a user from logging onto a system with the STC ACID.

3) Ensure the OPTIONS control option specifies a value of 4 to disable password checking for STCs. Otherwise operators will be forced to supply a password when STCs are started. Refer to Section 3.4.1, Standard Global Options (Control Options) for further details.

4) All STC ACIDs will be sourced to the internal reader. This control will further protect the unauthorized use of STC ACIDs.

    ADD(stc-acid) SOURCE(INTRDR)

5) Every STC will be defined to the STC table, associated with a specific procedure, and granted minimum access.

6) All STCs not defined to TSS will fail upon initiation. The following command may be used to associate all undefined STCs with a default action of FAIL:

   TSS ADD(STC) PROCNAME(DEFAULT) ACID(FAIL)

7) 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 requirement is to grant the BYPASS privilege or NO***CHK attributes to these STCs.

8) Started task user ACIDs do not require an associated profile ACID, and may be directly granted privileges as necessary.

9) STCs should be granted the NOSUSPEND privilege to exempt an STC's associated ACID from suspension for excessive violations. However, an STC will be canceled for excessive violations.

10) If a valid requirement exists to establish a default STC, the following restrictions also apply:

- The IAO will maintain the written request, justification, and authorization.
- The STC will have no other facilities permitted to it.
- It will have DSN(*****) ACCESS(NONE).
- The STC's ACID will be sourced to the internal reader:

  ADD(stc-acid) SOURCE(INTRDR)

- An entry will be made in the STC table identifying the default ACID name as follows:

  TSS ADD(STC) PROCNAME(DEFAULT) ACID(default name)

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 the default STC ACID is set with a default action of (FAIL).
- The IAO will ensure that only trusted STCs are granted the BYPASS privilege.
- The IAO will ensure that all STC ACIDS assigned a unique USER ACID, have a corresponding USER ACID defined with the STC FACILITY specified, and have a password generated in accordance with DAA defined requirements, and are sourced to the OS/390 internal reader. All ACIDS with STC FACILITY specified have a corresponding entry defined in the STC RECORD.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.2.3 STC Users.

3.2.2 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; 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, Volume 1, and Section 3.1.2.6 Emergency Userids.

3.2.3 EMERGENCY PRIVILEGED ACCESS IN TSS

As discussed above the STIG recommends use of two emergency ids, on located in SYS1.UADS in the case that the ACP is not functional and one in the ACP.

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) The system emergency administration ACID (an SCA) is to be stored in the safe as the userid capable of performing ACP administration.

2) The ACID to be used in emergencies for systems programming to resolve problems will be set up with the following attribute:

   NAME

3) This userid is granted access to the TSO and BATCH facilities. All permissions under the TSO AUTH resource class will be permitted. To allow all data to be accessed by this userid, grant the following permission:

   TSS PER(acid) DSN(*****) ACC(ALL) ACTION(AUDIT)

4) This will be used in lieu of the NODSNCHK option since auditing of data access can then be performed.

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 all access to emergency ACIDs are limited to resources required to support the specific functions of the owning department and access to these resources are audited.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.2.6 Emergency Userids.

3.2.4 PRIVILEGED ACCESS USERS

Every ACP provides user attributes (types of privileges) that can allow a user to modify the security environments, perform auditing tasks, and circumvent security. These attributes within TSS are defined within the ACID record.

Within TSS these attributes must be controlled because of the privileges that they allow; privileges that could override security controls in place. These attributes include the following:

Table 6 Privileged User Attributes

Attribute	Definition
MODE	This provides the ACID, either user or profile, with its own mode which overrides the system and facility modes.
NODSNCHK	This allows the user to bypass all security checking for data sets. Auditing is not disabled if the ACID being used or data set being accessed is subject to auditing.
NOVOLCHK	This allows the user to bypass all security checking for volumes, with no auditing.

Attribute	Definition
NOSUBCHK	This allows the user to submit jobs using an ACID other than his/her own, whether or not he/she has been permitted to use the ACID. Thus, with this attribute, the user can submit a job under any ACID's authority, which gives that user all the authority of the specified ACID under which the job was submitted.
NOPWCHG	The user is not required to periodically change the password.
NORESCHK	Allows the ACID to bypass all security checking for all resources except data sets and volumes.
CONSOLE	This attribute allows the user to change CA-Top Secret control options through the OS/390 operating system MODIFY command from the OS/390 console.

The DISA STIG recommends the following 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.

   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.

2) 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.

3) 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.

4) 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.

5) 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.

6) 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.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, 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 ACF2; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

1) Limit the number of administrative (control) ACIDs to the minimum number necessary. The system MSCA will be a limited use ACID, which is not available to any individual for day to day processing. Limit its use only to performing security administration functions. An SCA will assume the use of, and the responsibility for, the MSCA by changing the MSCA password. The password change command will include a comment indicating the reason. The SCA will remain responsible for the MSCA until the next change/assumption of responsibility.

2) The TSS CONSOLE privilege allows a user to change TSS control options. It will be limited only to authorized security administrators.

3) Assign the NOATS parameter to all security administration userids.

4) Limit the assignment of the MISC9 (ALL) or MISC9 (CONSOLE) authorities to IAOs authorized to assign the CONSOLE attribute.

5) The AUDIT attribute should not be turned ON for all users who have the CONSOLE attribute. Only perform auditing activities as necessary when a user is suspected of some wrongdoing.

6) Use the TRACE attribute only for trouble shooting purposes.

7) The ability to execute privileged programs will be strictly controlled and only permitted to a minimum number of users.

8) TSS provides a number of NOxxxCHKs (bypass attributes) that permit capabilities by bypassing authorization checking. Use of these NOxxxCHKs will be tightly controlled and their access only granted to those required user ACIDs. Avoid NOxxxCHKs unless a special requirement necessitates their use. The IAO will document all uses of NOxxxCHKs. Documentation will be maintained explaining and justifying any bypass attributes that are granted.

9) Blanket access to all facilities, FACILITY(ALL), will never be granted.

10) The NOSUSPEND privilege may be granted to STC ACIDs as discussed in Section 3.4.2.3, Started Task Control (STC) Users. It will not be granted to any other type of ACID.

11) The MODE resource is used to specify the operating MODE of a user or profile ACID. The use of this resource will override the MODEs specified in the Global and the FACILITY

Control Options and provide the user with unrestricted access. All MODE resources will be owned by the MSCA. Access to the MODE resources will be controlled and access removed in a timely manner when the users access requirement have been resolved. At the IAOs discretion a profile may have access and ACIDs added and removed when the users access requirement have been resolved. This profile can have controls in place that can restrict access to sensitive resources.

TSS PERMIT(profile) DSN(SYS1.LINKLIB) ACCESS(FETCH) ACTION(FAIL)

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 the TSS Console privilege is limited to only authorized security administrators
- The IAO will ensure that only a limited number of ACIDS authorized to assign the CONSOLE attribute are allowed MISC9 (ALL) or MISC9 (CONSOLE) authority.
- The IAO will ensure that all security administrators userids have the NOATS parameter specified.
- The IAO will ensure that only a limited number of ACIDS authorized to assign the CONSOLE attribute are allowed to specify the AUDIT attribute and is only used when a user is suspected of wrong doing.
- The IAO will ensure that the trace attribute is only used for trouble shooting purposes.
- The IAO will ensure that the use of NOxxxCHKs is avoided unless a special requirement necessitates their use and the IAO documents all uses of NOxxxCHKs.
- The IAO will ensure that blanket access to all facilities; FACILITY(ALL), is never granted.
- The IAO will ensure that the MODE resources is owned by the MSCA. Access is restricted and a letter justifying access is filed.

In addition to these special attributes, TSS utilizes a hierarchy of administrator ACIDs to grant access and make other modifications within the security package. Access through these ACIDs should be limited to proper personnel and closely monitored.

Table 7 Administrator ACID Hierarchy

Admin ID	Description
MSCA	Master Security Control ACID. It has complete administrative authority and control. There is only one MSCA and it is created as part of the installation procedure. Like other Central Security Administrators, an MSCA has unlimited scope; however, only an MSCA has implicit unlimited administrative authority. The MSCA's ACID cannot be deleted, although it can be renamed. The MSCA can log on or initiate with only password checking in force; no expiration, facility, source, or terminal checking is performed by CA-Top Secret. These types of security checking, in addition to password checking, can be performed on all other Control ACIDs.
SCA	Central Security Control ACID. It has unlimited scope; however, administrative authority for this ACID must be provided explicitly. Therefore, an SCA is usually defined to do almost everything except for some specific functions that a MSCA can do (e.g. define another SCA or change administrative authorities of an existing SCA).
LSCA	Limit Central Security Control ACID. It is an SCA whose scope of authority has been limited. Its scope is determined by the MSCA through the ADMIN SCOPE keyword. That scope can include Zones and even other LSCAs. SCOPE authority does not apply to any other Control ACID and cannot be defined by any Control ACID other than the MSCA.
ZCA	Zone Control ACID. Zone administrators can only be defined by a SCA. Each ZCA is associated with a particular zone, and can perform administrative tasks for the divisions, departments, users, and profiles linked to this zone.
VCA	Divisional Control ACID. Divisional administrators can only be defined by a SCA or a ZCA. Each VCA is associated with a particular division, and can perform administrative tasks for the departments, users, and profiles linked to this division.
DCA	Departmental Control ACID. Departmental administrators can be defined by a SCA, a ZCA, or a VCA, for a department that is linked to that VCA's division. The responsibilities that can be performed by a DCA include administrative tasks for the users and profiles that belong to this department.

The DISA STIG recommends the following 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.

- The IAO defines SCAs and uses them for the day to day administrative functions of TSS. Further delegation of responsibilities by the IAO may be accomplished using the other security control authorizations (LSCA, ZCA, VCA, and DCA).
- The number of administrative (control) ACIDs (SCAs, LSCAs, VCAs, ZCAs, and DCAs) granted audit privileges will be limited to the minimum number necessary and only to authorized users. ACIDs established to perform only audit functions will be restricted to those functions.

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 the system MSCA ACID is a limited use ACID, which is not available to any individual for day to day processing it is only used to perform security administration functions.
- The IAO will ensure that the system MSCA ACID password changes are documented in the change log and filed with the IAO.
- The IAO will ensure that the number of control ACIDS are limited to as few as possible at a site.
- The IAO will ensure that control ACIDS are granted a limited amount of administrative authorities as possible.

Tape label bypass privileges allow a user to access data on a tape, using bypass label processing (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.

Another powerful form of access is MOUNT authorization, which is found within the TSOAUTH resource class.

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

1) The tape label bypass privilege is restricted and will only be granted to authorized data center personnel at the user level. Use the following parameter to specify BLP authority:

   TSS PERMIT(user-acid) VOL(xxxxxx) ACCESS(BLP,READ)

2) The TSOAUTH resource class will authorize the resource name of MOUNT. Do not grant the Device Mount privilege to on line TSO users. It may be granted to STC ACIDs who execute TSO in batch on an as needed basis.

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 the TAPE BYPASS LABEL PROCESSING (BLP) privilege is limited to only a few and is documented with the IAO.
- The IAO will ensure that the MOUNT resource is assigned only on an as needed basis for userids associated with STCs and LOGONIDS that need to execute TSO in batch.
- The IAO will strictly control and limit access to TSOAUTH resources. 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 3.4.4 Special Privilege Access, 3.4.4.1 Access Control Product Modification Privileges, 3.4.4.2 Audit Privileges, 3.4.4.3 Tape Label Bypass Privileges, 3.4.4.4 Other Sensitive 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 OS. 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 ACF2, RACF, and TSS 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.

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

Table 8 Sensitive Utility Types

Sensitive Utility Controls	
UTILITY TYPE	LEGITIMATE USERS
Tape Management	Tape Librarian
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 9 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 TSS; please note that responsibilities delegated to the IAO should be performed by an individual with appropriate knowledge and authority within the organization.

- Access to sensitive utilities will be strictly controlled via PROGRAM protection authorizations. TOP SECRET does not allow masking of program names for program protection control. Control access to the data sets in which the utilities reside through the use of data set access permission at the lowest required access level.

The DISA STIG provides the following technique related to the above recommendation 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 strictly controlled via PROGRAM protection authorizations. Access to protected programs considered sensitive in nature are audited.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.5.3 Sensitive Utility Controls.

3.3.1 DYNAMIC CONTROL LIST

As documented above 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 TSS, Dynamic list controls are provided via resources in the FACILITY resource class. The actual owning ACID specified for deptacid are to be named in accordance with installation

recommendations. When protecting the facilities for dynamic lists via the FACILITY class, use the following controls:

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

   TSS ADDTO(deptacid) IBMFAC(CSVAPF.)

   TSS ADDTO(deptacid) IBMFAC(CSVDYNEX.)

   TSS ADDTO(deptacid) IBMFAC(CSVDYNL.)

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. The following is a sample command to grant profile ACID sysprog permission to add SYS1.NEWLIB to the APF list:

   TSS PERMIT(sysprog) IBMFAC(CSVAPF.SYS1.NEWLIB)

   ACCESS(UPDATE) ACTION(AUDIT)

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 CSV resources in the IBMFAC resource class is properly owned.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 3.4.5.4 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. Access to which must be limited to only required personnel. 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, Volume 1, Section 2.1.2.12 MCS Consoles.

Within TSS, MCS console controls are provided via resources in the SYSCONS, OPERCMDS, and TSOAUTH resource classes. Name the actual owning ACID specified for deptacid in accordance with installation recommendations.

The DISA STIG recommends the following in regards to controlling console access within TSS; please note that functions assigned 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 for each console consname and each authorized group and profile ACID oprprofileacid as follows:

   TSS ADDTO(deptacid) SYSCONS(consname)

   TSS PERMIT(oprprofileacid) SYSCONS(consname) ACCESS(READ) ACTION(AUDIT)

   TSS ADDTO(deptacid) OPERCMDS(MVS.)

   TSS ADDTO(deptacid) TSOAUTH(CONSOLE)

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

   TSS PERMIT(consname) SYSCONS(consname) ACCESS(READ) ACTION(AUDIT)

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

   TSS PERMIT(oprprofileacid) SYSCONS(consname) ACCESS(READ) ACTION(AUDIT)

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 3.4.5.6, OS/390 System Command Controls.

   TSS ADDTO (userid) MCSAUTH(INFO)

   TSS PERMIT(userid) OPERCMDS(MVS.MCSOPER.userid) ACCESS(READ) ACTION(AUDIT)

   TSS PERMIT(oprprofileacid) TSOAUTH(CONSOLE) ACCESS(READ) ACTION(AUDIT)

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 all consoles of the CONSOLE resource class (SYSCONS) are properly owned.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, VOLUME 1, Section 2.1.2.12 MCS Consoles, Section 3.4.5.5 MCS Console Controls.

3.3.2 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. Name the actual owning ACID specified for deptacid in accordance with installation recommendations.

The DISA STIG recommends the following in regards to controlling system commands within TSS; 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 permissions with logging as required using the resources defined in Table A-29, Controls on OS/390 System Commands. For example:

   TSS ADDTO(deptacid) OPERCMDS(MVS.)

   TSS PERMIT(usracid) OPERCMDS(MVS.ACTIVATE) ACTION(AUDIT)

   TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.) ACTION(AUDIT)

   TSS PERMIT(usracid) OPERCMDS(MVS.CONTROL.) ACCESS(UPDATE) ACTION(AUDIT)

TSS PERMIT(usracid) OPERCMDS(MVS.DISPLAY.) ACCESS(READ)

TSS PERMIT(usracid) OPERCMDS(MVS.MONITOR) ACCESS(READ)

TSS PERMIT(usracid) OPERCMDS(MVS.STOPMN) ACCESS(READ)

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 TSS PERMIT statements are to include the ACCESS and ACTION values specified in the SOP, or ACTION(AUDIT) if not specified.

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

     TSS PERMIT(usracid) OPERCMDS(MVS.CANCEL.JOB.pfx*) ACCESS(UPDATE) ACTION(AUDIT)

     TSS PERMIT(usracid) OPERCMDS(MVS.MODIFY.JOB.pfx*) ACCESS(UPDATE) ACTION(AUDIT)

     TSS PERMIT(usracid) OPERCMDS(MVS.STOP.JOB.pfx*) ACCESS(UPDATE) ACTION(AUDIT)

   - The following is an example of granting users with a profile ACID of oprprofileacid permission to issue ROUTE commands to sysid from consid, after obtaining permission from the IAO:

     TSS PERMIT(oprprofileacid) OPERCMDS(MVS.ROUTE.CMD.sysid) ACCESS(READ) ACTION(AUDIT) WHEN(CONSOLE(consid))

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 OPERCMDS resource class is active.

Refer to the DISA O/S 390 & z/OS STIG, V5R2, Section 3.4.5.6 OS/390 System Command Controls.

3.3.3 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.

Every CICS region can be secured using the TSS/CICS sub-product. TSS uses information within an ACID record to determine access by CICS. It is recommended to the organization require individual CICS users to sign on to the CICS region. This will ensure accountability and appropriate access control. CICS sign-on is optional with the TSS CICS interface. Therefore if

a terminal runs under CICS but a sign-on has not been performed TSS will use the organizations defined default ACID for validating terminal requests.

The DISA STIG, volume 2, discusses controls for CICS transaction control within TSS. 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.

TSS CICS Security Related System Initialization Parameters

CICS Region Logonid Controls

CICS User Control

CICS Transaction Control

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.

(This Page Intentionally Blank)

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
CMSRs	CMS Minimum Security Requirements
CPU	Central Processing Unit
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

- OS/390-Z/OS Security. (2004). *Audit and Control Features.* Peter Thingsted
- Computer Associates International, Inc. (2005). *e Trust CA-Top Secret: Security for z/OS, Auditors Guide.* Islandia, New York.
- Computer Associates International, Inc. (2005). *e Trust CA-Top Secret: Security for z/OS, Control Options Guide.* Islandia, New York.
- Computer Associates International, Inc. (2005). *e Trust CA-Top Secret: Security for z/OS, Users Guide.* Islandia, New York.
- 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)