IBM Z/OS
SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

27 April 2023

Developed by DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

1. INTRODUCTION

1.1 Executive Summary

A core mission for the Defense Information Systems Agency (DISA) is to secure Department of Defense (DOD) computing systems. The processes and procedures outlined in this Security Technical Information Guide (STIG), when applied, will decrease the risk of unauthorized disclosure of sensitive information. Security is clearly still one of the biggest concerns for our DOD customers, including the warfighter.

This STIG was developed to enhance the confidentiality, integrity, and availability of sensitive DOD Automated Information Systems (AIS).

The requirements set forth in this document will assist Information System Security Managers (ISSMs), Information System Security Officers (ISSOs), Network Security Officers (NSOs), and System Administrators (SAs) in support of protecting DOD virtual computing systems.

The Information Operations Condition (INFOCON) for the DOD recommends actions during periods when a heightened defensive posture is required to protect DOD computer networks from attack. The ISSO will ensure compliance with the security requirements of the current INFOCON level and will modify security requirements to comply with this guidance. Password length and complexity given throughout this document must be adjusted as needed to comply with INFOCON guidance.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be […] configured […] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from https://public.cyber.mil/.

1.5 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked Controlled Unclassified Information (CUI) will be available for items that did not meet requirements. This report will be available to component authorizing official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.7 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production

environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.8 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (https://www.niap-ccevs.org/) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (https://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (https://www.disa.mil/network-services/ucco) IAW DODI 8100.04.

2. INTRODUCTION TO Z/OS

2.1 z/OS Background

Operating system security design for most mainframe information systems deployed throughout DOD uses the International Business Machines (IBM) z/OS operating system. Controls within z/OS have been developed and documented in IBM references to ensure operating system integrity is maintained.

Security mechanisms that provide MAC II Sensitive level controls for the z/OS operating environments are implemented by External Security Managers (ESMs). Previously these ESMs were known in the industry as Access Control Products (ACPs). In this document, as well as the STIGs that it supports, the terms ESMs and ACPs will be referenced interchangeably.

ESMs currently in use throughout DOD are listed below:

- Access Control Facility 2 (ACF2) – Computer Associates (CA).
- Resource Access Control Facility (RACF) – IBM Corporation[1].
- TOP SECRET (TSS) – Computer Associates (CA).

To maintain the integrity of the site, the ESM must be properly installed and configured. Options specified during the installation and techniques involved in the administration of these products can reduce the information assurance introduced into the individual operating environment. As a result, guidance is needed on how these products should be configured in the operational environment.

The System Authorization Facility (SAF) provides an installation with centralized control over system security processing through a system service called the MVS router. The MVS router provides a focal point for all products that provide resource management. Access to the MVS router is via the RACROUTE macro, which invokes the router program itself. The router in turn invokes the ESM to determine if authorization exists for the resource being tested.

This concept provides a single interface that encourages the use of common functions across products and platforms. Products that interface via SAF calls can be protected with any of the three ESMs discussed in this document without modification of their interface code.

All new software acquired for or developed by DOD will fully use the SAF interface. Existing software that fails to use the SAF interface will be converted to do so where possible.

2.2 z/OS Data Set Types

z/OS operation data is held in many types of data sets that have a specific purpose in the system operation. Many of these data set types require security protection to ensure the confidentiality, integrity, and accessibility of the system. Major types are detailed below:

[1] IBM has renamed RACF as the z/OS Security Server. In the interest of brevity, clarity, and continuity, this document continues to refer to the product as RACF.

- **Installation data sets** primarily are system and product datasets that contain modules or data required to place a system/product into operation on the mainframe. The files are usually shipped with the operating system/product and for the most part are unmodified by the site. They are usually in one central location and are required for system/product maintenance. The data sets are generally the basis for the system/product.
- **Started Task (STC) data sets** are read, controlled, created, and/or sustained by the STC. Since the system/application can require elevated access, it is important to protect these data sets from inappropriate use.
- **User data sets** require some level of interaction with a user. Since there are differing levels of users in the z/OS arena, e.g., systems programmer users, production control users, end users, etc., security requirements must be defined according to those levels.
- **Program data sets** are specific data sets necessary for application operation. These data sets can contain operation-sensitive information and must be appropriately protected.

2.3 z/OS Additional Access/Logging Restrictions

Data set and resource access documented in the vulnerabilities establishes the basic access requirements. At the ISSO's discretion, additional controls may be implemented to provide additional restrictions. An example of additional controls would be the use of program pathing to restrict access to a data set or resource when a specific program and/or program mask is used.

Data set and resource logging requirements documented in the vulnerabilities specify where successful access logging starts. By default, all violations to access a data set and/or resource will require that logging be performed.

3. Z/OS PRIVILEGED USERS

Due to its architecture and structure, the mainframe definition of a privileged user will refer to any users or tasks that require a level of access that provides for control, monitoring, or administration of the mainframe platform.

Common roles include:

- System Programmers.
- System Security Administrators.
- Operators.
- Tape Librarians.
- Storage Administrators.
- Automation Specialist.
- Schedulers.
- Application Support Teams (Domain level).
- Any team member who has physical access to the data center and data storage.

Members of these teams will be granted special privileges and special accesses that will be controlled by the systems ESM. These individuals will be assigned by and be the responsibility of the site ISSM.

For example, references to System Programmers in the z/OS STIG will be as follows:

For the purpose of the z/OS STIG, Systems Programmers will be defined as individuals who are responsible for the z/OS system software and z/OS system products. These individuals will have Level 1 responsibility to keep the z/OS operating system software and its associated system software products functioning in a stable and well-maintained status and will be under management and control of the data center. These individuals will be assigned by the site ISSM to perform these duties.

System programmers include such roles/functions as: OS System Programmer, DASD or Storage Administrator, CICS System Programmer, MQ Series System Programmer, Communications System Programmer, Database System Programmer (including but not limited to IDMS, IMS, DB2, ADABAS, ORACLE, etc. — DBAs who install executive software on the mainframe).

IBM z/OS deems certain started tasks and procedures to be “TRUSTED”. These key started procedures and address spaces are allowed to bypass ESM authorization checking and to successfully access or create any resource as needed. A list of required and optional candidates for the TRUSTED attribute can be found in z/OS MVS Initialization and Tuning Reference “Assigning the RACF TRUSTED attribute”. Other started tasks can be added to this list as required by product documentation and approved by ISSMs.

4. Z/OS UNIX SYSTEM SERVICES

4.1 z/OS UNIX System Services Background

z/OS UNIX System Services, abbreviated by IBM as z/OS UNIX, provides a UNIX environment to z/OS users. It is now a base component of the z/OS operating system, conforms to the XPG4 UNIX 1995 standard (with UNIX 98 elements), and offers services designed to support applications written to open systems standards. z/OS UNIX also provides z/OS users the traditional UNIX structure for data storage through the Hierarchical File System (HFS)/zSeries File System (zFS). Finally, z/OS UNIX supports the UNIX User Identifier (UID) and Group Identifier (GID) concepts that establish identity in the UNIX environment.

In z/OS UNIX, security is handled, in part, through the UID and GID constructs that identify users and groups. This security impacts file access and process (e.g., z/OS task) control. While it is possible in some environments for multiple users to be assigned the same UID, this does not provide a desirable level of security.

z/OS UNIX provides an operating environment that can host many services such as File Transfer Protocol (FTP) and z/OS UNIX Telnet servers. In addition, z/OS components such as Communications Server provide support to z/OS UNIX. This section of this document is intended to describe the security considerations for the z/OS UNIX environment and does not cover these supporting and supported components in detail. Refer to other sections of this document and the pertinent vendor documentation for security considerations for these components.

4.2 z/OS UNIX General Considerations

Because of the scope of z/OS UNIX and its difference from the traditional MVS environment, several considerations must be addressed to understand the security implications. This section discusses security considerations for the following areas:

- User Identity – UID and GID Assignment.
- Data Storage – HFS/zFS Directories and Files.
- Interactive Environment – The UNIX Shell.
- Background Processes – Daemons and Servers.
- Miscellaneous Considerations.

These considerations are discussed to explain the z/OS UNIX environment. This background is used when discussing the specific controls that implement security policy.

Table 4-1: General FACILITY Class BPX Resources

General FACILITY Class BPX Resources	
Resource Name	**Description/Notes**
BPX.DAEMON	Allows a daemon to use the seteuid, setuid, setreuid, and spawn services.
BPX.DEBUG	Allows a user to use ptrace (via dbx) to debug programs that run with APF authority or with BPX.SERVER authority.
BPX.FILEATTR.APF	Allows a user to set the APF-authorized attribute in an HFS file.
BPX.FILEATTR.PROGCTL	Allows a user to set the program-controlled attribute in an HFS file. This attribute is required, in most cases, for all programs executed by daemons or servers.
BPX.JOBNAME	Allows a user to set jobnames using the _BPX_JOBNAME environment variable or the inheritance structure on spawn.
BPX.SAFFASTPATH	Enables SAF fastpath support. This means that successful security checks are not audited. No access list is needed; the existence of the profile enables the function.
BPX.SERVER	READ: Allows the server to establish a thread-level security environment for its clients. Access control decisions are based on the server's userid and the client's userid unless the server specifies a password on the service invocation. UPDATE: Allows the server to establish a thread-level security environment for its clients. Access control decisions are based only on the client's userid. The pthread_security_np (create/delete security environment) and the auth_check_resource_np (resource authorization checking) services are used. Also see the BPX.SRV.*userid* profile description.

General FACILITY Class BPX Resources	
Resource Name	**Description/Notes**
BPX.SMF or BPX.SMF.*type.subtype*	Allows permitted user access to write an SMF record or to test if an SMF type or subtype is being recorded. • The BPX.SMF profile grants the permitted user the authority to write or test for any SMF record that is being recorded. The program-controlled attribute is not required if BPX.SMF is used. • For more granular access to writing SMF records, BPX.SMF.*type*.*subtype* allows a permitted user the authority to write or test only the SMF record of the specific type and subtype contained in the FACILITY class profile name. **Note**: BPX.SMF must not be permitted to regular interactive userids.
BPX.STOR.SWAP	Allows a user to make address spaces non-swappable or swappable.
BPX.SUPERUSER	Allows a user to switch to superuser authority (i.e., effective UID of "0").
BPX.WLMSERVER	Allows a user to access Work Load Manager (WLM) server functions and C language WLM interfaces. These functions and interfaces are commonly used by server applications. Also see the BPX.SERVER profile description.

Table 4-2: UNIXPRIV Class Resources

UNIXPRIV Class Resources	
Resource Name	**Description/Notes**
CHOWN.UNRESTRICTED[2]	Allows all z/OS UNIX users to transfer ownership for files they own to any UID or GID on the system. No access list is needed. The existence of the profile enables the function. Therefore, the resource will not be defined.

[2] The CHOWN.UNRESTRICTED profile defeats a basic file ownership protection and must not be defined unless justified and documented to the ISSO.

UNIXPRIV Class Resources	
Resource Name	**Description/Notes**
SHARED.IDS (RACF only)	Allows users to assign UID and GID values that are not unique. To specify non-unique UID or GID, users must specify the SHARED keyword in the RACF AG, AU, ALG, and ALU commands. These users must have the SPECIAL attribute or at least READ authority to the resource. Therefore, the resource will be defined with no access given to users.
SUPERUSER.FILESYS	READ: Allows the user to read any HFS file and to read or search any HFS directory. UPDATE: Allows the user to write to any HFS file and includes *read* access. CONTROL: Allows the user to write to any HFS directory and includes *update* access. **Note**: Allows access only to local HFS files, not to NFS files.
SUPERUSER.FILESYS.CHANGEPERMS	READ: Allows a user/group to do a CHMOD to any file.
SUPERUSER.FILESYS.CHOWN	READ: Allows the user to change the ownership of any file.
SUPERUSER.FILESYS.MOUNT	READ: Allows the user to mount a file system with the nosetuid option and to unmount a file system mounted with the nosetuid option. UPDATE: Allows the user to mount a file system with the setuid option and to unmount a file system mounted with the setuid option.
SUPERUSER.FILESYS.QUIESCE	READ: Allows the user to quiesce and unquiesce a file system mounted with the nosetuid option. UPDATE: Allows the user to quiesce and unquiesce a file system mounted with the setuid option.
SUPERUSER.FILESYS.PFSCTL	READ: Allows the user to use the pfsctl() (physical file system control) callable service.
SUPERUSER.FILESYS.VREGISTER	READ: Allows a server to use the v_reg() callable service to register as a virtual file system (VFS) file server.

UNIXPRIV Class Resources	
Resource Name	**Description/Notes**
SUPERUSER.IPC.RMID	READ: Allows the user to issue the ipcrm command to release IPC (Interprocess Communication) resources.
SUPERUSER.PROCESS.GETPSENT	READ: Allows the user to use the w_getpsent callable service to receive process status data for any process.
SUPERUSER.PROCESS.KILL	READ: Allows the user to use the kill() callable service to send signals to any process.
SUPERUSER.PROCESS.PTRACE	READ: Allows the user to use the ptrace() function through the dbx debugger to trace any process. Also allows users of the ps command to output information on all processes. **Note**: Authorization to FACILITY class resource BPX.DEBUG is required to trace processes that run with APF authority or BPX.SERVER authority.
SUPERUSER.SETPRIORITY	READ: Allows the user to increase that user's own priority.

Table 4-3: MVS Data Sets with z/OS UNIX Components

MVS Data Sets with z/OS UNIX Components		
Data Set Name/Mask	**Maintenance Type**	**Function**
SYS1.ABPX*	Distribution	IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.AFOM*	Distribution	IBM z/OS UNIX Application Services
SYS1.BPA.ABPA*	Distribution	IBM z/OS UNIX Connection Scaling Process Mgr.
SYS1.CMX.ACMX*	Distribution	IBM z/OS UNIX Connection Scaling Connection Mgr.
SYS1.SBPX*	Target	IBM z/OS UNIX ISPF panels, messages, tables, clists
SYS1.SFOM*	Target	IBM z/OS UNIX Application Services
SYS1.CMX.SCMX*	Target	IBM z/OS UNIX Connection Scaling Connection Mgr.

4.3 z/OS UNIX User Identity

Within UNIX systems, users are assigned a user name and password that allow identification and authentication when the system is accessed. Each user is also assigned a numeric identifier known as the UID. Users are members of one or more groups, and each of these groups has a name and a numeric identifier known as the GID. While it is possible in some environments to assign multiple users the same UID, this is not done where meaningful security is desired.

There are no software-specific UID or GID numbers, with one exception. If a user is assigned a UID value of 0 (zero), the user has *superuser* status and effectively bypasses all security checks. There are a limited number of instances where superuser status is actually needed, and z/OS UNIX provides some security resources that can be used to further limit the need to assign UID (0) to users.

During a UNIX shell session or during the execution of commands with certain attributes, it is possible for a user to temporarily use a different UID or GID value than what was assigned. The userid defined to the security system and used at system sign on is referred to as the real ID. The temporary userid used for a specific period or process is referred to as the effective ID. For this reason, it is important to check the effective ID when researching access control issues.

4.4 z/OS UNIX User Identity

This section discusses the considerations related to data storage in the z/OS UNIX environment. These considerations include the logical and physical structures, file access permissions,

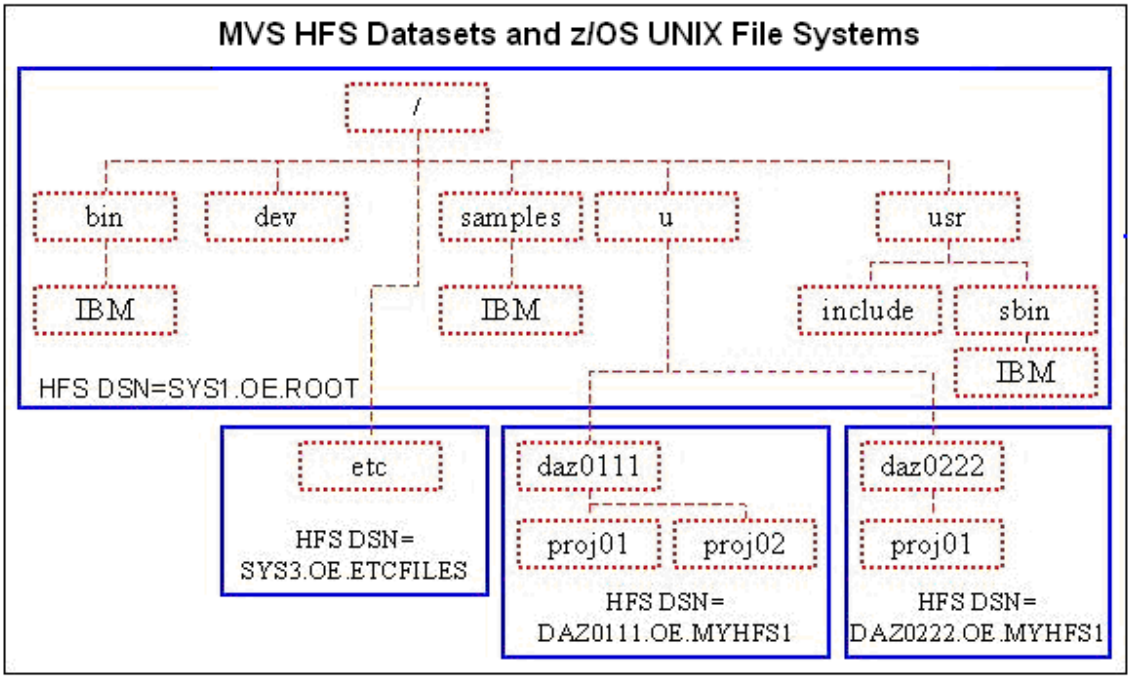
extended attributes for executable files, and audit attributes. Understanding these considerations is important to setting and maintaining data and command security.

Hierarchical File System (HFS)/zSeries File System (zFS) is a tree structure consisting of multiple file systems. A file system is a logical collection of directories and files. The highest-level directory in the hierarchy is the root directory, which is often kept in a file system with only a few other directories. Each file system is made available by a process known as mounting the file system. It is mounted at a *mount point* that is a directory in the higher-level file system.

The entire file hierarchy is made up of a collection of HFS/zFS data sets. Each physical HFS/zFS data set is a mountable file system. This means it can be attached to the HFS/zFS tree at a mount point in the root directory or at a mount point further down in the hierarchy. Each HFS/zFS data set needs data set access rules defined to protect it.

The following diagram illustrates the relationship between MVS HFS/zFS data sets and z/OS UNIX file systems. This is an example with four MVS data sets (SYS1.OE.ROOT, SYS3.OE.ETCFILES, DAZ0111.OE.MYHFS1, and DAZ0222.OE.MYHFS1) corresponding to four z/OS UNIX file systems (*root*, etc., daz0111, daz0222).

Figure 4-1: MVS HFS Datasets and Z/OS UNIX File Systems



5. EXTERNAL SECURITY MANAGER IMPLEMENTATION

5.1 ESM General Considerations

The ESM is the primary mechanism that controls access to data and resources in z/OS systems. Each ESM in use on the DOD platforms provides the flexibility to tailor the implementation to meet the needs of the local installation.

Many different implementations of various ESMs exist. These different implementations meet the needs of each local installation but make it difficult to coordinate and control the DOD Enterprise.

All deviations are to be specifically noted, with justification and approval documentation, in the system security plan and the accreditation package submitted to the Authorizing Official (AO).

To provide full compliance with the security support required by *DOD Directive 8500.1*, control all products within the operating system using the ESM. Use the following guidance in the acquisition of products to ensure that security-related issues are adequately addressed:

(1) Products are to be on the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Validated Products List before procurement and implementation.
(2) At a minimum, evaluate products for sensitive functions and implement controls to protect these functions.
(3) Restrict all data sets associated with a product to the access levels necessary for support and operation based on the requirements. Only authorized personnel who require the authority to modify or maintain the product are to have *update* and *alter* access.

Each ESM provides the capability for customization using global ESM configuration and processing options. These global options provide the flexibility to tailor the configuration and processing of the ESM to the needs of the local operating environment. These options also can pose the danger of compromising the operational environment when misused or not properly applied.

DOD, as a large organization, has the additional complication of diversity. There are many different applications of the global options. These different applications meet the needs of each local installation but make it difficult to manage the organizational computing base as a whole. The task of optimizing the processing load of the enterprise across the myriad platforms becomes almost impossible.

For the above reasons, and to mitigate the above risks and difficulties, all DOD processing environments are to implement the z/OS STIG-required global options for each ESM installed. The z/OS STIG-required options are specified in the individual External Security Manager Installation sections of this document. The options specified are z/OS STIG requirements, and each site can choose to be more restrictive.

5.1.1 ESM Userid Controls

ESM Userid Controls require that each system user is uniquely identified to the operating environment and that access to resources is limited to those needed to perform the function. In this case, a user is defined as either an individual accessing a computer resource or as a task executing on the system that requires access to a resource. On z/OS systems, a user is identified by means of a unique userid. This z/OS STIG requires that audit data record the identity of the user, time of access, interaction with the system, and sensitive functions that might permit a user or program to modify, bypass, or negate security safeguards.

It then follows that any userid (user) on the system must be associated with only one individual. However, any given individual may be assigned responsibility for multiple userids on a given system, depending on functional responsibilities, to ensure task segregation.

5.1.2 ESM Access Authorizations

ESM data set and resource access controls detail the proper userid and level of access required by the Site Security Plan in accordance with DODI 85000.01. z/OS STIG “data set rules” are intended to include the access list(s) (Standard and Conditional) and access through being the owner. Access through ownership as determined by the high-level qualifier (HLQ) is considered to be implied and is not mentioned specifically in z/OS STIG controls.

Access to privileged profiles is noted as “Write or Greater.” The access determination of “WRITE or Greater” indicates a generic IT term to describe the level of access. The “or Greater” determines that the privilege not only gives the ability to change an object but also to create and delete it.

5.1.3 Password Complexity

Password complexity is a measure to minimize guessing and brute-force attacks. The DOD has instituted the requirement that all passwords must be at least 15 characters in length. Currently the zOS operating system can only support a maximum password length of 8. As mitigation to this shortfall, each of the ESMs has introduced additional measures to assist in password complexity. One of these measures is a restriction of reserved words and prefixes. The following contains the default list of reserved words and prefixes for each ESM. For CA-ACF2, they are contained in RESWORD in the GSO record. In CA-TSS, use the RPW control option to view and modify the restricted password list. For RACF, the list is loaded in IRRPWREX.

Each site can add to this list to reflect regional common words and prefixes.

Table 5-1: Reserved Words and Prefixes

APPL	APR	ASDF	AUG	BASIC
CADAM	DEC	DEMO	FEB	FOCUS
GAME	IBM	JAN	JUL	JUN
LOG	MAR	MAY	NET	NEW
NOV	OCT	PASS	ROS	SEP
SIGN	SYS	TEST	TSO	VALID
VTAM	XXX	1234		