VIRTUAL MACHINE (VM)

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 2, Release 1

JULY 2003

DISA
FIELD SECURITY OPERATIONS

This page is intentionally left blank.

TABLE OF CONTENTS

Page

LIST OF TABLES

This page is intentionally left blank.

SUMMARY OF CHANGES

Changes in this document since the previous release (Version 1, Release 3, dated 29 April 2002) are listed below.

General

- Minor wording, grammar, formatting, and typographical changes and corrections to this document are not included in the Summary of Changes.
- This document is undergoing language and format standardization to conform to the stipulations in Section 1.5, Writing Conventions and to conform with the other STIGS published by the Field Security Operations (FSO) Division. Formatting changes are being introduced to make requirements easier to identify. An example of these changes may be found in Section 1.15. It should be noted these are formatting and linguistic changes only and do not affect the security requirements incumbent upon the reader, therefore those sections are not identified under Summary of Changes.

Section 1.1 Background

- Made changes based on recent STIG consistency efforts.

Section 1.4 Authority

- Corrected authority information.

Section 1.5 Writing Conventions.

- Replaced.

Section 1.7 Security Administration

- Replaced.

Section 1.8 Processing Environments

- Made changes based on recent STIG consistency efforts.

Section 1.9 INFOCON

Deleted this section and its sub-sections. Re-numbered sections appropriately.

Section 1.9.2 Security Controls (renumbered)

- Made changes based on recent STIG consistency efforts.

Section 1.12 Extensions

- Replaced.

Section 1.14 STIG Distribution

- Replaced.

Section 1.15 Document Review Process

- Made changes based on recent STIG consistency efforts.

Section 1.16 Document Revisions

- Added section based on recent STIG consistency efforts.

Section 4. External Security Manager Implementation

- **4.3 RACF** – This new section has been added to document the features and security requirements for DISA sites using the RACF security product. Please review in its entirety.

This page is intentionally left blank.

1. INTRODUCTION

1.1 Background

Department of Defense Directive (DoDD) 8500.1 establishes policy and assigns responsibilities to the Defense Information Systems Agency (DISA) to develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with the National Security Agency. Paragraph 4.18 of the 8500.1 states, " All IA and IA-enabled IT products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines." DISA Field Security Operations (FSO) develops the guidelines which are called Security Technical Implementation Guides (STIGs).

These STIGs serve as the security configuration guidelines required by DODD 8500.1. The specific guidance contained in this STIG will change considerably in the future with the new international standard (Common Criteria for Information Technology Security Evaluation - ISO/IEC 15408) being implemented by the National Information Assurance Partnership (NIAP) and the planned release of DOD Manual 8500.bb. These issues will be addressed in an upcoming release of this STIG. This document has been supplemented with additional information concerning specific operating system environments including the Microsoft Windows NT, Windows 2000, and Windows XP operating systems.

1.2 Purpose

The *VM Security Technical Implementation Guide (STIG)* defines the technical criteria necessary to implement secure functionality within DISA information systems. The purpose of this document is not to define policy, but to document the procedures and parameters necessary to implement policy. Policy serves no value if it cannot be technically implemented.

When implementing security within the VM operating platform, or within any platform, essentially three criteria must be considered – confidentiality, integrity, and availability. For purposes of this document, each is defined as follows:

- **Confidentiality:**

  Assurance that information is not disclosed to unauthorized entities or processes. Confidentiality encompasses *least privilege*. *Least privilege* says that users or processes have only the authority to access those resources necessary to perform their functions.

- **Integrity:**

  Assurance that resources, to include data, are the same as that in the source and have not been exposed to accidental or malicious alterations or destruction.

  - **Availability:**

  Assurance that resources, to include data, are in the place, at the time, and in the form needed by the user or process.

This document defines the requirements, standards, controls, and options that must be in place for the Access Control Products (ACPs) under VM, and for each utility to comply with DISA requirements. The site may implement additional security as necessary.

1.3 Scope

The requirements set forth in this document are for VM and for the installed ACP. Internal Product Security Controls (IPSCs) will be limited to augmenting the ACPs for the following sites:

- Systems Management Centers (SMCs)
- Computing Services Processing Element (CSPE)
- Systems Support Offices (SSOs)
- DOD Components
- Other DISA customers

1.4 Authority

The Security Technical Implementation Guides (STIGs) were initially developed to assist the sites in securing their systems against security and infrastructure vulnerabilities. All sites have a vested interest in maintaining system security, as it directly impacts the site's Certification and Accreditation (C&A). Sites are mandated by DISA to have a valid C&A status by the authority derived from *DOD Directive 8500.1, Security Requirements for Automated Information Systems, 24 October 2002*, and the *Computer Security Act of 1987, Public Law 100-235, January 1988*. The requirements for accreditation of DISA Information Technology, as described here, are found in *DISAI 630-230-19, DISA Information Systems Security Program, July 1996*. Compliance with the applicable Security Technical Implementation Guide (STIG) is mandatory for systems residing in a DISA facility and for any system directly administered by DISA. The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the Mission Assurance Category (MAC) II Sensitive level, containing unclassified but sensitive information.

1.5 Writing Conventions

Throughout this document, statements are written using the words "**will**" and "**should**." The following paragraphs are intended to clarify how these statements are to be interpreted.

A reference using "**will**" implies mandatory compliance. All requirements of this kind will also be documented in the italicized policy statements in bullet format, which follow the topic paragraph. This will make all "**will**" statements easier to locate and interpret from the context of the topic. The IAO, System Administrator (SA), or Telephone Switch Administrator must adhere to the instruction as written. Only an extension issued by DISA will table this requirement for DISA facilities. The extension will normally have an expiration date, and does not relieve the IAO, SA, or Telephone Switch Administrator from continuing their efforts to meet the requirement.

A reference to "**should**" is considered a recommendation that further enhances the security posture of the site. These recommended actions will be documented in the text paragraphs, but not in the italicized policy bullets. All reasonable attempts to meet these recommendations will be made.

1.6 Organizational Relationships

Organizational relationships play a significant role in providing for the security of the environment. The DISA site organization must provide a robust and secure environment that protects the software environment from unauthorized access. This is to include the protection of system-level resources (i.e., mainframe hardware, system products such as VM, database systems, and other utilities used by the DOD user community/customers). Data owners must also play a role in determining access requirements for their resources (i.e., actual databases, master files, and interactive transactions). It is the responsibility of the data owner to provide an access matrix that reflects subjects (processes and authorized personnel) and their access to objects (processes, files, and other resources).

1.7 Security Administration

DISA is currently consolidating all system management functions, including security administration, for OS/390 and z/OS mainframe computing into three locations. This includes the formation of two System Management Centers (SMCs) and one Computing Services Processing Element (CSPE). While OS/390, z/OS and VM processing will occur at the SMCs and CSPE, the SMCs will provide the security administration for all three locations utilizing remote support for the CSPE.

1.8 Processing Environments

Some Information Systems (ISs) used throughout DISA sites use the International Business Machines (IBM) Virtual Machine (VM) operating system. The VM operating system, as distributed by IBM, provides integrity of the operating environment as part of the trusted computer base, as defined in *Department of Defense (DOD) Directive 8500.1, Information Assurance.* Controls have been developed and documented in IBM references to ensure this integrity.

Security mechanisms that provide MAC II Sensitive functionality for the VM operating environment are implemented by the addition of Access Control Products (ACPs). The ACPs currently in use throughout DISA are ACF2, RACF, TOP SECRET (TSS), and VM:Secure.

To maintain the integrity of the site, the ACP must be properly installed and configured. Options specified during the installation and techniques involved in the administration of these products can either enhance or reduce the security of the individual operating environment. As a result, guidance is needed on how these products should be configured in the operational environment.

1.9 VM Security Design

1.9.1 Access Control Interface

The Access Control Interface (ACI) is a group of modules that provides an installation with centralized control over system security processing. The ACI serves as a mediator between the Control Program (CP) and the External Security Manager (ESM). Access to the ACI is via the CP. Whenever an event occurs that requires the ESM's involvement, the CP checks the security bit settings for that event, calls the ACI, and passes security information through the ACIPARMS control block. The ACI then passes the request to the ESM through the Inter-User Communication Vehicle (IUCV). The ESM performs the requested function, records its response in the ACIPARMS, and passes it back to the CP, which carries out the ESM's decision.

All new software acquired for or developed by DISA will fully utilize the CP ACI. Existing software that fails to use the CP ACI will be converted to do so where possible.

1.9.2 Security Controls

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

(1) DISA Field Security Operations, in coordination with the DISA Denver Executive Software/Configuration Control Board (ES/CCB), will approve all products before procurement and implementation.

(2) At a minimum, evaluate products for sensitive functions, and implement controls to protect those functions. DISA Field Security Operations will coordinate and approve all security controls implemented.

(3) Restrict all files associated with a product to the access levels necessary for support and operation based upon the requirements. Only those authorized personnel who require the authority to modify or maintain the product will have *update* and *alter* access.

Many products require special security considerations. Enforce the following considerations relating to compatibility and interfacing with the CP ACI:

(1) Protect Commercial-Off-The-Shelf (COTS) products and associated files within the operating system using the ACP. Ensure that all COTS products being procured have and use the CP ACI to the ACP.

(2) Secure Government-Off-The-Shelf (GOTS) products and newly developed applications, along with associated files, using the ACP. Whenever possible, develop applications using the CP ACI. Safeguards enforced by the ACP will not be duplicated by security mechanisms implemented within an application. Limit developed internal security mechanisms to those functions that augment the safeguards present in the ACP.

(3) Internal Product Security Controls (IPSCs) are security mechanisms internal to COTS products and GOTS applications. Only use IPSCs when existing products or applications do not interface to the ACP through the CP ACI, or to augment the protections provided by the existing interface. Reconfigure products using IPSCs, which are capable of taking advantage of the CP ACI.

Whenever IPSCs are being used, develop and maintain security documentation. The documentation will include descriptions of the IPSCs, the configuration, and the policy being enforced. The IAO will maintain the documentation and will perform the administration of IPSCs where practical.

(4) Modify all GOTS products and applications (if using ACP-specific interfaces) to interface with the ACP via standard CP ACI calls.

All applications will eventually migrate from IPSCs to using the ACP. If this is unreasonable for any given application, the application will eventually be phased out.

1.9.3 Development and Test Domains

Testing of new or modified software will be performed in a carefully constrained environment. All testing will be in accordance with the following guidelines:

(1) Classify a software test domain/VM image as falling into one of the following three risk groups:

Group 1 Software that cannot bypass any of the ACP access controls. Applications software usually falls into this group.

Group 2 Software that can bypass ACP access controls but cannot bypass the CP and CMS (Conversational Monitor System) controls. Utilities, commands, and user exit software usually fall into this group. Testing of new software products requiring relaxed access control policies also falls into this category.

Group 3 Tests that bypass the CP and CMS controls. Contact Field Security Operations prior to conducting these tests.

(2) If there is any doubt of the appropriate group for a software test candidate, either place it in the next (numerically) higher group, or contact Field Security Operations for guidance.

(3) Test candidates fully qualifying for membership in Group 1 will comply with the following detailed guidelines:

(a) DASD units will be on-line only to one system at a time. The only exception to this is when moving software between domains. DASD may be on-line concurrently to

multiple systems for the duration of the software move. The DASD will be taken off-line from the additional system(s) upon completion of the software move.

(b) Install and configure the ACP to be fully compliant with the *VM STIG*.

(c) All data files used by applications will be sacrificial copies of production files.

(d) Upon completion of the tests, overwrite the data files used by the test with an approved routine before releasing the space occupied by the data files, or enable the object reuse facility.

(e) Serious consideration should be given to complying with the guidelines for Group 2.

(4) Test candidates fully qualifying for membership in Group 2, or those Group 1 candidates selected for consideration as Group 2, will comply with the following detailed guidelines:

(a) DASD units will be on-line only to one system at a time. The only exception to this is when moving software between domains. DASD may be on-line concurrently to multiple systems for the duration of the software move. The DASD will be taken off-line from the additional system(s) upon completion of the software move.

(b) Sever or disable all network connections outside the site.

(c) Any additional privileges granted to the Test Support staff will only be for the duration of the test.

(d) All operating system and data files used will be sacrificial copies of production files.

(e) Upon completion of the tests, overwrite the operating system and data files used by the test prior to release.

(5) Test candidates fully qualifying as Group 3 will not be tested at a site. For further guidance, coordinate with Field Security Operations prior to testing for methods of handling such test requirements.

1.10 Information Operations Condition (INFOCON)

1.10.1 Purpose

The Information Operations Condition (INFOCON) for the Department of Defense recommends actions to uniformly heighten or reduce defensive posture, to defend against computer network attacks, and to mitigate sustained damage to DOD information infrastructure, including computer and telecommunications networks and systems. It is the responsibility of the site to ensure compliance with the *CJCS INFOCON Memo* that was signed on 10 March 1999 by General Joseph W. Ralston, Acting Chairman of the Joint Chiefs of Staff. Additionally, the ISM will be

responsible for developing any new supplemental procedures that are required (or for modifying old procedures) in order to comply with INFOCON guidance.

1.10.2 Description

The INFOCON system presents a structured, coordinated approach to react to and defend against adversarial attacks on DOD computers and telecommunications. While all communications systems are vulnerable to some degree, factors such as low-cost, readily available information technology, increased system connectivity, and standoff capability make a computer network attack (CNA) an attractive option to our adversaries at present. CNA is defined as "operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." INFOCON also outlines countermeasures to scanning, probing, and other suspicious activity, unauthorized access, and data browsing. INFOCON levels are NORMAL, ALPHA, BRAVO, CHARLIE, and DELTA. Countermeasures at each level include preventive actions, actions taken during an attack, and damage control/mitigating actions.

1.10.3 Authority

The INFOCON system is established by the Secretary of Defense and administered through the Director of Operations, Joint Staff (J-3). INFOCON applies to the Joint Staff, combatant commands, and Defense agencies, as well as joint, combined, and other DOD activities throughout the entire conflict spectrum—peacetime through war.

INFOCON Levels
Normal (Normal Activity)
Alpha (Increased Risk of Attack)
Bravo (Specific Risk of Attack)
Charlie (Limited Attacks)
Delta (General Attacks)

- *Sites will comply with INFOCON procedures in accordance with the CJCS INFOCON Memo dated 10 March 1999.*

- *IAOs will develop supplemental procedures, as required, in consonance with INFOCON guidance.*

1.11 Education and Awareness Programs

For the system integrity guidelines and policies to function, managers and employees in the Systems/Technical Support and Security offices will periodically be advised of their responsibilities regarding the protection of the VM operating system.

The IAO, and others to whom security administration functions have been delegated, will receive adequate and continuing training in the use and implementation of the ACP(s) being used at the site(s) for which they are responsible.

Personnel in the Systems/Technical Support office will receive adequate training in the installation and maintenance of the ACP(s) in use at the site(s) for which they are responsible. They will also receive adequate and continuing training covering VM system internals. This will facilitate evaluation and validation of the use of utility programs, commands, system exits, and other critical areas of the VM operating system.

CDA (Central Design Activity) personnel will periodically be advised of their responsibilities regarding the protection of the VM operating system and the use of ACIs, system exits, and other critical areas of VM.

1.12 Extensions

With the recent migration of the Security Readiness Review Database (SRRDB) into the Vulnerability Management System (VMS), one of the major changes is that the previous Security Readiness Review (SRR) waiver and exemption process has been discontinued. Instead, sites must submit an on-line request for extension for any SRR finding that cannot be fixed and closed within the designated timeframe. This is the same process used by VCTS. The VMS SRRDB extension process for reviews and approvals will be similar as well.

Deviations from the standards will be allowed as long as:

- MAC II Sensitive controls are not jeopardized.
- A true business case justifies each deviation.
- The security of the site is not adversely affected.

After an SRR is completed, a report of findings will be presented to the organization. If findings cannot be resolved in a timely manner, an extension may be requested. Justification may include operational reasons, technical conflicts, and insufficient funding. An extension request will identify a plan and timetable for resolving the finding(s). Any supplemental security countermeasures should also be addressed.

Further details of this process are found in the *Computing Services Security Handbook*.

- The IAO will maintain a file for each server/workstation that has deviations to security recommendations. The file will document each exception and will contain a risk assessment for each deviation that the site Commander has approved. Lack of such documentation will result in findings for non-compliant systems.

1.13 Related Documentation

Refer to *Appendix A, Related Publications*, for a list of Government publications and vendor product references that contain additional material related to the subject matter in this document.

1.14 STIG Distribution

Compliance with the applicable Security Technical Implementation Guide (STIG) is mandatory for systems residing in a DISA facility and for any system directly administered by DISA. The use of the principles and guidelines in this STIG will provide an environment that meets or exceeds the security requirements of DOD systems operating at the MAC II sensitive level, containing unclassified but sensitive information.
In the interest of promoting enhanced security for systems both inside DOD and within the Federal Government's computing environments, DISA encourages any interested DOD activity or party to obtain the applicable STIG from the Information Assurance Support Environment (IASE) web site. This site contains the latest copies of any STIG, as well as checklists, scripts, and other related security information.

The NIPRNet URL for the IASE site is https://iase.disa.mil/. The Secret Internet Protocol Router Network (SIPRNet) URL is http://iase.disa.smil.mil/. The DISA FSO URL is http://guides.ritchie.disa.mil/. Access to the STIGs on the IASE web server requires a network connection that originates from a .mil or .gov address. The STIGs are available to users that do not originate from a .mil or .gov address by contacting the FSO Support Desk at DSN 570-9264, commercial 717-267-9264, or e-mail to fso_spt@ritchie.disa.mil.

1.15 Document Review Process

DISA Field Security Operations will review this document on a semi-annual basis to ensure that it meets the needs of the current site environments with respect to state-of-the-art security practices, security vulnerabilities, and solutions.

- *The IAO will ensure that the site maintains documentation on: system startup, shutdown, hardware configuration/reconfiguration, backup, recovery, physical security protection of the hardware configuration, security protection of the software used in the VM development/production environments, restricting access to the hardware components, restricting access to the functions of the master console from the local and/or remote operator consoles.*
- *The IAO will maintain a list of all of the ACPs used in the VM environment.*
- *The site will maintain a configuration chart describing all of the host VM machines, guest machines, operating system releases in each, workload names and access control products used in each.*
- *The IAO will ensure that that site maintains a current list of the VM system files to include:* ***USER DIRECTORY, CONFIGURATION FILE, ACCOUNTING FILE, and ALTERNATE CONFIGURATION FILE.***
- *The site will maintain a current list of all* ***SYSTEM SOFTWARE*** *and* ***VENDOR SOFTWARE PRODUCTS*** *running in the VM environment.*

1.16 Document Revisions

Revisions to this document should be sent via e-mail to **stig_comments@ritchie.disa.mil**. DISA FSO will coordinate all change requests with the relevant DISA Field Security Operations organizations, and other DISA organizations as appropriate, before inclusion in this document.

This page is intentionally left blank.

2. VIRTUAL MACHINE/ENTERPRISE SYSTEMS ARCHITECTURE - VM/ESA

2.1 Overview

Virtual Machine/Enterprise Systems Architecture (VM/ESA) is a multi-access, interactive operating system used in conjunction with the S/390 architecture. VM is able to support interactive processing, client/server environments, and other fully functioning operating environments (e.g., Multiple Virtual Storage [MVS], OS/390, and VM). VM provides a platform not only for hosting the traditional guest operating systems such as VSE and OS/390, but also for dependent guests such as MUMPS/VM and AIX*/ESA. VM/ESA is a true interactive application platform that provides cross platform application environment support. In addition, VM/ESA complements these services with VM-specific Application Programming Interfaces (APIs) such as the Callable Services Library and VM Data Spaces.

In a VM environment, the three types of processors are the master processor, dedicated processors, and alternate processors. The master processor is used by the Control Program (CP) to perform CP required work. Every VM machine must have a master processor. When the CP is loaded during an Initial Program Load (IPL), it must be IPLed on the master processor. A dedicated processor is a processor that belongs to a virtual machine and is reserved by the CP for working with that virtual machine. A dedicated processor will only run the work generated by that virtual machine's virtual processor. An alternate processor is a processor that can be used by any virtual machine to do work. It is the CP's responsibility to schedule alternate processors for processing.

VM is composed of a set of functions and services that support multiple types of system users. These functions, although independent, work in conjunction with each other to provide cross platform application environment support. VM provides the facilities for coding (integrated editing using XEDIT), compilation (using numerous compilers supported under VM/ESA), and running applications. In addition, VM/ESA complements these services with VM-specific APIs such as the Callable Services Library and VM Data Spaces.

2.2 Base Components

As mentioned above, VM is composed of a set of functions and services that are used to support multiple types of system users. These functions and services are categorized into different components. It should be noted that additional functions and services might be added to these components to support additional operating requirements.

The components that comprise VM/ESA are as follows:

- Control Program (CP)
- Conversational Monitor System (CMS)
- Restructured Extended Executor/VM (REXX/VM)
- Group Control System (GCS)
- Transparent Services Access Facility (TSAF)
- Advanced Program-to-Program Communication/VM (APPC/VM) VTAM Support
- Virtual Machine Serviceability Enhancements Staged/Extended (VMSES/E)
- Dump Viewing Facility
- RSCS (Remote Spooling Communications Subsystem)

2.3 Control Program

The Control Program (CP) is the nucleus of the VM operating environment. It is responsible for managing the resources of the real machine (i.e., processors, storage, consoles, and input/output [I/O] devices). The CP controls the allocation of the processing power of the available real processors in order to process virtual machine instructions. It does this by scheduling and dispatching real processor resources to virtual processors based on an internal dispatching priority scheme defined to the CP. The CP provides each user with a private working environment. This working environment is referred to as a virtual machine. Each virtual machine has the functional equivalent of a real system, sharing a portion of the real resources. (Real resources consist of processors, storage consoles, and I/O devices.) When a user first logs on to VM/ESA, the CP controls the working environment and makes available many system management tasks. The CP then invokes the CMS component or another operating system to assist with the processing.

As mentioned earlier, the CP schedules and dispatches real processor resources through the use of internal lists. These lists (known as the dormant list, the eligible list, and the dispatch list) are used by the CP to allocate system resources. The dormant list is a list of virtual machines that are not eligible to execute. The eligible list is for virtual machines that are ready to be placed on the dispatch list. The dispatch list is a list of the virtual machines that are active on the system. The CP distributes real processor control on availability of virtual processors on the dispatch list and their internal dispatching priority among the other virtual processors on the list. In this way, the CP is able to ensure that an ample number of virtual machines are available for use. Other functions of the CP are to keep track of currently available pageable real storage and to handle real machine interrupts.

2.4 Conversational Monitor System

The Conversational Monitor System (CMS) was originally designed to support other operating systems. It has developed into an interactive tool that enables users to perform such activities as the following:

- Writing, testing, and debugging applications that will run on guest systems
- Running applications developed on guest systems
- Creating and editing data
- Processing batch jobs
- Communicating with other system users

CMS not only has its own set of commands but also its own Graphical User Interface (GUI) that can be used to create VM/ESA object-based programming applications. It should be noted that in order for a user to be able to execute commands, the user must meet one of the authorization levels set under CMS.

2.4.1 CMS Files

All VM files have their own three-part identifier. The first part of the identifier is the **file name**. The second part is the **file type**. The third part is the **file mode**. These three file identifiers are often abbreviated as **fn**, **ft**, and **fm**.

The file name and the file type can be any combination of letters and numbers. Each can be no longer than eight characters. (Certain special characters can also be used.) File names usually describe the contents of the file and are easy to remember. The file mode is always a letter followed by a number. The **XEDIT** command can be used to create CMS files.

2.4.1.1 CMS Shared File System

In VM, data can be stored in the Shared File System (SFS) or on a minidisk. Depending on how the System Administrator sets up a system, a user may have SFS storage, minidisk storage, or the capability to use both types of storage. The **q** command is used to determine whether files are stored in an SFS file pool or on a minidisk. If a user has SFS storage, the System Administrator has enrolled the user in a file pool. A file pool is an amount of storage that is set aside to contain a user's work and the work of other users. If a user's files are stored on a minidisk, the user has an amount of storage in the computer set aside specifically for that user.

In SFS, a user is given a certain amount of space, a file space, to store files. The file spaces for many users are kept in an area of real disk storage called a file pool. Within file spaces, groups of related files can be organized into directories. When a System Administrator assigns a user to a file pool, one directory is set up for that user (a top directory). This top directory has as its name the userid followed by a period. The top directory can contain files. In addition to the top directory, a set of lower-level directories exists. Each of these directories may also contain files and other directories (up to eight levels of sub-directories). This file organization structure is called a **hierarchy** or **tree**. It resembles an upside down tree. The top directory is at the top, and lower-level directories branch out below it. Sub-directories may also contain files. To determine the location of files within the SFS, use CMS commands. These commands are described in the *IBM CMS Commands* manual.

2.4.1.2 CMS Pipelines

In addition to the above, CMS enables programmers to solve large program problems through the use of the facility known as CMS pipelines. A CMS pipeline is the process of dividing programs into smaller programs known as stages. The two types of stages are **built in** (supplied by CMS) and **user written** (written by a programmer using REXX). Stages together with their operands can be used to read, write, or manipulate data. Stages are generally connected in order to obtain a desired output. It should be noted, however, that the output of one stage is usually the input to another.

In order for a stage to be executed, a CMS **PIPE** command must be issued. Once a command is issued, the stage is first scanned by the CMS pipeline scanner for both logic and syntax errors. If errors are found during this process, a non-zero return code is issued and the stage is flushed by the machine. If no errors are encountered, the CMS pipeline dispatcher takes control of the stages and determines which ones are to be executed. Stages are not usually executed from front to back. Instead, the dispatcher determines which portions are to be executed using an internal priority scheme known as the commit level. Stages are processed starting with the lowest commit level, which is zero. Stages end in one of two ways. Either they successfully complete, or an error occurs and the stage is stopped.

2.5 REXX/VM

Restructured Extended Executor (REXX) is a 4th generation Virtual Machine (VM) programming language that also includes a language processor. REXX was designed to enable systems personnel to develop customized application programs and commands. REXX code is similar to PL/1. Because the programs are free formatted, the code can be written to enhance readability and understandability. REXX programs can contain CP, CMS, or XEDIT commands. (REXX programs that have a file type of EXEC usually contain CP and CMS commands, and REXX programs that contain XEDIT commands have a file type of XEDIT.)

As mentioned earlier, REXX functions as a language interpreter/processor. The primary function of the REXX interpreter is to scan and execute REXX programs. When a REXX program runs, its language processor reads each language statement from the source file and runs it one statement at a time. Languages that are not interpreted must be compiled into machine language (in separate files) before they can be run. To run a REXX program, the program's name is typed in on the console and the Enter key is pressed. Because advanced compilation of REXX programs is not necessary, program syntax errors can be easily identified and resolved. Programs are scanned from left to right and executed on a line-by-line (word-by-word) basis. Thus, whenever an error is encountered, the interpreter points directly to it.

2.6 Group Control System (Mini OS)

Group Control System (GCS) is a stripped down operating system (OS). It is often referred to as a mini OS. GCS runs in a virtual machine in place of CMS. GCS, with its common and private areas, forms a base for a particular group of virtual machines. It runs parallel to CMS as a VM/ESA component on the CP. GCS supports the following communications:

- Task to task within a virtual machine
- Task to task in different virtual machines within the group
- GCS virtual machine to a virtual machine outside the group

This communication is accomplished by using the GCS IUCV or APPC/VM support or GCS services that use the CP Signal System Service. For communications between virtual machines within the group or outside the group, applications should use the APPC/VM protocol and services.

The GCS support macros IUCVINI and IUCVCOM must be used by applications that want to communicate using GCS IUCV or APPC/VM services. The IUCVINI macro initializes, alters, or terminates a user's GCS IUCV or APPC/VM environment. The IUCVCOM macro must be used to establish or terminate an IUCV or APPC/VM path for all GCS support users. This allows GCS task termination to sever any IUCV or APPC/VM paths that may have been left by a terminating task.

An authorized application may use IUCV or APPC/VM directly by issuing the function directly to the CP, rather than going through GCS through the IUCVCOM macro for all functions other than connect or sever. This is accomplished by specifying **PRIV=YES** when initializing the GCS IUCV or APPC/VM environment with the IUCVINI macro. All unauthorized GCS IUCV or APPC/VM users must use the IUCVCOM macro for GCS communications.

GCS also can communicate with other members of the group by using the CP Signal System Service. A virtual machine joins a group when the GCS supervisor is IPLed. At initialization time, GCS will issue an IUCV Declare Buffer and an IUCV CONNECT to the Signal System Service. The connection is made by specifying ***SIGNAL** as the userid and indicating that parameter list data will be used (**PRMDATA=YES**). Only one connection is allowed to the Signal System Service per virtual machine.

When a source virtual machine determines that it needs to communicate with a target virtual machine in the group, GCS places information describing the request for service into a read/write common storage area and chains it into a queue of requests for the target virtual machine. The source virtual machine then issues an IUCV SEND to the Signal System Service specifying an 8-byte parameter list of data and the target virtual machine's signal ID. This signal ID was assigned at initialization time. When the SEND is issued, the CP generates an external interrupt to be queued for the target virtual machine. The next time the target virtual machine is dispatched by the CP and is enabled for interrupts, it processes the request. The request is then processed by the IUCV interrupt handler. The GCS IUCV interrupt handler identifies the interrupt as one from the Signal System Service, and sends the request to the appropriate second-level interrupt handler to be processed. This method of communication allows all the virtual machines in the group to communicate on only one IUCV path.

Several GCS services use the Signal System Service for communication. One is to allow for cross-machine lock synchronization. If two virtual machines want to access the same resource, they can obtain the common lock. This is done by using the LOCKWD service in GCS. When a requested lock is released, LOCKWD uses the Signal System Service to notify any waiting virtual machines in the group that the lock is now available.

GCS also uses the Signal System Service to allow for cross-machine exits. One virtual machine can schedule an exit to run on another virtual machine. This is done by using the GCS SCHEDEX function. SCHEDEX uses the Signal System Service to generate the external interrupt on the target virtual machine.

The Signal System Service is also used by the CP to notify members of a group when one of the virtual machines leaves that group. As part of the virtual machine reset process, the CP will issue an IUCV SEND to all of the remaining members of the group. The IUCV SEND generates a signal-out external interrupt and the departing virtual machines signal ID. The signal-out external interrupt is used by the virtual machine designated as the recovery machine. The recovery machine runs machine termination exits and does any necessary cleanup.

GCS may appear to offer some of the services offered by IBM's OS/390 system. There are similarities between the two, but there are also some very significant differences in function and use. GCS provides multitasking services that allow numerous tasks to remain active in the virtual machine at one time.

GCS supports the following applications:

VTAM (Virtual Telecommunications Access Method)

The specific version of VTAM designed for GCS is ACF/VTAM, Version 3.3 (for VM/ESA). ACF/VTAM controls data flow between SNA network devices and programs running in other group machines. Part of ACF/VTAM provides a shared VTAM interface through which other program products (such as RSCS [Remote Spooling Communications Subsystem], NCCF [Network Communications Control Facility], and NetView) pass information. RSCS uses this shared VTAM interface to communicate with SNA devices, NCCF, and NetView to perform network management functions. For more information, see the *ACF/VTAM General Information (for VM)* manual.

VSCS (VTAM SNA Console Support)

This is a VTAM component that lets SNA-connected terminals function as virtual machine consoles. VSCS succeeds the earlier VM/VCNA product, and makes a guest System Control Program (SCP) (such as VSE or VS1) unnecessary. For more information, see the *ACF/VTAM General Information (for VM)* manual.

SSP (Systems Support Program)

With GCS, parts of SSP are VTAM subtasks. SSP does utility functions for the SNA network's communication control unit. SSP aids the Network Control Program (NCP), which governs the communication control unit. That control unit, in turn, manages network lines and routing of data. For more information, see the *ACF/VTAM Network Program Products Planning* manual.

AVS (APPC/VM VTAM Support)

AVS is a VM/ESA-supplied VTAM application that runs in a GCS virtual machine. It provides the functions necessary for APPC/VM programs within a TSAF collection to communicate with APPC programs anywhere in an SNA network. VTAM provides the LU 6.2 services necessary to communicate with a remote LU. AVS handles the transformation between APPC/VTAM and APPC/VM. AVS can coexist with VSCS in the same system, GCS group, and virtual machine. For more information, see the *VM/ESA: Connectivity Planning, Administration, and Operation* manual.

RSCS (Remote Spooling Communications Subsystem)

RSCS, designed as a GCS application, runs in a group virtual machine and relies on ACF/VTAM to help transfer information through the SNA network. RSCS also can run in a group by itself, spooling files and transmitting messages through non-SNA links. For more information, see the *RSCS Networking General Information* manual.

NetView

NetView is an enhanced network management program. It is an optional but recommended VTAM application that helps in the operation and control of a SNA network. It permits the network operator to control any portion of the network regardless of its physical location. NetView includes the function of the network management products that are also supported by GCS. For more information, see the *ACF/VTAM Network Program Products Planning* manual.

2.6.1 GCS Groups

GCS governs group machines. A group is one or more virtual machines that have IPLed the same GCS shared segment. A virtual machine group is an extension to the current virtual machine supported by the CP, which allows several virtual machines to be in a common group and controlled by a common supervisor. One of the primary reasons for having groups of virtual machines is to gain performance in communication. This is accomplished by GCS services such as common storage, Inter-User Communication Vehicle (IUCV), APPC/VM, and the CP Signal System Service. More than one group may be active at any given time in a single processor.

Virtual machine groups can consist of multiple user groups or single user groups. Multiple-user groups share common storage space and a supervisor, and can communicate with each other. Single-user groups do not need to share storage space or supervisor because there are no other machines in the group, and they do not need to have the ability to communicate with other machines in a group. Therefore, applications that do not require group communication are able to IPL and run without the overhead of group initialization and multiple virtual machines. In a single-user group, the user authorization is initialized as specified in the configuration file. The user may change the authorization by using the AUTHUSER parameter of the **CONFIG** command.

Groups are defined at installation time. GCS group information is defined in the configuration file that resides in GCS private storage. Some of the information contained in that file is as follows:

- Supervisor name
- Maximum group size
- Names of other shared segments (such as VTAM and others)
- Location of the internal trace table
- Userids that will be accessing the VSAM segment
- Userids of machines authorized to run in supervisor state
- Userid of the recovery machine that is used to clean up group resources when other machines leave the group

GCS is the base that holds the group together and the supervisor that provides many services for each member machine. The type of services available depends on the authorization of individual group members. Unauthorized members run only in problem state and are prevented from using certain GCS services. Authorized members can run in supervisor state and use more GCS services.

After building the configuration file and installing it in the GCS segment, the GCS supervisor admits machines that IPL the shared segment, by name, into the group. On a single VM/ESA system, a user can build multiple GCS segments and multiple virtual machine groups. After installing GCS and defining it as a named, saved system, userids can IPL it and share a group copy of the GCS shared segment if the segment was not defined as restricted. Those userids then share access to GCS supervisor code and common storage. If the segment was defined as restricted, the user needs to put a NAMESAVE control statement in the directory to IPL it. To join a virtual machine group, log on and IPL the GCS shared segment.

A GCS shared segment is declared using the **DEFSYS** command with the VMGROUP parameter. When a GCS segment is built, the CP does not check for changes in the virtual machines that access the GCS segment. The CP is notified that any virtual machine that IPLs this named segment will be running in a virtual machine group. The common storage is described in the **DEFSYS** command with the SW descriptor code. This allows the pages of this segment to be altered by any authorized program in the group. GCS has been structured to run in such an unprotected shared segment to gain the advantages of common storage, fast communication between virtual machines, and less dispatching overhead for better system performance. Protect areas of these segments that require protection with storage keys.

GCS provides protection for both the system and its applications by authorities. There are methods for controlling the execution of programs and the protection of data. In GCS, applications may be either authorized or unauthorized. An authorized application will run in supervisor state and has the power to process authorized GCS functions. Unauthorized applications run in problem state and cannot access these authorized functions (except when they are provided access from an authorized application).

The three types of authorization in GCS are listed below:

- **Virtual Machine**

  A virtual machine is authorized when its userid is entered at build time using the GCS GROUP EXEC. When an authorized userid is IPLed, its applications process in supervisor state. Therefore, a program executing in that virtual machine is authorized and may process both authorized and unauthorized programs.

- **Task**

  When a GCS task is authorized, the programs running under that task are executing in supervisor state. This happens when the task is authorized using the SM=SUPV parameter on the ATTACH macro.

- **Entry Point**

  An authorized entry point can be created using the AUTHNAME macro. This entry point must reside in the GCS shared segment. An authorized application can make this entry point available to unauthorized applications by using AUTHNAME. This declares the entry point

(and name) to GCS so unauthorized applications can run it by using the AUTHCALL macro from any virtual machine in the group. When the AUTHCALL macro is called by an unauthorized program, the authorized entry will be given control in supervisor state (authorized). When it returns control to the unauthorized program, problem (unauthorized) state is restored. In this way, authorized applications can provide unauthorized applications a controlled means of accessing authorized functions.

2.7 Transparent Services Access Facility

Transparent Services Access Facility (TSAF) runs in a CMS virtual machine. It serves as both a collection manager and a communications link manager. Up to eight VM systems (known as a TSAF collection) can use TSAF to exchange information about the resources. Global resources are known throughout the collection, and their names are unique within a collection. Userids uniquely identify a particular user. For programs in a TSAF collection to communicate, a logical connection must be established between the programs. Within a single VM system, the CP provides an APPC/VM path that logically connects two programs. Within a TSAF collection, the CP provides an APPC/VM path that connects each program with the TSAF virtual machine on its system. The TSAF virtual machines provide a logical APPC/VM path (a communications link) between the two systems, which lets the programs communicate.

Whenever the CP is unable to find a resource in the CP's resource table, a request is forwarded to TSAF to locate the resource. TSAF then locates the resource and sends the request on to its destination. If the resource is a global resource, TSAF routes the information by resource name. If the resource is a private resource, the information is routed by userid. A major benefit of TSAF is that this exchange of information is transparent to application programs. Communications between the application programs proceed as if the applications were running on the same virtual machine. Installation of TSAF is optional.

2.8 APPC/VM VTAM Support

APPC/VM is a VTAM programming interface that VM uses for communication within a single system or a collection of systems. With AVS, an APPC/VM program in a collection of VM systems can connect to APPC programs in the SNA network. Also, APPC programs in the SNA network can access global and private resources on VM. AVS runs in a GCS group and requires Advanced Communications Function for Virtual Telecommunications Access Method (ACF/VTAM) to communicate with an SNA network.

The APPC/VM VTAM Support (AVS) component, along with VTAM, lets users in a single VM system or in a VM system in a TSAF collection communicate with resources using the APPC (LU 6.2) protocol.

2.9 Virtual Machine Serviceability Enhancements Staged/Extended (VMSES/E)

VMSES/E is used to install VM/ESA and other VMSES/E-enabled products and to apply code changes that correct or circumvent reported problems. VMSES/E handles both source code and object code. VMSES/E also helps define, build, and manage saved segments. VMSES/E consists of two user interfaces (the VMFINS and VMFSIM EXECs), enhanced service execs (e.g., VMFREC and VMFBLD), and the system-level and service-level Software Inventories.

VMSES/E provides the following functions:

- An exec for installing, migrating, building, and deleting products
- Execs for receiving service, applying service, and building the serviced usable forms
- Files to direct the operation of these execs and to save the status of their execution
- Software Inventory that stores information on the status of installed products
- Program Temporary Fixes (PTFs) applied to products
- Requisite relationships among products and PTFs
- Information about managing saved segments
- An exec for managing saved segments
- A database structure that isolates executable code from the control structure used to manage it

The supporting structure for saved segments in VMSES/E is described in the *VM/ESA: Planning and Administration* manual in *Part 3, "Servicing Products,"* in *Topic 3.0* and *Part 4, "Planning and Managing Your Software Inventories,"* in *Topic 4.0*.

The VMFINS EXEC is used to install products. The VMFINS EXEC can also be used to migrate products while keeping previously tailored files, build products, update the Software Inventory tables, and delete products no longer needed on the system. The VMFINS EXEC provides a planning option to help check product requisites and resource requirements before installing, migrating, and deleting products. The VMFINS planning option allows for specifying the installation location for a product, and specifying installation related parameters. The VMFINS EXEC can process products from installation tapes formatted for VMSES/E, or a VM/ESA System Delivery Offering. The command syntax for the VMFINS EXEC is consistent across functions, yet flexible, to provide for ease-of-use and personal preference in how a task is completed. The VMSES/E EXECS (VMFREC, VMFAPPLY, and VMFBLD) are used to service products. For more information on servicing products with VMSES/E, see the *VM/ESA: Planning and Administration* manual, *Part 3, "Servicing Products,"* in *Topic 3.0.*

The VMFSGMAP EXEC provides a saved segment mapping interface that allows the modification of saved segment definitions and viewing of the saved segment layouts prior to actually building them on a system. The VMFSGMAP EXEC is a saved segment mapping and management interface. VMFSGMAP provides a full-screen segment map that shows the saved segments defined on a system and in the Software Inventory. Using VMFSGMAP, saved segment definitions can be changed, added, and deleted, and the results can be displayed. Then the VMFBLD EXEC can be used to build or delete the saved segments.

The VMFSIM EXEC is the interface between the Systems Programmer and the system-level and service-level Software Inventories. When using VMFINS to install products in VMSES/E format, the product installation defaults that have been provided for each product by IBM can be overridden. The Make Override Panel shows the default minidisks, userids, or Shared File System directories that will be used when the product is installed, unless they are overridden.

2.9.1 VMSES/E Software Inventory

The Software Inventory contains control and status information that is used when products are installed, migrated, built, deleted, and serviced. The service-level Software Inventory contains information on the service applied to each product on the system, if it is serviced with VMSES/E. The Software Inventory information resides in a series of tables on the Software Inventory minidisk or Shared File System directory. VMFSIM is used to manage the Software Inventories on the system. The VMFSIM EXEC creates and updates the Software Inventory and provides queries so that the status of products and service can be reviewed. When the VMFINS **INSTALL** command with the ADD option is used to install products, the VMSES/E product management files, the product parameter files, and the PRODPART files are loaded from the product tape to the Software Inventory disk.

2.10 Dump Viewing Facility

The Dump Viewing Facility is an interactive tool that is used in problem determination and resolution. The Dump Viewing Facility enables a Systems Programmer to interactively dump data, format and print dumps, reduce trace tables created by trace service tools, and recognize duplicate problems. The types of dumps that can be processed vary from VM (which includes CMS and GCS) and CP dumps. The Dump Viewing Facility provides a variety of commands and subcommands that enable a Systems Programmer to locate dump data and display the needed information in a format that is easily used. Such information as control blocks, control block chained, registers (including vector registers), load maps, entry point locations, trace tables and data can be displayed. The Dump Viewing Facility displays information in Extended Binary Coded Decimal Interchange Code (EBCDIC), hexadecimal.

Whenever a problem occurs, a symptom record is produced with a dump. The dumps can be stand-alone dumps and soft abend or snap dumps. In order for the Dump Viewing Facility to process the dump, it must be stored on disk or tape. It should be noted that the Dump Viewing Facility can be used to direct the dump to a printer on a virtual machine. When an abend occurs, the CP commands **VMDUMP** or **SNAPDUMP** are used to produce the dump. Once the dump is created the **DUMPLOAD** command is used to load the dump into a CMS file. Then the **VIEWSYM** or **INSPECT** commands can be used to display diagnostic information. The BLOCKDEF utility can also be used to display, format, and print control block information. IPCSDUMP can also be used to process and analyze dumps.

This page is intentionally left blank.

3. VM INTEGRITY

The integrity of the VM environment consists of securing the system-level processes and the data-level processes. The following sections discuss each of these in detail.

3.1 System-level Integrity

System-level integrity consists of protecting hardware and software resources.

3.1.1 Hardware Integrity

Every operating environment is composed of hardware resources. These include facilities such as the central processing units (CPUs), direct access storage devices (DASDs), tapes, consoles, printers, and communications devices.

When handled improperly, these components can create exposures within the operating environment that cannot be controlled with any software process. As an example, the CPU service console provides facilities where memory in the CPU can be displayed and altered. If access to this facility is not restricted, the exposure exists that memory could be altered. This could result in outages or access to data without proper authorization.

As another example, equipment manufacturers and service technicians generally have facilities that allow local (or dial-up) access to a service facility so diagnostics can be run if equipment problems occur. Data can potentially be accessed and/or destroyed by personnel who are not qualified or who cannot be trusted to perform such diagnostics.

Printout presents a significant exposure if the information is not handled in accordance with applicable regulations. The information on output media (e.g., fiche or paper) must be properly safeguarded.

This document is not intended to address the resolution of the integrity of the hardware environment. Access controls must be designed and implemented as part of the physical security plan for the site. The concept of Identification and Authorization (I&A) is the principal mechanism for controlling these resources. One example of such a process is a card key system that provides both identification and a code number for authentication.

DISA Instruction 630-230-19 and the *DISA Computing Services Security Handbook* provide further guidance on the proper protection of the physical environment.

3.1.2 Software Integrity

IBM has created a formal integrity statement that defines the integrity philosophy of the operating system. Controlling potential integrity exposures is the responsibility of the Systems Programmer. As such, standards have been developed to limit the exposure potential for each of the operating system elements.

The IBM manual, *VM Planning and Administration: Security, SC24-5750-03, Chapter 13, Version 2.4,* lists several areas of concern regarding the integrity of a VM operating system.

A product usually does not harm a system's integrity if the product does the following:

- Uses only authorized and non-restricted VM interfaces
- Uses guest operating system security to control resources
- Does not modify VM in some way

A product that performs any of the following actions, however, could introduce a system integrity exposure:

- Obtains control in real supervisor state without privilege class authority or directory capabilities greater than assigned.

- Uses the CP to circumvent the system integrity of any guest operating system that has system integrity.

- Circumvents VM/ESA main storage protection or auxiliary storage protection.

- Accesses, without authority, a VM/ESA password-protected resource.

- Accesses, without authority, a resource protected by an ESM.

If any of the above conditions is true, then the possibility exists that installing the product on VM could introduce system integrity exposures. In such cases, follow the IBM system integrity guidelines to ensure that exposures are not created.

Areas of critical importance to VM integrity, and the steps required to secure each of them, are discussed below.

To facilitate maintaining system integrity, use the following guidelines:

(1) Install and maintain all products with the capability for installation via IBM's Virtual Machine Serviceability Enhancements Staged/Extended (VMSES/E) process. This will ensure proper control and tracking of maintenance and changes.

(2) Install products not capable of installation using VMSES/E and the methodology recommended by the vendor. However, for these products it is especially critical that change control mechanisms are strictly enforced, as their effect on the operating environment will not be recognized by VMSES/E.

(3) Install and maintain any modification or ACI to the CP, or to products that act as extensions of the CP or CMS (e.g., the ACP or a tape management system) using VMSES/E.

(4) The sites (Defense Enterprise Computing Centers) will use VMSES/E to install and maintain all DISA standard products approved, released, or supported by the SSO.

(5) Ensure that VMSES/E is available at the local site level for the installation of non-SSO supported products and for COOP (Continuity of Operations Plan) purposes.

(6) Test all products for security impacts in a test environment before being authorized for production, and correct any deficiencies.

(7) Integrity assurances are required and will be obtained for any products or applications that require or provide CP and CMS Access Control Interfaces, commands, utilities, or any other modifications to the CP. This requirement may be satisfied by either of the following:

(a) DISA will obtain a Vendor Integrity Statement (VIS) from the vendor of the product. The DISA Field Security Operations Technical Library will centrally maintain the VIS.

(b) Obtain the written approval of DISA Field Security Operations to install and use the product, application, or system modification. This requires submitting (prior to installation) the following items to Field Security Operations for analysis and review:

- Documentation describing the product or application
- Documentation and source code for the system modification

(8) Any locally-developed extension to the CP or CMS (e.g., utilities, commands, etc.) requires the following:

(a) Advance written approval of the concept by Field Security Operations before its development.

(b) Review and written approval of the concept's implementation by Field Security Operations before installation and utilization. This requires submitting documentation and source code for the local system modification to Field Security Operations for analysis and review.

Field Security Operations will provide responses to (a) and (b) above within 30 days of receipt of each request.

3.1.2.1 Privilege Classes

A class is the categorization of a user by job, function, and responsibilities. In a VM/ESA environment, privilege classes are used to control the level of access a command, utility, program, or user has with the system software, and to identify which VM/ESA commands and DIAGNOSE codes may be used. A user can be assigned to one or more privilege classes. If a user attempts to issue commands that are outside of that user's privilege class assignment, the system ignores the commands.

IBM has determined that there can be up to a maximum of 32 privilege classes. They are labeled **A-Z** and **1-6** or with the word **any**. There are times that the class structure, as distributed with the system, are inadequate to meet the needs of a site. When that occurs, special user privilege classes can be defined by using the CP OVERRIDE utility to create a class override file. The class override file is a fixed format file made up of control statements that override either the PRIV_CLASSES system configuration file statement or the SYSFGN macro instruction in the **HCPSYS ASSEMBLE** file. For a description of the standard class structure, see the *IBM VM/ESA Planning and Administration Manual, SC24-5750-03, Chapter 28.*

Use the following standards and techniques to control privilege classes:

(1) The Software Support organization and the sites will maintain all privilege classes. Before any changes are made to this file, create a copy of the previous version with a name as specified in the *DISA Computing Services Naming Convention Standards*.

- *The local IAO will document and maintain any deviations from this standard.*
- ***Privilege command classes** will be established*

(2) Establish user privilege classes on an as-needed basis in accordance with DISA standards.

(3) On a semi-annual basis, Software Support will review all privilege user classes and will verify that they follow requirements as determined by DISA. Software Support will remove all unauthorized user classes. The IAO will ensure that modification/deletion is in accordance with DISA standards.

(4) The IAO will implement controls to specify the valid users authorized to create and modify privilege user classes. Only systems programming personnel will be authorized to create, modify, and delete privilege user classes.

(5) The IAO will maintain the privilege user class requirements (e.g., *DISA Form 41s*), and will maintain and review the ACP logging reports.

- *The **DIAG98** operand on the **OPTION** statement will not be enabled for any userid*
- *The **DIAGNOSE code X'08'** will be restricted in the User Directory.*
- *The **D8ONECMD** directory statement will be coded for server virtual machines.*
- *The **OVERRIDE utility** will be restricted to authorized personnel and audited*
- *The **FEATURES statement** in the System Configuration file will have the SET PRIV class option enabled.*
- *The **privileged class C** will be restricted to authorized personnel.*
- *The automatic generation of system definition files, using the utilities:* **HCPDCON, HCPDSYS, and HCPRDEVS,** *will be restricted to authorized users.*
- *The FEATURES statement in the System Configuration file will have **CLEAR_Tdisk** enabled.*
- *The FEATURES statement in the System Configuration file will have **PASSWORDS_ON_CMDs** for **Autolog, Link and Logon** coded "No" or omitted ("No is the default value).*
- *The CPXLoad statement will not be coded in the System Configuration file.*
- *If the CPXLoad statement is used in the System Configuration file, the file will be restricted to authorized personnel and audited.*
- *The IAO will ensure that modification/deletion to privilege user classes is in accordance with DISA standards.*
- *The IAO will implement controls to specify the valid users authorized to create and modify privilege user classes.*
- *The IAO will maintain the privilege user class requirements*

3.1.2.2 VM and Other Product Routines

VM and many other products provide routines that can be used to perform additional processing for an installation. Examples of these system-level routines are CMS, Auditing, and ESM. Some of these routines have the potential to open integrity exposures since the code may be entered in a privileged mode. Every exit point used within a product (especially VM) needs to be validated so the code does not bypass the integrity of the operating environment.

Complete the following steps to maintain the integrity of the system:

(1) Document all exit points used. Provide this to the IAO for backup documentation purposes.

(2) Using the ACP, protect the minidisks associated with all products installed in the VM environment. This reduces the potential of an unauthorized person adding a routine to a library and possibly creating an exposure.

(3) Track all exits using VMSES/E. Develop usermods to include the source/object code used to support the exit.

(4) Systems programming personnel will review all VM and other product exits to confirm that the exits are required and are correctly installed.

(5) All *update* and *alter* access to system files containing VM and other system-level exits will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the files containing VM and other system-level exits. The IAO will maintain the access requirements (e.g., *DISA Form 41s*), and will maintain and review the ACP logging reports.

Refer to the *OS/390 STIG, Section 3.1.2, Software Integrity*, for information on integrity statement requirements.

- *The IAO will ensure that the mini disk containing the User Directory is password protected.*

3.1.2.3 Access Control Product Exits

The ACPs themselves present some of the greatest exposures. The three products mentioned in this document (ACF2, RACF, and TOP SECRET) have been evaluated by the National Security Agency (NSA) to support the criteria for a MAC II Sensitive security rating. Each ACP allows installation exit points that can be used to support additional security-related requirements for a site. One example of such an exit is a password validation exit program restricting the contents of a password.

Installations use these exits to force algorithms, such as the following:

- A numeric must exist in a certain location.
- The user's name cannot be used.

Use of an exit within the ACP does not reduce the assurance category of the product, provided changes to the actual MAC II Sensitive criteria have not been introduced. The process for controlling ACP exits is as follows:

(1) DISA Field Security Operations must approve the use of any ACP exit. Use of any exit without this approval is prohibited. All code will be provided to this organization for review.

(2) DISA Field Security Operations will review the exit for use and integrity, and will evaluate the need for such an exit across all VM platforms. If deemed a viable process, steps will be taken to prepare the exit for distribution to applicable sites.

(3) Where applicable, control all ACP exits via VMSES/E to ensure accurate tracking of the installation and maintenance of the exits.

(4) Systems programming personnel will review all ACP exits to confirm that the exits are required and are correctly installed.

(5) All *update* and *alter* access to system files containing ACP exits will be logged using the ACP's facilities. Only systems programming personnel will be authorized to update the files containing ACP exits. The IAO will maintain the access requirements (e.g., *DISA Form 41s*), and will maintain and review the ACP logging reports.

Refer to *Section 3.1.2, Software Integrity*, in this document for information on integrity statement requirements.

3.1.2.4 VM Data Collection

For systems rated MAC II Sensitive and above, *DODI 8500.2* mandates that audit data be maintained for security and security-related events to ensure individual user accountability. Audit data presents a critical component in providing the required audit trails to maintain VM system integrity. All relevant audit data will be collected and retained for at least one year to ensure that adequate audit trails are available.

- *The **Journaling** option will be turned on in the System Configuration file.*

3.1.3 Object Reuse

Within the criteria for achieving MAC II Sensitive compliance, a requirement exists for ensuring the integrity of an object when reused. According to *A Guide to Understanding Object Reuse in Trusted Systems, NCSC-TG-018*, a definition of object reuse is "… to prevent a user who is allocated storage from accessing information put there by a previous user." *DoDD 8500.1* does not specify how object reuse requirements are to be technically implemented, but allows the system flexibility in meeting the requirement.

To meet the criteria for the entire operating environment, the use of an automatic erasing facility is required since the operating system itself cannot provide this level of integrity. However, the use of such a facility can cause considerable system overhead in actually erasing the data from a device. Additionally, such a tool cannot erase data from magnetic tape media or from other removable media, thus requiring additional physical security controls.

3.1.3.1 Unclassified Systems

The Chief Information Officer (CIO) has granted an exemption from the object reuse requirement for unclassified systems. For these systems the automatic ERASE option within the ACP may be disabled. Optionally, the site may enable the option if so dictated by customer requirements.

The customer community must determine the sensitivity of their data according to applicable policies and regulations, and must submit their object reuse requirements to the site. The site is responsible for providing the means by which the requirement is then met.

The sites must determine their object reuse requirements and provide the mechanisms to ensure the requirements are met. For systems processing **unclassified** and **sensitive but unclassified** data, DISA will provide solutions allowing the sites to meet the object reuse requirements for identified sensitive files.

The site should consider optionally protecting some of its own sensitive data with automatic erasure. As an example, the following files would be candidates for object reuse protection:

- Accounting data
- Any file possessing information
- Security audit data and reports
- All billing-related data

3.1.3.2 Classified Systems

For any system that processes classified information, object reuse requirements will be met by enabling the automatic ERASE option within the ACP. This will ensure that all DASD data is overwritten as files are deleted.

Any data on removable media (reel tape, tape cartridges, diskettes, etc.) must be handled manually using approved degaussing procedures. For information regarding approved degaussers, consult the current *NCSC Evaluated Products List*.

The use of Redundant Array of Inexpensive Disks (RAID) technology presents a special problem to classified processing. Not all implementations of RAID technology support automatic, in-place erasure and destruction of data. Some implementations simply change table pointers and recover the storage locations for reuse, without destroying the stored data.

It is likely that as RAID technology advances, methods for recovering the data will be developed to recover inadvertently *deleted* data. Such methods would enable the recovery of any data not destroyed in place, potentially compromising the information. For these reasons, only those implementations of RAID technology that support the automatic erasure features of the ACPs and perform in-place destruction of stored data will be used on classified systems.

3.1.4 Auditing

In an effort to minimize the risks inherent with the VM environment, DISA has directed that a process be developed and implemented to identify the potential exposures presented by VM, and that measures be taken to ensure that the system's integrity is not compromised.

As part of the requirement to review VM, documentation supporting the performance of a review will also be maintained by the site.

3.1.4.1 Review and Documentation Requirements

DISA requires that all locally written exits or modifications to the operating system, or products that act as extensions to the operating system, be provided to DISA Field Security Operations for analysis and approval *prior to installation in a production environment*.

Vendor software will be accepted as **trusted**, providing DISA Field Security Operations has a Vendor Integrity Statement (VIS) on file. When a VIS is not obtainable, source code for the vendor-supplied software should be obtained and submitted to DISA Field Security Operations for an integrity analysis.

Refer to *Section 3.1.2, Software Integrity*, in this document for information on integrity statement requirements.

3.2 Data-level Integrity

The concept of data-level integrity involves the protection of actual data loaded on the system. Data-level integrity is composed of **data integrity** and **data labels**.

DISAI 630-230-19 provides the concepts to be used in evaluating the data integrity requirements supporting application data. This *VM STIG* is not intended to address data-level integrity in detail, but to provide techniques that can be used to ensure security of the data residing under the control of VM.

3.3 Control Requirements

File controls play a critical role in maintaining the integrity of VM systems. Several key areas of control requirements are discussed in the following sections.

3.3.1 File Integrity

File integrity is a key factor in the protection of VM systems. Critical system files that must be protected include, but are not limited to, the following:

- System directory files
- System files (including VM files [e.g., CP, GCS, CMS], system-level product files, and VM and product installation files [e.g., VMSES/E])
- Access Control Product files and databases
- System and subsystem trace files
- System dump files
- Logs
- Backups, dumps, and off-loads of the above

Enforce control restrictions for these files to ensure that (1) only those routines or users with a legitimate need are granted access, and (2) the access granted is restricted to the minimum level necessary. For example, DASD management routines should have access to backup files, and systems programming personnel should have access to system dump files.

- *The VM System Configuration file will be **read** and **write** protected.*
- *The alternate System Configuration file will be **read** and **write** protected.*

3.3.2 File Location

File location is an often-overlooked factor in system integrity. It is important to ensure that the effects of hardware failures on system integrity and availability are minimized. Avoid collocation of files such as primary and alternate databases. For example, the loss of the physical volume containing the ACP database should not also cause the loss of the ACP backup database as a result of their collocation. Files that must be segregated from each other on separate physical volumes include, but are not limited to, the ACP database and its alternate or backup file.

3.3.3 File Backup

Adequate backup scheduling is also an often overlooked integrity exposure. Back up system backup files on a regular schedule. Store the backups off-site to prevent concurrent loss of the live production system and the backup files. Backup scheduling will vary depending on the requirements and capabilities of the individual data center.

While the requirements of data owners may necessitate more frequent backups, a recommended schedule is as follows:

- Weekly and monthly full-volume backup of volumes with low update activity, such as the operating system volumes

- Nightly backup of high *update* activity files and volumes, such as application system databases and user data volumes

- At a minimum, nightly backup of the ACP databases, and of other critical security files (such as the ACP parameter file). More frequent backups (two or three times daily) will reduce the time necessary to effect recovery. The IAO will verify that the backup job(s) ran successfully.

- *The spool file will be backed up on a regularly-scheduled basis.*

3.3.4 File Recovery

The logical complement to adequate backup of data is to have a written, verified, and regularly practiced recovery procedure for each manner of backup. Responsible personnel should have timely and adequate access to the recovery procedures, and should be thoroughly experienced in their execution to lessen the impact of recovery.

3.4 Password Files

Access to minidisks on VM systems can be protected using the MDISK password capability. This capability has been available in VM for many years, and its use is commonly found in data centers. With the use of ACPs, the need for passwords for file protection has diminished. The use of VM passwords is not supported by all of the ACPs.

3.5 Banner Pages

The Session Manager will display a logon banner to the user according to the requirements mandated in *DISAI 630-230-19* and the *DISA Computing Services Security Handbook*.

4. EXTERNAL SECURITY MANAGER IMPLEMENTATION

4.1 General Considerations

The External Security Manager (ESM), in conjunction with the User Directory, is the primary mechanism that controls access to data and resources in VM systems. Each ESM in use on the DISA platforms provides the flexibility to tailor the implementation to meet the needs of the local installation.

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

The installation and implementation of each ESM should be standardized across all DISA processing environments. DISA standard implementation criteria are specified in the individual ESM installation sections of this document.

Any deviation from these standards will be coordinated with and authorized by DISA Field Security Operations. All deviations will be specifically noted, with justification and approval documentation, in the system security plan and the accreditation package submitted to the DISA Designated Accreditation Authority (DAA).

4.1.1 Standard Global Options

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 when not properly applied.

In an organization as large as DISA, the additional complication of diversity exists. Many different applications of the global options exist. 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 virtually impossible.

For the above reasons, and to mitigate the above risks and difficulties, all DISA processing environments will implement standard global options for each ESM installed. The DISA standard options are specified in the individual External Security Manager Product installation sections of this document.

4.1.2 Userid Controls

DOD policy requires that each system user is uniquely identified to the operating environment, and that access to resources is limited to those needed to perform their 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 VM systems a user is identified by means of a unique userid. For systems rated MAC II Sensitive, *DODI 8500.2* together with other audit documentation, mandates that audit data be maintained for security and other related events to ensure individual user accountability.

It then follows that any userid (user) on the system must be associated with only one individual. It also follows, however, that any given individual may be assigned responsibility for multiple userids on a given system, depending on functional responsibilities, to ensure task segregation. The following sections discuss the requirements for each type of user and the elements that will be considered in defining user access.

4.1.2.1 Interactive Users

To achieve compliance with the criteria mandated for MAC II Sensitive, all personnel will identify themselves to the system before access to resources is granted. A means to authenticate the user's identity (e.g., passwords) will be used. *DISAI 630-230-19* provides the policy regarding general user access. Each user of resources will be defined using ESM facilities to control I&A.

The standard process used in the sites consists of a userid and a password, which together enable the user to access the system. The IAO controls access to computing resources and adds additional functions to a userid.

When entering a VM system, the user must use a Session Manager.

4.1.2.2 Batch Users

A major user of system resources is a batch job. A batch job is essentially a stand-alone task submitted to CP for processing. Batch jobs may be submitted in several ways. A user accessing the system through CMS or a similar facility may have the capability to submit batch jobs for execution. Each of these batch jobs should be identified to the system to designate the resources that should be available to the job. Each ESM allows the association of a userid with the job stream.

Batch jobs submitted to the operating system by a user (e.g., CMS) should inherit the userid of the submitter. This will identify the batch job with the user for accessing resources. Userid and password inheritance is the DISA standard method for batch jobs submitted by an interactive user.

Under no circumstance will user jobs inherit the authority associated with a virtual machine.

4.1.2.3 Special Storage Management Users

Every data center uses special jobs for maintenance processing that require more authority than any one user may be granted. Examples include jobs performing volume backups, file archiving, and restoration processes. Each ESM allows special privileges that may be assigned to a userid. Userids used for jobs that perform such functions will be processed using special privileged userids to avoid the assignment of all resources to a single userid.

Refer to *Section 4.2.6, Special Privilege Access,* for further information. Also, refer to the specific Access Control Product section on the methodology to be employed for this process.

4.1.2.4 Emergency Userids

In emergencies, the access necessary to perform a function may not be available to recovery personnel. To handle such emergencies, super IDs or **firecall** procedures will be available.

Use the following rules and conditions to handle these userids:

(1) One class of userids will exist to perform all operating system functions except ESM administration. These super IDs may be released according to DISA policy to effect repairs of the operating system in emergencies.

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

(3) Normally both super IDs will not 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 will be implemented with logging to provide an audit trail of their activities.

(5) Both classes of super IDs will be maintained in the ESM.

(6) Each super ID will have distinct, different passwords in the ESM, and the site will establish procedures to ensure that the passwords differ.

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

- *The IAO will ensure that a password is associated with the **MAINT** userid.*
- *The VMSES mini disk will be located under the **MAINT** userid and protected.*

4.1.2.5 VM System Operator Userids

To control entry of CP system commands in VM, apply the following standards when implementing security:

(1) Define each operator to the ESM as a user.

(2) At the discretion of the IAO, the operators' userids may be given privileges and profiles beyond those needed to log on and perform routine operational tasks.

- *The IAO will ensure that a password is associated with the OPER userid.*
- *The IAO will ensure that the mini disks associated with the OPER userid are password.*

4.1.3 Password Controls

Each ESM allows the specification of a password. Certain guidelines will be followed for password settings to ensure I&A criteria are in accordance with the *DISA Computing Services Security Handbook*.

- *The IAO will ensure that all userids have associated passwords on the User Directory*
- *The IAO will ensure that the mini disks associated with the **MAINT** userid are password protected.*
- *The IAO will ensure that all mini disks are password protected.*
- *The nucleus mini disk will be located under the **MAINT** userid on the User Catalog.*

4.1.3.1 DISA Password Guidelines

DODI 8500.2 requires that the ESM protect the authentication data (i.e., password) from access by an unauthorized user.

Industry analysis has shown that people are more likely to remember their passwords and not write them down if they are allowed to create their own. The most effective means is to allow users to select their own passwords, and to force certain guidelines regarding the composition of the passwords. Users will also change their passwords regularly. This reduces the possibility of a user’s password being acquired, and possibly used, by someone else.

After three consecutive password failures, the userid will be suspended until reset by the IAO, TASO (Terminal Area Security Officer), or other authorized personnel.

The following standards concerning password requirements are mandatory, and apply equally to both classified and unclassified systems:

(1) Passwords will be eight (8) characters in length.

(2) Passwords will 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 1: *For VMSecure the following special characters are valid for passwords:*

$
+
- (hyphen)
_ (underscore)

NOTE 2: *Lower case alphabetic characters are not supported by the ACPs.*

(3) Each character of the password will be unique, prohibiting the use of repeating characters.

(4) Passwords will contain no consecutive characters (e.g., 12, AB).

(5) Passwords will not include the user's name, telephone number, userid, or any standard dictionary word.

(6) Users will be required to change their password every 90 days at a minimum. Users are permitted to manage and change their own passwords.

(7) Passwords will not be changed more than once every 24 hours without the intervention of the IAO. (Refer to the *DISA Computing Services Security Handbook*.)

(8) Users will not be permitted to reuse a password assigned within the last ten password changes.

(9) The password file will be stored in encrypted form.

Password requirements will be enforced by standard security product controls where possible. Exits will only be used where the requirements cannot be enforced by standard security product controls. (Refer to *Section 4.1.3.2, Password Exit Processing,* for further information.)

NOTE: Adherence is required when the software has the capability to enforce. Otherwise the password policies not enforced by the software will be documented in the site Security Features Users Guide (SFUG).

4.1.3.2 Password Exit Processing

All the ESMs provide exit facilities and/or installation options that allow customers flexibility in defining password structures. These options and exits may be used to allow users the capability to specify the same password in multiple locations, according to the guidelines in *Section 4.1.3.1, DISA Password Guidelines*. This process does not change a password in multiple environments where a user has access, but allows a user to specify the same password in multiple platforms.

As stated in *Section 4.1.3.1, DISA Password Guidelines*, the site may, at its own discretion, extend the capabilities of the ESM by way of an exit to enforce any or all of the password requirements not already enforced by the ESM. If implemented, the enforcement of these password requirements will conform to the guidelines specified in *Section 4.1.3.1, DISA Password Guidelines,* and to those specified in the *DISA Computing Services Security Handbook.* The site *Security Features Users Guide (SFUG)* will document those requirements that are not enforced by the software, and will provide administrative direction for adhering to them.

Field Security Operations will approve all exits.

4.1.4 Special Privilege Access

Each ESM provides special privileges. When assigned to a userid, these special privileges allow the user to do tasks such as the following:

- Modify the security environment
- Perform auditing tasks
- Perform functions that circumvent the ESM

The following sections outline standards that will be used to reduce any effect on the operating environment.

4.1.4.1 External Security Program Modification Privileges

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

Users allowed to perform security administration for application-related data will be limited by the ESM to only change properties for which the user is responsible.

4.1.4.2 Audit Privileges

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.

4.1.4.3 Other Sensitive Privileges

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 ESM 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:

- Access system console information
- Issue console commands
- Execute restricted programs
- Access data and resources despite rule restrictions

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.

4.1.5 Resource Controls

Resource controls are the base capabilities supplied by the ESM to control access to system-level resources. These include Minidisk controls, VM reader controls, Diagnose Code controls, CP command controls, RSCS node controls, DCSS controls, program controls, and IUCV and VMCF controls.

4.2 TOP SECRET

4.2.1 Standard Global Options (Control Options)

The following table depicts the DISA standard values for the TSS Control Options records. Default parameter values should be coded for documentation purposes.

Table 1: STANDARD GLOBAL OPTIONS (CONTROL OPTIONS) – TOP SECRET (4.2.1)

4.2.1 STANDARD GLOBAL OPTIONS (CONTROL OPTIONS) - TOP SECRET		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
AUTH	Controls authorization checking.	OVERRIDE, ALLOVER
AUTOERASE	Controls auto-erase feature necessary to meet NCSC requirements.	Unclassified Systems: Optional Classified Systems: YES *CAUTION: Usage will affect performance.*
BACKUP	Controls automatic Security File backup.	Site defined
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.*
CPF	Controls startup of Command Propagation Facility.	Site defined
CPFNODES	Identifies remote nodes to which TSS commands can be transmitted.	Site defined
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
CPFTARGET	Controls default for TSS command TARGET keyword.	LOCAL
CPFWAIT	Controls default for TSS command WAIT keyword.	YES
DATE	Sets date display format.	MM/DD/YY
DEBUG	Controls debugging feature. Use as directed by CA support.	OFF
DOWN	Controls action taken when TSS address	SB, BW, OW, and either

4.2.1 STANDARD GLOBAL OPTIONS (CONTROL OPTIONS) - TOP SECRET		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
	space is inactive.	TW **or** TN
DRC	Modifies or lists particular DRC attributes.	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: A review by Field Security Operations is required for each exit point activated.*
FACILITY	Controls facility processing.	As applies to a specific system
INACTIVE	Controls users who have been inactive for a specific period.	35 days maximum
LOG	Controls incident recording for all facilities.	MSG, SEC9, INIT, SMF
MODE	Controls processing mode for all facilities.	FAIL
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
NEWPW	Selects new password specification rules.	MIN=6, MINDAYS=1, RS, ID, WARN=10, NR=0, TS
PTHRESH	Specifies password violation threshold.	3
PWEXP	Specifies password expiration interval.	90
PWHIST	Specifies number of previous passwords to be maintained in history file.	10
PWVIEW	Controls display of passwords by administrators.	NO
RECOVER	Controls change recovery. *NOTE: Requires the RECFILE DD statement in the TSS STC.*	ON
RESETSTATS	Used to reset all counters displayed by the STATS control option to zero (**0**).	Site defined
RPW	Allows the site to modify and list the	Site defined

4.2.1 STANDARD GLOBAL OPTIONS (CONTROL OPTIONS) - TOP SECRET		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
	contents of the Restricted Password list.	
SECTRACE	Controls security diagnostic trace.	OFF *NOTE: May be activated on an as-needed basis, only for diagnostic purposes.*
SHRFILE	Specifies whether TSS files will be shared.	Site defined
ST	Produces a display that combines the information produced for the VERSION, STATUS, and STATS control options.	Site defined
STATS	Displays numeric counts concerning TSS security processing.	Site defined
STATUS	Provides the current settings of various control options and information concerning cross memory requests and Security File service requests.	Site defined
SUSPEND	Allows an operator to suspend any ACID.	Site defined
TIMER	Interval at which data is written from TSS buffers to AUDIT/TRACKING file.	30
VERSION	Displays TOP SECRET version.	Site defined
VTHRESH	Selects violation threshold and action.	10, NOT, CAN

- *The **PWVIEW** option will be set to **NO.***
- *The **TIMER** option will be set to **30.***
- *The **CPFRCVUND** option will be set to **NO**.*
- *The **INACTIVE** option will be set to **35**.*
- *The **PWEXP** option, in the Global System Options, will be stet to **90.***
- *The **PTHRESH** option will be set to **3**.*

4.2.2 Userid Controls

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 virtual machine, or a batch job. Every user type ACID will be fully identified within TSS with the following completed fields:

NAME User's name

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 IAOs will ensure that the values for these fields are maintained and current.*

4.2.3 Emergency Userids

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

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

NAME

This userid is granted access to the **VM** facilities. All permissions will be permitted. To allow all data to be accessed by this userid, grant the following permission:

TSS ADD(acid) FAC(VM)
TSS ADD(acid) NORESCHK

Refer to *Section 4.1.2.4, Emergency Userids*, for further information.

4.2.4 VM System Operator Userids

In order to control which VM system operator can issue which commands, each operator will have a personal user ACID, and the console definition will require operators to log on prior to entering CP commands. If an operator already has a User ACID, that User ACID may be used for the purpose. Otherwise define a new User ACID.

Normally several operators at a site have similar duties, responsibilities, and roles, and require the ability to enter the same CP system commands. User ACIDs will not be shared.

4.2.5 Password Controls

4.2.5.1 Password Guidelines – TOP SECRET

The site will use the capabilities of the TSS control options, and (optionally) the password validation exit entry point to enforce the password requirements specified in *Section 4.1.3.1, DISA Password Guidelines*, and those specified in the *DISA Computing Services Security Handbook*. Several of the password requirements can be enforced through the use of standard TSS mechanisms. The requirements that are not already enforceable by TOP SECRET are as follows:

Table 2: PASSWORD REQUIREMENTS NOT ENFORCED BY TOP SECRET (4.2.5.1)

4.2.5.1 PASSWORD REQUIREMENTS NOT ENFORCED BY TOP SECRET
No words found in standard dictionaries will be used.
No obscene words will be used (i.e., restricted word list).[1]
Will not contain the user's name, userid (ACID), or telephone number.[2]

4.2.5.2 Password Exit Processing

As indicated previously (refer to *Section 4.1.3.2, Password Exit Processing*), the site may use the TOP SECRET installation exit to extend the capabilities of TOP SECRET to enforce any or all of the password requirements not already enforced by the ACP.

4.2.6 Special Privilege Access

The special privileges discussed in this section are all of an extremely sensitive nature, and will be rigidly controlled. The number of users granted these privileges will be kept to an absolute minimum.

[1] While not an explicit requirement, the exclusion of obscenity is deemed to be an implicit requirement serious enough to warrant independent mention. TOP SECRET provides a default list of 33 word prefixes which may not be used as/in a user's password. This list can be expanded up to 133 word prefixes at the discretion of the installation. Exceeding this number will require the coding of an exit. This list appears in *cleartext* in the TOP SECRET startup parameter library, and is viewable by any users who have *read* access to that library.

[2] TOP SECRET can prevent a new password that contains a user's ACID (userid), or one whose first four characters are equal to part of the user's name. Restricting the telephone number requires the use of an exit.

4.2.6.1 Access Control Product Modification Privileges

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.

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

4.2.6.2 Audit Privileges

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.

4.2.7 Resource Controls

TSS provides masking characters that can be used to identify certain values. The MSCA will own the following masking characters:

***** **(asterisk or star)**
+ **(plus sign)**
% **(percent sign)**
- **(dash or hyphen)**

4.2.7.1 Minidisk Controls

The most common controls used in the ESM are for the protection of files and Minidisks. File and Minidisk protection with the ESM is a time-consuming task, but presents the best way to ensure that compromise does not occur.

When writing controls for file and Minidisk access, consider the following common rules:

(1) Update file controls as users are added/deleted from the systems, as the responsibilities of an individual change, and/or as files or Minidisks are added/deleted/renamed.

(2) On a semi-annual basis, review all system-level data sets to ensure that the authority granted to individual users is valid.

(3) Limit user access to system-level and product-level execution files to execution (*exec/fetch*) access. To prevent a user from copying a program and executing it from a personal library, restrict *read* access to the systems personnel responsible for the installation and maintenance of the software. Also restrict *write/update* access to the systems personnel responsible for the installation and maintenance of the software.

(4) Ensure that all files defined as part of a specific executive software product have established protection mechanisms. Only specific users who require authorization to make changes to these data sets should have such access.

(5) Protect all audit trail data via the ESM. These audit trails are required for problem diagnosis, security investigations, and customer billing. *Update* and *alter* access needs to be tightly controlled from the point of the log/dump files down to the point where the final repository is located. Specific batch userids will have the authority to manage these processes. Restrict authority for an individual to *update*, *alter*, or *read* the file(s) to authorized DISA and site personnel. Log all personnel access for *update* or *alter* using the ACP's logging facility.

(6) Tightly restrict access to all ESM files. *Update* and *alter* access is restricted to the systems programming personnel and Security Administrators. The IAO or IAM (Information Assurance Manager) will document and maintain any exceptions. Updates to the security database will always be tracked by the utility programs provided with the ESM. Access to these files will be audited at all times.

(7) Protect all system files via the ESM to prevent update activity against it outside of, and without the approval of, the change management process. Update activity includes the addition or deletion of files. Log all *alter* and *update* access to the system files using the ESM's facilities. Only systems programming personnel and/or security personnel will be authorized to alter or update system files. The IAO will maintain the access requirements (e.g., *Form 41s*), and will maintain and review the ESM logging reports.

(8) Under normal circumstances, files will not contain hard-coded passwords in clear text. On rare occasions a business requirement may exist for passwords to be hard-coded in a file. To prevent compromise in such cases, ensure that the data set is adequately protected. The IAO will review and approve all such requirements.

- *The IAO will ensure that any ESM file exceptions are documented and maintained.*
- *The IAO will review and approve all business requirement requests for hard-coded passwords.*

4.2.7.2 VM Reader Controls

The capability exists within the products to protect the submission of work from one virtual machine to another on the same CPU. Protection of the VM Reader should be controlled at the discretion of the site.

4.2.7.3 Diagnose Code Controls

The capability exists within the products to protect Diagnose codes from being issued. Where applicable, ensure that Diagnose codes are restricted to authorized personnel.

4.2.7.4 CP Command Controls

CP commands are grouped into three categories—general user commands, privileged commands, and mixed commands.

4.2.7.4.1 General User Commands

General user commands only require a class of **G**. Since such commands as SPOOL, Link, Tag and Send only are able to perform the same function, they are categorized as general user commands. General user commands should be restricted to authorized personnel.

4.2.7.4.2 Privileged Commands

Privileged commands also perform the same function regardless of the authorized user. ATTACH, SHUTDOWN, NETWORK, and STORE HOST are examples of privileged commands. Privileged commands should be restricted to systems programming individuals.

4.2.7.4.3 Mixed Commands

Mixed commands perform different functions depending on the class of the user who issues them. QUERY DASD and SET are examples of mixed commands. Ensure that all authorized personnel are restricted by class, based on function, and limit the use of mixed commands to authorized personnel.

4.2.7.5 RSCS Node Controls

Since RSCS is used to transfer files between virtual machines, restrict file transfers when dealing with classified processing.

4.2.7.6 DCSS Controls

Discontiguous save segments are used to share *read only* storage between two or more virtual machines.

4.2.7.7 Program Controls

Sensitive utilities are required in a data center to support operations. However, the uncontrolled use of these utilities could result in a major system failure, loss of data, or a potential security exposure. Restrict these sensitive utilities only to the personnel who require access to them. Each ESM product offers protection of utilities at the program level. Systems personnel should evaluate utilities installed on the system to determine if the criteria mentioned above apply. They should also follow up with the IAO to ensure the utilities are protected.

Systems personnel should evaluate utilities installed on the system to determine if the criteria mentioned above apply. They should also follow up with the IAO to ensure the utilities are protected. Program controls should be enforced when restricting the use of TSSUTIL and TSSRECVR.

4.2.7.8 IUCV and VMCF Controls

Each ESM product offers protection from unauthorized communications either through the Inter-User Communications Vehicle (IUCV) or the Virtual Machine Communications Facility (VMCF).

4.2.7.9 Sensitive Utility Controls

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.

Access to protected programs considered sensitive in nature will be audited.

4.3 RACF

4.3.1 Standard Global Options (SETROPTS)

The following table depicts the DISA standard values for the RACF SETROPTS Options records:

NOTE: *Values listed are deviations from product default settings.*
Values not listed are to be the default values for the product.

Table A-3. STANDARD GLOBAL OPTIONS (SETROPTS) - RACF (4.3.1)

STANDARD GLOBAL OPTIONS (SETROPTS) - RACF		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
AUDIT	Logging RACF command and RACDEF SVC activity	AUDIT(*)
CLASSACT	General resource protection	The following classes will be activated on all systems: MINIDISKS FACILITY USER GROUP

STANDARD GLOBAL OPTIONS (SETROPTS) - RACF		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
		The following class will be activated only if no tape management system is installed on the system: TAPEVOL
CMDVIOL	Logging of RACF command violations	CMDVIOL
EGN	Enhanced generic naming	EGN
GENCMD	Generic profile creation	GENCMD(*) This option does not apply to the following resource classes: CCICSCMD GLOBAL KERBLINK PROGRAM REALM All group resource classes (e.g., GCICSTRN, GDASDVOL, etc.)
GENERIC	Generic profile checking	GENERIC(*) This option does not apply to the following resource classes: CCICSCMD GLOBAL KERBLINK PROGRAM REALM All group resource classes (e.g., GCICSTRN, GDASDVOL, etc.)
GLOBAL	Global access checking	Site defined **Refer to the Global Access Table Information note below.*
GRPLIST	List-of-Groups authority checking	GRPLIST

STANDARD GLOBAL OPTIONS (SETROPTS) - RACF		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
INACTIVE	Unused userid interval	35 days
INITSTATS	Records RACINIT statistics	INITSTATS
MODEL	Data set modeling	Site defined.
OPERAUDIT	Logging activities of users with the OPERATIONS attribute	OPERAUDIT
PASSWORD (HISTORY)	Number of previous passwords	10
PASSWORD (INTERVAL)	Maximum password change interval	90 days
PASSWORD (REVOKE)	Consecutive password verification attempts	3
PASSWORD (RULEn)	Password syntax rules	LENGTH(8) ALPHANUM(1:8)
PASSWORD (WARNING)	When password expiration message is issued	10
REALDSN	Places actual data set names in messages and SMF records	REALDSN
RETPD	Selects security retention period for tape data sets	99999
RVARYPW	Sets the RVARY passwords	Site defined. To be set in accordance with standard password guidelines.
SAUDIT	Logging of activity of users with SPECIAL attribute	SAUDIT
SECLEVELAUDIT	Auditing for security levels	NOSECLEVELAUDIT
STATISTICS	Activates resource statistics collection	Site defined.
SURROGAT	Controls who can logon to shared user IDs.	Site defined
TERMINAL	Universal access authority for terminals	READ
VMCMD	Certain CP commands and other requests on VM.	Site defined
VMMDISK	VM minidisks	Site defined
VMSEGMT	Restricted segments, which can be named saved segments (NSS) and discontiguous saved segments (DCSS).	Site defined

STANDARD GLOBAL OPTIONS (SETROPTS) - RACF		
OPTION	***DESCRIPTION***	***STANDARD VALUE***
TERMINAL	Universal access authority for terminals	READ

****Global Access Table Information:***

The use of the RACF Global Access Table option (**GLOBAL** in **SETROPTS**) is optional for each site and may improve system performance.

When access is requested, the Global Access Table is checked first because it resides in memory. By placing resources that are frequently accessed and have a UACC of *read* in this table, no further checking is made **if** the requested access is granted. If no entry exists in the Global Access Table, or the desired access is greater than specified in the table, a search is then made of the RACF database.

While the use of the Global Access Table is a site option, the decision to use it should be carefully made and will consider the following:

(1) Only frequently accessed resources should be considered.

(2) No ***RACLISTed*** resources will be included because these requests bypass the table.

(3) Only widely available resources will be included.

(4) Any resources that require logging and/or audit trails will not be included in the Global Access Table.

For any questions regarding the use of the Global Access Table, refer to the *RACF Security Administrator's Guide* and the *RACF Auditor's Guide*.

- *The IAO will ensure that GLOBAL OPTIONS are set in accordance with DISA requirements.*
- *The IAO will ensure that only authorized personnel are able to use the SETROPTS command.*
- *The IAO will ensure that RSCS nodes are protected using RACF resource classes.*
- *The IAO will ensure that **Any CP** command or **DIAGNOSE code** (including **privileged commands and DIAGNOSE codes**) are restricted to authorized personnel.*
- *The IAO will ensure that the creation, opening, and deletion of spool files are restricted using RACF classes.*
- *The IAO will ensure that the dumping and loading of spool files through the **SPXTAPE** and **SPTAPE** commands are restricted to authorized personnel.*
- *The IAO will ensure that **UCV CONNECT** and **SEVER** operations and certain **VMCF** functions are restricted.*
- *The IAO will ensure that **APPC/VM CONNECT** and **SEVER** operations are restricted using RACF classes.*
- *The IAO will ensure that the creation and deletion of logical devices is restricted to authorized personnel.*

4.3.2 Userid Controls

Every user will be identified to RACF via each user's unique userid profile. To RACF, a user is an individual (user). Every userid will be fully identified within RACF with the following fields completed:

NAME - User's name
DFLTGRP - Default group
OWNER - User's profile owner
PASSWORD - Password

RACF will automatically assign the default group as the password if a password is not explicitly coded. Assign a unique password to every userid to prevent unauthorized access by a person who knows the default group for a new userid.

- *The IAO will ensure, that at a minimum, the above **USER PROFILE** fields are completed for each user on the system.*

4.3.2.1 Users

Apply the principle of *least privilege* in the granting of all user privileges. Grant individual users the minimum resource authorizations necessary to accomplish their assigned functions. Only grant access to system resources as required.

Generate group profiles for all groups of users where applicable. These group profiles will identify the minimum privileges necessary for each group of users to accomplish its assigned functions. Associate every user's userid with at least one group profile.

Alternatively, if a user requires additional authority not granted to that user's default group, the user might be connected to one or more additional RACF groups on a permanent or a temporary basis. Because the installation is employing List-of-Groups checking (as is the DISA standard), the user will be given the highest level of authority allowed by any associated RACF group.

When a RACF userid initially is added, the Last Access Date (LAST-ACCESS) is set to UNKNOWN. Hence, an unused userid **never** expires due to inactivity. This results in non-expired, unused userids in the RACF database. Therefore the site will ensure that the local procedures for adding an interactive user include issuing the **ALTUSER <userid> RESUME** command. This will set LAST-ACCESS from UNKNOWN to the current date and time and thus enforce the expiration of the userid after 35 days of inactivity, even if the userid is never used.

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

Table A-4. USERS - RACF (4.3.2.1)

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

- *The IAO will ensure that a user profile exists for each user on the system.*
- *The IAO will ensure that all security-relevant events are audited.*

4.3.2.2 Batch Users

The following controls will be applied to production batch userids:

(1) All userids assigned to production batch jobs will be defined as **PROTECTED** userids. The following command shows the **ALTUSER** command used to assign the **PROTECTED** attribute to an existing userid:

ALTUSER *batch-userid* NOPASSWORD

(2) The DISA standard prohibits the use of surrogate processing.

For production batch work define userids associated with batch production jobs using **SURROGAT** processing. Each individual userid used for batch submission by a scheduler will have its userid coded as an **execution-userid** with the production scheduler being the **surrogate-userid**. For example:

RDEFINE SURROGAT *batch-userid*.SUBMIT UACC(NONE)
PERMIT *batch-userid*.SUBMIT CLASS(SURROGAT)
ID(*scheduler-userid*) ACCESS(READ)

- *The IAO will ensure that rules exist in the RACF data base restricting surrogate processing.*

4.3.2.3 Special Storage Management Users

Control userids assigned to production maintenance tasks, such as DASD maintenance userids, with program protection. File access for backup and recovery will be handled through the **DASDVOL** and/or **GDASDVOL** resource classes. Refer to the vendor's product documentation for the specific requirements of the resident DASD management software.

Use of these resource classes will effectively and discretely restrict the privileges of these userids. The **OPERATIONS** attribute will not be used for such processes, since data sets cannot be accessed if authorization has been explicitly revoked.

4.3.2.4 Emergency Userids

Define the userid established for emergency access with the **GROUP(NONE)** specification and the **OPERATIONS** attribute.

Define the userid established for security administration with the **SYSTEM-SPECIAL** attribute.

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

- *The IAO will ensure that emergency userids are restricted to authorized personnel and limited in duration.*

4.3.2.5 VM System Operator Userids

In order to control which system operator can issue which commands, each operator will have a personal userid and the console definition will require operators to log on prior to entering commands. If an operator already has a userid, that userid may be used for the purpose.

Normally several operators at a site have similar duties, responsibilities, and roles, and require the ability to enter the same system commands. Where such a group of operators exists, define a RACF group and connect the operators to that group, instead of issuing identical permits of individual operators to commands.

- *The IAO will ensure that all VM operators have assigned userids restricting, which commands they are able to enter.*

4.3.3 Password Controls

4.3.3.1 Password Guidelines

The site will utilize the capabilities of the RACF **SETROPTS PASSWORD** controls, and (optionally) the password validation exit to enforce the password requirements specified in *Password Guidelines*, and those specified in the *Computing Services Security Handbook*. Several of the password requirements can be enforced through the use of standard RACF mechanisms. The requirements that are not already enforceable by RACF are as follows:

Table A-5. PASSWORD REQUIREMENTS NOT ENFORCED BY RACF (4.3.3.1)

PASSWORD REQUIREMENTSNOT ENFORCED BY RACF
No words found in standard dictionaries will be used.
No obscene words will be used (i.e., restricted word list).[3]
At least one alphabetic, numeric, and special character will be used.[4]
Each character of the password will be unique.

[3] While not an explicit requirement, the exclusion of obscenity is deemed to be an implicit requirement serious enough to warrant independent mention.
[4] RACF can require that passwords contain at least one alphabetic or national character (i.e., $, #, and @) and one numeric character. Enforcing the DISA requirement that passwords contain at least one alphabetic, numeric, and special character requires the use of an exit.

PASSWORD REQUIREMENTSNOT ENFORCED BY RACF
Passwords will contain no consecutive characters (e.g., 12, AB).
Will not contain the user's name, userid, or telephone number.
Passwords cannot be changed more than once every 24 hours without IAO intervention.

- *The IAO will ensure that password requirements are enforced.*

4.3.3.2 Password Exit Processing

As indicated previously (refer to *Section 3.1.3.2, Password Exit Processing*), the site may use the RACF password exit to extend the capabilities of RACF to enforce any or all of the password requirements not already enforced by the ACP. If implemented, use the following exit to implement these controls:

RACF Exit: **ICHPWX01**

- *The IAO will ensure that all exits are reviewed by FSO prior to implementation.*

4.3.4 Special Privilege Access

The special privileges discussed in this section are all of an extremely sensitive nature, and will be rigidly controlled. Keep the number of users granted these privileges to an absolute minimum.

- *The IAO will restrict special privilege access to authorized personnel.*

4.3.4.1 Access Control Product Modification Privileges

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

4.3.4.2 Audit Privileges

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

- *The IAO will ensure that the FSO SRR team has Auditor privileges.*

4.3.4.4 Other Sensitive Privileges

RACF controls a number of other privileges in the general resource class. Do not grant the Device Mount privilege to non-operator or system users. It may be granted on an as-needed basis.

OPER and **ACCOUNT** privileges, as well as access to the **CONSOLE** facility, will be strictly controlled.

RACF provides the ability to limit the commands that a user can issue through userid keywords. If command limiting is implemented, the ability to bypass the command limiting will be strictly controlled, and will only be granted to selected users.

The ability to execute privileged programs will be strictly controlled, and will be permitted to the minimum number of users. The IAO will maintain the documentation justifying the requirement to execute these programs.

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

4.3.5 Resource Controls

4.3.5.1 File Controls

File controls are provided via the **file** resource, or **minidisk** resource. All files/minidisks will be fully protected. Protection by default will be globally enabled. The universal access parameter (**UACC**) will be defined as **NONE** for all file and minidisk profiles, since undefined users have access to resources permitted through the use of the UACC. For any files or minidisks requiring global access, use the **PERMIT ID (*)** command structure. Only permit data set access to users requiring access via data set profiles.

Restrict the use of global file/minidisk access to a minimum. Certain file/minidisks, such as general purpose or public, may use global permissions, but these should be restricted to the appropriate level of access.

Great care and consideration needs to go into defining the access given to the files and minidisks. The Security staff, along with the Systems staff, will work together to define the access needed and restrict the level of access appropriately.

- *The IAO will ensure that file controls are enforced.*
- *The IAO will ensure that minidisk controls are enforced.*
- *The IAO will ensure that password controls are enforced on resources.*

4.3.5.2 Volume Controls

Volume controls are provided via the **MINIDISK** resource class. Permit access to volumes for which volume-level protection will be provided (rather than data set-level protection) only to users requiring access.

When protecting volumes via the **MINIDISK** class, use the following controls:

(1) Prevent access to minidisks by default. Create a generic profile of "*****" with **UACC (NONE)**.

(2) Individual users will be discretely granted the required accesses to specific volumes. The granted access will be the minimum required by users to perform their respective assigned duties.

- *The IAO will ensure that all minidisks are protected in accordance with DISA requirements.*

4.3.5.3 Sensitive Utility Controls

Access to sensitive utilities will be strictly controlled. Control access to the minidisks in which the utilities reside through the use of access permission.

Control maintenance as previously described. The ability to execute privileged programs will be strictly controlled, and will be permitted to the minimum number of users.

Audit access to protected programs considered sensitive in nature

(1) Use RACF controls to control files that reside on public minidisks.

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

- *The IAO will ensure that sensitive utilities and commands are password restricted.*

4.3.5.4 Dynamic List Controls

Dynamic list controls are provided via resources in the **FACILITY** resource class. This class should already be active and use generic masking, but the sample commands shown below include the relevant **SETROPTS** commands[5] for the sake of completeness. 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.

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

RDEFINE FACILITY *resource* AUDIT(ALL) UACC(NONE)

PERMIT *resource* CLASS(FACILITY) ID(*sysprog*)
ACCESS(READ)

4.3.5.5 Console Controls

Console controls are provided via resources in the **CONSOLE**, **OPERCMDS** resource classes. These classes should already be active, and **OPERCMDS** should already use generic masking, but the sample commands shown below include the relevant **SETROPTS** commands[6] for the sake of completeness. When protecting the facilities consoles via these classes, use the following controls:

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

RDEFINE CONSOLE * AUDIT(ALL) UACC(NONE)
RDEFINE CONSOLE *consname* AUDIT(ALL) UACC(NONE)
PERMIT *consname* CLASS(CONSOLE) ID(*opergrp*) ACCESS(READ)
SETROPTS CLASSACT(CONSOLE)
SETROPTS RACLIST(CONSOLE) REFRESH
SETROPTS GENERIC(OPERCMDS)
RDEFINE OPERCMDS *command* AUDIT(ALL) UACC(NONE)
SETROPTS CLASSACT(OPERCMDS)
SETROPTS RACLIST(OPERCMDS) REFRESH

[5] The SETROPTS REFRESH is only shown once; it must be repeated as necessary.
[6]

(2) The user profile for each real console will be granted *read* access to the corresponding console resource:

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

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

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

- *The IAO will ensure that all consoles are restricted to authorized personnel.*

4.3.5.6 CP Command Controls

CP command controls are provided via a RACF resource class. This class should already be active and use generic masking. The following are examples of masking operator commands:

SETROPTS GENERIC(OPERCMDS)
RDEFINE OPERCMDS *commands* AUDIT(ALL) UACC(NONE)
RDEFINE OPERCMDS *command* AUDIT(ALL) UACC(NONE)

(2) Only grant access to system commands to the extent documented in the installation SOP. The **RDEFINE** statements will include the **AUDIT** and **UACC** values specified in the SOP, or **AUDIT(ALL) UACC(NONE)** if not specified.

The following is an example of granting a user permission to issue commands:

PERMIT *Command* CLASS(OPERCMDS) ID(*userid*)
ACCESS(UPDATE)

SETROPTS RACLIST(OPERCMDS) REFRESH

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

PERMIT command CLASS(OPERCMDS) ID(*opergrp*)
ACCESS(READ) WHEN(CONSOLE(*consid*))

SETROPTS RACLIST(OPERCMDS) REFRESH

- *The IAO will ensure that all operator commands are restricted the authorized personnel.*
- *The IAO will ensure that the CP **DIAL** and **MSG** commands are restricted and audited prior to their logging on.*

4.4 VM:Secure

Vendor: Computer Associates

VM:Secure is an external security product developed to control access to VM systems and resources. It is integrated with other features to ensure compatibility between releases of VM. The other features involve directory management, disk space management, and data encryption, and are supported by thirteen other Computer Associates VM products.

4.4.1 Configuration Files

In order to control VM:Secure processing, multiple configuration files are used. Each configuration file is designed to support a specific function of VM:Secure. The records contained in the files can only appear in the designated file. VM:Secure can be reconfigured using the CONFIG command, which should be restricted to systems programmers and the security administrator. The files used to control VM:Secure are outlined in the following sub-sections.

- *The **VMXRPI CONFIG** file will be restricted to authorized personnel.*
- *The VM:Secure **AUDIT** file will be restricted to authorized personnel.*

4.4.1.1 PRODUCT CONFIG File

Created as part of the installation of VM:Secure, the PRODUCT CONFIG file is used to configure and control the normal processing of VM:Secure. The PRODUCT CONFIG file resides on the VM:Secure A-disk, and should be backed up as part of the normal backups. The following table lists the records found on the product configuration file and a brief description:

Table 6. PRODUCT CONFIGURATION FILE RECORDS (4.4.1.1)

RECORD	*DESCRIPTION*
ACCESS	Identifies the minidisks used by VM:Secure as directory database minidisks.
ALTERNAT	Specifies commands to be used by various VM:Secure macros in place of the CMS COPYFILE and FORMAT commands.
AUTOUSER	Specifies the userid to be used as the system's service virtual machine.
CPUID	Allows VM:Secure to run on a specific CPU.
DELAYHIS	Specifies the amount of time for VM:Secure to wait before updating the last logon (*LL=), last (x)autolog (*LA=), and history (*HS=) special comments.
DELAYLOG	Used to impose a minimum wait between a user's invalid logon attempt and the next attempt.
DIRECT	Identifies the CP-owned volume that contains the page-formatted directory area for the CP object directory.
DUMP	Identifies the userid that will receive a VMDUMP if the VM:Secure virtual machine abends.
ENCRYPT	Tells VM:Secure that all information in the directory database is encrypted.
IPLDISK	Identifies an IPLable minidisk owned by the VM:Secure service virtual machine.
MACLOAD	Specifies which command macros to load and keep in virtual memory.
MESSAGE	Controls VM:Secure messages.
MSGCASE	Specifies how VM:Secure will display its messages.
PRODUCT	Identifies other service virtual machines that are running Computer Associates products and activates the interface between VM:Secure and the other service virtual machines.
SERVANT	Enables or disables the Servant Facility.
SYSOPER	Identifies the system operators—the userids that are to receive messages generated during initialization, by commands, during termination, and when an abend occurs. There can be multiple SYSOPER records.
USEREXIT	Specifies the filename of a user exit routine.

NOTE: *All but three records on this file can be changed dynamically. The three records that cannot be changed dynamically are ACCESS, DIRECT and ENCRYPT. These require VM:Secure to be brought down and the file changes made manually.*

- *The **PRODUCT CONFIG** file will be restricted to authorized personnel.*

4.4.1.2 SECURITY CONFIG File

Also created as part of the installation of VM:Secure, the SECURITY CONFIG file contains records that provide security features and control the use of the Rules Facility. The SECURITY CONFIG file resides on the VM:Secure A-disk. The following table lists the records found on the security configuration file and a brief description:

Table 7. SECURITY CONFIGURATION FILE RECORDS (4.4.1.2)

RECORD	*DESCRIPTION*
AUTOEXP	Controls the automatic expiration of userid logon and is valid only if the Rules Facility is in use.
AUTOPASS	Forces minidisk passwords to automatically be the same as logon passwords.
DISPRULE	Displays information about rules.
GROUP	Defines a group name to be associated with the ACIGROUP directory control statement.
JOURNAL	Controls the monitoring of invalid password conditions.
NORULE	Determines whether to allow a CP command to execute when no applicable rule is found. This enables VM:Secure to be an open system or a closed system.
PWSUPRES	Use the PWSUPRES record to suppress, or mask, VM:Secure password display.

NOTE: *The records used in this file in cannot be used in any other configuration file. To make any changes to the AUTOPASS record, VM:Secure must be taken down.*

- *The **SECURITY CONFIG** file will be restricted to authorized personnel.*
- *The **AUTOEXP** option will be enabled.*
- *The **JOURNAL** option will be enabled.*

4.4.1.3 AUTHORIZ CONFIG File

This file is used to tailor user authorizations and is created as part of the installation of VM:Secure. The following table describes the records found on the authorization configuration file and a brief description:

Table 8. AUTHORIZATION CONFIGURATION FILE RECORDS (4.4.1.3)

RECORD	*DESCRIPTION*	*AUTHORIZED USER*
GRANT	Authorizes users to use VM:Secure commands, utilities, and screen selections.	Security Administrator
LIST	Creates a list of userids or authorizations to use on GRANT and WITHHOLD records.	Security Administrator
WITHHOLD	Restricts users from using VM:Secure	Security Administrator

	commands, utilities, or screen selections. Also used to define exceptions to general authorizations.	

- *The **AUTHORIZ CONFIG** file will be restricted to authorized personnel.*

4.4.1.4 DASD CONFIG File

The DASD configuration file is created as part of the installation of VM:Secure and resides on the VM:Secure A-disk. The DASD configuration file is used to define the DASD configuration. The following table describes DASD configuration file records and a brief description:

Table 9. DASD CONFIGURATION FILE RECORDS (4.4.1.4)

RECORD	*DESCRIPTION*
DEVTYPE	Customizes the name, attributes, or space characteristics of a specific device type.
IGNORE	Identifies which userids or minidisks are to be ignored by VM:Secure when it checks for overlapping minidisks.
NOLINK	Indicates which directory links are not to be mapped by VM:Secure.
VOLUME	Identifies a real DASD volume that VM:Secure can control.

NOTE: *The records identified in this table should be considered for security purposes. Not all of the DASD configuration records are listed in the table.*

- *The **DASD CONFIG** file will be restricted to authorized personnel.*

4.4.1.5 SFS CONFIG File

The SFS configuration file is used to control the addition/deletion of file pools and user storage groups. In order for this file to be used, SFS must be described to VM:Secure. The SFS administrator's userid is used to configure the SFS configuration files. The SFS administrator userid is used to perform user administration tasks through VM:Secure. All but one of the configuration functions for VM:Secure SFS are performed by SFS administrators. The only function that must be performed by the VM:Secure System Administrator rather than the SFS administrator is identifying the SFS administrators to VM:Secure.

In order to make changes to the SFS configuration, the CONFIG SFS command displays the SFS Configuration Menu, which allows the changing of the VM:Secure configuration for SFS. The CONFIG SFS command should be restricted to the security manager or authorized systems programmers.

If the SFS parameter is not included on the CONFIG command, VM:Secure displays the System Configuration Menu, from which the configuration file can be chosen to be opened or the SFS Configuration Menu. When a configuration file is saved after being modified, VM:Secure verifies the changes and puts them into effect immediately. If VM:Secure finds a non-existent userid on a record when it updates the file, it writes warning messages on the console but still

updates the file. When exiting the SFS Configuration Menu, VM:Secure puts any changes into effect immediately.

- *The **SFS** configuration file will be restricted to authorized personnel.*

4.4.1.6 VM:Secure GLOBALS File

The VMSECURE GLOBALS file, which resides on the VM:Secure DRCT minidisk, contains the global default system settings used by VM:Secure during directory processing. The global settings apply to all users on the system. VM:Secure reads the VMSECURE GLOBALS file as part of its initialization process. The GLOBALOPT records in the VMSECURE GLOBALS file identifies a specific setting and can be update dynamically using the ADMIN GLOBALS command. The ADMIN GLOBALS command should be restricted to systems programmers and authorized personnel.

- *The **ADMIN GLOBALS** command will be restricted to authorized personnel.*

4.4.2 VM:Secure Rules Facility

The VM:Secure Rules Facility enables the creation of rules to control access to system resources, virtual machines, minidisks and the transfer of data between virtual machines. Rules can be defined at the user, security group, and system level. Each time a command is issued, CP passes the request to VM:Secure. VM:Secure then checks its rules database to find the rule that applies to the request. If the rule allows execution, VM:Secure executes the command as requested. If the rule disallows execution, VM:Secure does not execute the command. VM:Secure may send a message to the user depending on what is coded in the configuration files. If no rule is found, VM:Secure accepts or rejects the command based on the default action defined in the configuration files.

- *The **VM:Secure Rules Facility** will be restricted to authorized personnel.*

4.4.2.1 Security Administrators, Security Group Managers, and Directory Managers

The Security Administrator can create and change rules for any userid at a site. The Security Administrator also determines which userids are to be assigned to each security group manager. The Security Administrator must have authorization to use all VM:Secure rules commands on all users on the system. All other commands should be restricted by group and logged.

Security group managers can create and change rules for their own userids and for userids in their security groups. A security group manager is different from a directory manager in that a directory manager is authorized to manage directory entries for a group of userids, while a security group manager manages users' rules files.

At some sites, the directory manager for each userid is also that userid's security group manager. Even though VM:Secure allows general users the capability to create and change rules that

pertain to their own userids, this is not recommended and should be limited to the system security and directory managers.

Because system rules can be created to serve as common rules for all userids, service machines and other product components, when using VM:Secure is conjunction with other Computer Associates VM product components, ensure that all security administration remains with the system security administrator and not with the product component administrators.

- *The IAO will ensure that **Security Administration** is restricted to authorized personnel.*
- *The IAO will ensure that **Security Group Administration** is restricted to authorized personnel.*
- *The IAO will ensure that **Directory Administration** is restricted to authorized personnel.*

4.4.2.2 Rules Database

VM:Secure rules are stored in the VM:Secure rules database. The rules database consists of a group of files stored on the RULE minidisk created for the VM:Secure service virtual machine. Each rules file contains a number of statements that set up the rules for a particular userid or security group. The filename of each rules file matches a userid or group name. The file type of each rules file indicates what kind of rules the file contains. The following is a breakdown of the rules database and should be restricted to Security Administrators and authorized systems programmers. The following sections outline the five types of files that make up the rules database.

- *The **Rule mini disk** will be restricted to authorized personnel.*
- *The **Rule mini disk** will be backed up on a regular basis.*
- *The **VMXBKPxx** utilities will be restricted to authorized personnel.*

4.4.2.2.1 System Override Rules File

This file contains rules that override default rules.

4.4.2.2.2 Security Group Rules Files

These files contain security group rules that can be established by security group managers.

4.4.2.2.3 User Rules Files

These files contain user rules that can be established by the user, by the security group manager, or by the VM:Secure system administrator. Users must not be given authorization to create user rules. User rules cover requests where the user's virtual machine is the target of the request.

- *The User Rules Files will be restricted to authorized personnel.*

4.4.2.2.4 Security Group Default Rules Files

These files contain security group rules that can be established by security group managers.

4.4.2.2.5 System Default Rules File

These files contain rules that serve as system security defaults. These rules are processed last and before the NORULE record in the SECURITY CONFIG file.

4.4.2.3 VM:Secure Rules

The following table identifies the rules that may be coded on the rules database and recommended usage:

Table 10. RULES DATABASE (4.4.2.3)

RULE	*DESCRIPTION*	*RECOMMENDED USAGE*
AUTOLOG	Controls autolog access to a virtual machine	Required
DIAL	Controls the terminal addresses that can use the CP DIAL command to dial to a userid.	Required
LINK	Controls linking to a minidisk.	Required
LOGON	Controls logon to a userid.	Required
LOGONBY	Limits logon access to target userids to authorized users only, using the VM:Secure LOGONBY Facility or the CP LOGONBY command.	Restrict
MEMBER	Allows system administrators and security group managers to decide who can become a temporary member of a security group.	Site Defined
SPOOL	Controls the spooling and transferring of files to a virtual unit record device.	Site Defined
STORE	Allows restriction of specified userids or terminals from issuing the CP STORE HOST command.	Site Defined
TAG	Controls the use of the CP TAG command by writing rules that accept or reject userids specifying a certain node name on a tag.	Site Defined
TRANSFER	Controls spooling and transferring of files to a virtual unit record devices.	Site Defined
VMSCHED CANCEL	Controls cancellation of VM:Schedule jobs scheduled to run on a virtual machine.	Restrict
VMSCHED QUERY	Controls querying the status of VM:Schedule jobs scheduled to run on a virtual machine.	Site Defined
VMSCHED SCHEDULE	Controls job scheduling for a virtual machine.	Site Defined
VMTAPE CATALOG	Controls access to the tape catalog entries in the VM:Tape Tape Management Catalog (TMC).	Site Defined

RULE	*DESCRIPTION*	*RECOMMENDED USAGE*
VMTAPE LIST	Controls the listing of the TMC entries for tapes owned by a virtual machine.	Site Defined
VMTAPE MOUNT	Controls tape mount authorization.	Site Defined
XAUTOLOG	Controls xautolog access to a virtual machine.	Restrict

- *The **LOGONBY Facility** will not be used.*

4.4.2.4 Security Groups

A security group is a group of users who perform the same types of functions and work in the same area. As a result it may be easier to assign users to security groups for ease of authorization maintenance. All security groups should be reviewed on a regular basis to ensure that only authorized users have appropriate access.

4.4.3 VM:Secure Commands

Many of VM:Secure's functions are performed dynamically. As a result, the authorization to issue the commands below must be restricted in accordance with the authorizations specified in the following table:

NOTE: *The table below uses the following—SA-Security Administrator, GM-Group Manager, SP-Systems Programmer, SO-Senior Operator.*

Table 11. VM:Secure COMMANDS (4.4.3)

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
ABEND	Terminates VM:Secure operation abnormally	SA GM SP SO	Y N Y Y	Y Y Y
ACITRACE	Dynamically traces ACI security events	SA GM SP SO	Y N Y N	Y Y
ADDENTRY	Creates a userid or directory profile	SA GM SP SO	Y Y N N	Y Y
ADDMDISK	Adds a minidisk for a userid	SA GM SP SO	Y N Y N	Y Y
ADMIN	Creates or opens for edit a directory pool	SA	Y	Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
	definition, a directory profile, or a skeleton file, or opens the VMSECURE GLOBALS file, the VMSECURE MANAGERS file, the VMSECURE POSIX file, or the SFS Managers Configuration Menu	GM SP SO	Y Y N	Y Y
ASSIGN	Assigns a userid to a different manager	SA GM SP SO	Y Y N N	Y Y
AUDITEXT	Extracts current audit information	SA GM SP SO	Y Y Y N	 Y
CAN	Queries the VM:Secure rules database about authorizations	SA GM SP SO	Y Y Y N	Y Y Y
CHANGE	Renames a userid	SA GM SP SO	Y Y N N	Y Y
CHGMDISK	Moves or changes a minidisk	SA GM SP SO	Y Y Y N	Y Y Y
CHGVOLNM	Changes all references to the volser of any DASD volume controlled by VM:Secure	SA GM SP SO	Y N Y N	Y Y
CLASS	Assigns a CP privilege class	SA GM SP SO	Y Y Y N	Y Y Y
CMS	Executes a CMS or CP command on the VM:Secure service virtual machine	SA GM SP SO	Y Y Y Y	Y Y Y
COMPRESS	Defragments disk storage	SA GM SP SO	Y Y Y Y	 Y
CONFIG	Opens the VM:Secure configuration files for editing or updates the VM:Secure SFS	SA GM	Y Y	Y Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
	configuration	SP SO	Y N	Y
DELENTRY	Deletes an existing userid or directory profile	SA GM SP SO	Y Y N N	Y Y
DELETE	Deletes file spaces for an active userid	SA GM SP SO	Y Y Y Y	Y Y Y Y
DELMDISK	Deletes a userid's minidisk	SA GM SP SO	Y Y Y Y	Y Y Y Y
DISPLINK	Displays links to a userid's minidisks	SA GM SP SO	Y Y Y N	
EDIT	Opens a userid's directory entry for editing	SA GM SP SO	Y Y Y N	Y Y Y
EDX	Opens a userid's directory entry for editing, expanding any INCLUDE statement in that directory entry	SA GM SP SO	Y Y Y N	Y Y Y
END	Terminates VM:Secure operation normally	SA GM SP SO	Y Y Y Y	Y Y Y Y
ENROLL	Enrolls a userid into an SFS file pool	SA GM SP SO	Y Y Y N	Y Y Y
EXPIRE	Expires a userid's logon password	SA GM SP SO	Y Y Y N	Y Y Y
EXTRACT	Extracts directory information	SA GM SP SO	Y Y Y N	
GENACI	Places a userid in a security group	SA	Y	Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
		GM SP SO	N Y N	 Y
GENHS	Adds history records to a userid's directory entry	SA GM SP SO	Y N N N	
GENINCL	Adds an INCLUDE statement to a userid's directory entry	SA GM SP SO	Y Y Y N	Y Y Y
GETENTRY	Retrieves a current copy of a userid's directory entry or a directory profile	SA GM SP SO	Y Y Y N	
GRANT AUTHORITY	Authorizes users to gain access to SFS directories or the files in them	SA GM SP SO	Y Y Y N	Y Y Y
GROUP	Makes a userid a temporary member of a new security group	SA GM SP SO	Y Y Y N	Y Y Y
HISTORY	Displays a userid's history records	SA GM SP SO	Y Y Y N	
IPLDISKX	Converts userids whose passwords expired before the Rules Facility was installed to the Rules Facility method of password expiration	SA GM SP SO	Y Y Y N	Y Y Y
JOURNAL	Displays password violations or resets a password violation count to zero	SA GM SP SO	Y Y Y N	
LISTAUTH	Lists all authorizations in the AUTHORIZ CONFIG file that pertain to an individual userid or authority	SA GM SP SO	Y N Y N	
LOCK	Prevents updates to a CMS file, userid, or directory profile	SA GM SP SO	Y N Y N	Y Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
LOGMSG	Creates messages to send to userids at specific events	SA GM SP SO	Y Y Y Y	
MACLOAD	Copies a macro from your A disk to the VM:Secure service virtual machine's A Disk	SA GM SP SO	Y Y Y Y	Y Y Y Y
MAINT	Performs line mode USER command and MANAGE command functions	SA GM SP SO	Y Y Y N	
MANAGE	Displays screens that let you define new userids and modify existing ones	SA GM SP SO	Y Y Y N	
MAP	Maps a volume	SA GM SP SO	Y Y Y Y	
MAY	Queries an authorization in the AUTHORIZ CONFIG file	SA GM SP SO	Y Y Y N	Y Y Y
MDSKSCAN	Scans a userid's minidisks	SA GM SP SO	Y Y Y N	
MODIFY	Modifies the SFS allocation limits for a userid	SA GM SP SO	Y Y Y N	Y Y Y
MOVE2SFS	Copies data from minidisks to SFS	SA GM SP SO	Y Y Y Y	Y Y Y Y
MULTIPLE	Performs userid management functions on many userids at the same time	SA GM SP SO	Y Y Y N	Y Y Y
NEWIPL	Changes an IPL system name or device in all directory entries to a new IPL system name or device	SA GM SP	Y N Y	Y Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
		SO	N	
NOLOG	Changes a userid's password to NOLOG 264	SA GM SP SO	Y N Y N	Y Y
OVERRIDE	Alters privilege classes without shutting down VM:Secure	SA GM SP SO	Y N Y N	Y Y
PAINT	Changes a VM:Secure screen	SA GM SP SO	Y N Y N	Y Y
PASSWORD	Sets a password for a userid	SA GM SP SO	Y Y Y N	Y Y Y
QCPCFG	Displays information about the CP component configuration	SA GM SP SO	Y Y Y N	 Y
QLOCK	Displays all VM:Secure locks	SA GM SP SO	Y Y Y N	Y Y Y
QPCB	Lists active VM:Secure processes	SA GM SP SO	Y Y Y N	
QRULES	Queries the rules set up for a userid	SA GM SP SO	Y Y Y N	
QSTART	Displays the time VM:Secure was most recently started	SA GM SP SO	Y Y Y Y	
QUERY	Provides information about a number of VM:Secure functions	SA GM SP SO	Y Y Y N	
REBUILD	Condenses and defragments the CP object directory (Use this command only under the	SA GM	Y Y	Y Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
	direction of Computer Associates Customer Services.)	SP SO	Y N	Y
RECLAIM	Reclaims DASD space from MOVERO minidisks	SA GM SP SO	Y Y Y N	Y Y Y
REPENTRY	Replaces a directory entry or a directory profile	SA GM SP SO	Y Y Y N	Y Y Y
RESET	Resets password violation counts	SA GM SP SO	Y Y Y N	Y Y Y
REVOKE AUTHORITY	Revokes access to SFS directories and the files in them from users	SA GM SP SO	Y Y Y N	Y Y Y
RULEMAP	Displays rules of various kinds	SA GM SP SO	Y Y Y N	
RULES	Changes a userid's rules, a group's override or default rules, or the system override or system default rules	SA GM SP SO	Y Y Y N	Y Y Y
SYSWORD	Queries and sets the system word	SA GM SP SO	Y Y Y N	Y Y Y
TRACE	Traces execution of a VM:Secure macro	SA GM SP SO	Y N Y N	
TRANSFER	Transfers a minidisk from one userid to another	SA GM SP SO	Y Y Y N	Y Y Y
ULIST	Displays information about userids	SA GM SP SO	Y Y Y N	
UNLOCK	Removes a lock from a CMS file, profile, or	SA	Y	Y

COMMAND	*FUNCTION*	*GROUP*	*AUTH*	*LOG REQ'D*
	userid	GM SP SO	Y Y N	Y Y
USER	Lets users modify their own directory entries	SA GM SP SO	Y Y Y N	Y Y Y

4.4.3.1 Predefined Variables

Since many of the above commands use similar variables, it is recommended that the VM:Secure documentation be consulted in the use of predefined variables.

4.4.4 Skeleton Files

A skeleton file is a prototype CP directory entry. It includes directory statements and special comments that describe a userid. The use of skeleton files **must** be limited to authorized administrators.

4.4.5 Granting Authorizations to Use Commands on Terminals

Command usage should be controlled at the terminal level. This is an effective way of limiting access to a VM system. Consult the VM:Secure documentation when applying this type of restrictions to terminals.

4.4.6 Automating Password Expiration

Automatic password expiration can be performed by VM:Secure as part of its Rules Facility operation. The automatic password expiration must be turned on for all userids within the system, and must be set to expire at 90 days. No userid should be allowed to have non-expiring user passwords. The only time that automatic password may be turned off is if required by a specific product, and in that case it must be approved by the security manager with appropriate documentation. Questions to this policy should be addressed to Field Security Operations. See *Appendix C, Document Revision Request*.

APPENDIX A. RELATED PUBLICATIONS

Government Publications

Department of Defense (DOD) Directive 8500.1, "Information Assurance (IA)," October 24, 2002.

Department of Defense 8500.1 STD, "DOD Trusted Computer System Evaluation Criteria, October 24, 2002."

Department of Defense (DOD) Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

Department of Defense CSC-STD-002-85, "DOD Password Management Guideline," 12 April 1985.

Defense Information Systems Agency Instruction (DISAI) 630-230-19, "Security Requirements for Automated Information Systems (AISs)," July 1996.

Defense Information Systems Agency Instruction (DISAI) 630-255-7, "Internet, Intranet, and World Wide Web," September 1996.

Defense Information Systems Agency (DISA) Computing Services Naming Convention Standards, February 1996.

Defense Information Systems Agency (DISA) Computing Services Security Handbook, Version 3, 1 December 2000.

Defense Information Systems Agency (DISA) Network Infrastructure Security Technical Implementation Guide, Version 4, Release 2, 15 October 2002.

Defense Information Systems Agency (DISA) UNIX Security Technical Implementation Guide, Version 3, Release 1.1, 5 January 2001.

Defense Information Systems Agency (DISA) OS/390 Security Technical Implementation Guide, Version 3, Release 2, 30 June 2002.
.
Defense Information Systems Agency (DISA) S/390 Logical Partition Security Technical Implementation Guide, Version 1, Release 4, 30 April 2002.

Defense Information Systems Agency (DISA) Computing Services Security Instruction 360-225-08, "Magnetic Tape Backup and Storage by Defense Megacenters," November 1997.

National Security Agency (NSA), "Information Systems Security Products and Services Catalog" (Current Edition).

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," 9 October 1991.

Army Regulation (AR) 380-19, "Information Systems Security," 1 August 1990.

Air Force Systems Security Instruction (AFSSI) 5100, "The Air Force Computer Security (COMPUSEC) Program," 2 June 1992.

Air Force Systems Security Memorandum (AFSSM) 5007, "A Methodology for Addressing DOD-Mandated "C2 by 92" for Operational Air Force Systems," 25 March 1991.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, "Department of the Navy Automated Information Systems (AIS) Security Program," 15 November 1989.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," August 1992.

Public Law 100-235, 100th Congress, an Act cited as the "Computer Security Act of 1987," 8 January 1988.

General Information Sites

http://www.cert.mil	Defense Information Systems Agency (DISA) DOD-CERT (Department of Defense - Computer Emergency Response Team)
http://www.specbench.org	The Standard Performance Evaluation Corporation
http://datahouse.disa.mil	Defense Information Systems Agency (DISA) Home Page
http://www.cert.org	A focal point for the computer security concerns of Internet users
http://www.auscert.org.au	Australian Computer Emergency Response Team. They maintain security "how to" documents.
http://ciac.llnl.gov/	The U.S. Department of Energy’s Computer Incident AdvIAOry Capability
http://nsi.org	National Security Institute’s Security Resource Net Home Page

http://csrc.nist.gov	National Institute of Standards and Technology's Computer Security Resource Clearinghouse
http://www.cs.purdue.edu	COAST (Computer Operations, Audit, and Security Technology) focuses on real-world research needs.
http://www.redbooks.ibm.com/redbooks/homepage.html	Redbooks, named for their red covers, are "how to" books, written by very experienced IBM professionals from all over the world.

This page is intentionally left blank.

APPENDIX B. LIST OF ANCRONYMS

ANCRONYM	DEFINITION
ABEND	Abnormal End. Abnormal termination of a job or task.
ACI	Access Control Interface.
ACP	Access Control Product.
ADP	Automated Data Processing.
AIS	Automated Information System.
API	Application Programming Interface.
APPC/VM	Advanced Program-to-Program Communication/VM.
CCB	Configuration Control Board.
CDA	Central Design Activity.
CMS	Conversational Monitor System.
COE	Common Operating Environment.
COMPUSEC	Computer Security.
COMSEC	Communications Security.
COOP	Continuity of Operations Plan. A process to ensure availability in the event of a system or component failure.
COTS	Commercial-Off-The-Shelf.
CP	Control Program.
CPU	Central Processing Unit. Computer hardware that processes computer software instructions.
CRYPTO	Cryptographic. A marking or designator identifying all COMSEC keying material use to secure or authenticate telecommunications.
C-Time	Creation time of a file.
DAC	Discretionary Access Control. A means of restricting access of files to those with appropriate access permissions.
DASD	Direct Access Storage Device. A hardware device (disk drive) used for temporary or permanent storage of data and software.
Data Integrity	Concept of ensuring that data is not manipulated or accessed in any way other than what was originally intended.
Data Labels	Labels that identify the classification level of data. Normally associated with B1 security processing.
Data Owner	Organization or individual that owns the data on a system and is responsible for the contents and integrity of that data.
DCA	Department Control ACID. Individual who controls users, profiles, departments, and resources within their own department.
DDN	Defense Data Network. A portion of the Internet that connects to US military bases and concentrators. Used for non-secure communications.
DECC	Defense Enterprise Computing Center.

DECC-D	Defense Enterprise Computing Center-Detachment.
DII	Defense Information Infrastructure.
DISA	Defense Information Systems Agency.
DISAI	Defense Information Systems Agency Instruction.
DOD	Department of Defense.
DOD-CERT	Department of Defense Computer Emergency Response Team (formerly *ASSIST*).
DODICS	Department of Defense Interest Computer System.
DODIG	DOD Inspector General.
e-mail	Electronic mail.
ESM	External Security Manager.
GCS	Group Control System.
GNOSC	Global Network Operations and Security Center (formerly *GOSC*).
GOTS	Government-Off-The-Shelf.
GUI	Graphical User Interface.
Host	A computer that acts as a client and/or server.
I&A	Identification and Authentication.
IAM	Information Assurance Manager.
IAO	Information Assurance Officer. Term replaces PSAO (Primary Security Administration Office/Officer) formerly used to identify the organization (or individual) responsible for security administration on the platform.
IAW	In Accordance With.
Internet	Any collection of distinct networks working together as one. The Internet provides file transfer, remote logon, electronic mail, news, and other services.
IP	Internet Protocol. The most important of the protocols on which the Internet is based. An IP allows a packet to traverse multiple networks on the way to the packet's final destination.
IPL	Initial Program Load.
IPSC	Internal Product Security Control.
IUCV	Inter-User Communication Vehicle.
LAN	Local Area Network.
M-Time	The time a file was last modified.
MVS	Multiple Virtual Storage.
NCCF	Network Communications Control Facility.
NCSC	National Computer Security Center.
NIPRNet	Non-classified (but Sensitive) Internet Protocol Routing Network.
NSA	National Security Agency.
OASD	Office of the Assistant Secretary of Defense.
Octet	Set of eight (8) bits (i.e., a byte).
OS	Operating System.
PC	Personal Computer.

POC	Point of Contact.
Port	Number that identifies a particular Internet application. Also, a physical connection for an input/output channel.
Protocol	Set of rules governing how computers will act when communicating with each other. Protocols allow computers from different manufacturers to communicate.
PTF	Program Temporary Fix.
RACF	Resource Access Control Facility.
REXX	Restructured Extended Executor. A 4th generation VM programming language that also includes a language processor.
RNOSC	Regional Network Operations and Security Center (formerly *ROSC*).
RSA	Regional Support Activity.
RSCS	Remote Spooling Communications Subsystem.
SA	System Administrator.
SCP	System Control Program.
Server	Software that allows a computer to offer services to other computers. Also, the computer on which the server software runs.
SFS	Shared File System.
SFUG	Security Features Users Guide.
SIPRNet	Secret Internet Protocol Router Network.
SOP	Standard Operating Procedure.
SSO	Systems Support Office.
STIG	Security Technical Implementation Guide. A document describing the requirements and methodology for implementing security in the DISA environment.
TASO	Terminal Area Security Officer.
TCB	Trusted Computing Base.
TCP	Transmission Control Protocol. One of the protocols on which the Internet is based. TCP is a connection-oriented, reliable protocol.
Trusted System	A system that is itself STIG-compliant.
TSAF	Transparent Services Access Facility.
UDP	User Datagram Protocol. An Internet-based protocol that provides connectionless, unreliable communications.
User	Person or machine authorized to access a computer system.
Userid	User ID. Mechanism used to uniquely identify a user of system resources.
VAAP	Vulnerability Analysis and Assistance Program.
VCTS	Vulnerability Compliance Tracking System.
VM	Virtual Machine.
VMSES/E	Virtual Machine Serviceability Enhancements Staged/Extended (VMSES/E).
WAN	Wide Area Network.

Workstation	Powerful Personal Computer configured to access a network host.
WWW	World Wide Web. An Internet service that permits users to weave information and resources together by using hypertext links; a means to bypass publishers.

APPENDIX C. AREA OF RESPONSIBILITY AND VM POLICIES

Authority

- *IAOs will develop supplemental procedures, as required, in consonance with INFOCON guidance.*

Extensions

- *The IAO will maintain a file for each server/workstation that has deviations to security recommendations. The file will document each exception and will contain a risk assessment for each deviation that the site Commander has approved. Lack of such documentation will result in findings for non-compliant systems. 1.12 Extensions.*

Document Review Process

- *The IAO will ensure that the site maintains documentation on: system startup, shutdown, hardware configuration/reconfiguration, backup, recovery, physical security protection of the hardware configuration, security protection of the software used in the VM development/production environments, restricting access to the hardware components, restricting access to the functions of the master console from the local and/or remote operator consoles.*
- *The IAO will maintain a list of all of the ACPs used in the VM environment.*
- *The IAO will ensure that that site maintains a current list of the VM system files to include:* ***USER DIRECTORY, CONFIGURATION FILE, ACCOUNTING FILE, and ALTERNATE CONFIGURATION FILE.***
- *The site will maintain a current list of all* ***SYSTEM SOFTWARE*** *and* ***VENDOR SOFTWARE PRODUCTS*** *running in the VM environment.*

Privilege Classes

- *The local IAO will document and maintain any deviations from this standard.*
- *The IAO will ensure that modification/deletion to privilege user classes are in accordance with DISA standards.*
- *The IAO will implement controls to specify the valid users authorized to create and modify privilege user classes.*
- *The IAO will maintain the privilege user class requirements*

VM and Other Product Routines

- *The IAO will ensure that the mini disk containing the User Directory is password protected.*

Emergency Userids

- *The IAO will ensure that a password is associated with the* ***MAINT*** *userid.*

VM System Operator Userids

- *The IAO will ensure that a password is associated with the OPER userid.*
- *The IAO will ensure that the mini disks associated with the OPER userid are password protected.*

Password Controls
- *The IAO will ensure that all userids have associated passwords on the User Directory*
- ***The IAO will ensure that the mini disks associated with the MAINT userid are password protected.***
- *The IAO will ensure that all mini disks are password protected.*

Userid Controls
- *The IAOs will ensure that the values for these fields are maintained and current.*

Minidisk Controls
- *The IAO will ensure that any ESM file exceptions are documented and maintained.*
- *The IAO will review and approve all business requirement requests for hard-coded passwords.*

Standard Global Options (SETROPTS)
- *The IAO will ensure that GLOBAL OPTIONS are set in accordance with DISA requirements.*
- *The IAO will ensure that only authorized personnel are able to use the SETROPTS command.*
- *The IAO will ensure that RSCS nodes are protected using RACF resource classes.*
- *The IAO will ensure that Any CP command or DIAGNOSE code (including privileged commands and DIAGNOSE codes) are restricted to authorized personnel.*
- *The IAO will ensure that the creation, opening, and deletion of spool files are restricted using RACF classes.*
- *The IAO will ensure that the dumping and loading of spool files through the SPXTAPE and SPTAPE commands are restricted to authorized personnel.*
- *The IAO will ensure that UCV CONNECT and SEVER operations and certain VMCF functions are restricted.*
- *The IAO will ensure that **APPC/VM CONNECT** and **SEVER** operations are restricted using RACF classes.*
- *The IAO will ensure that the creation and deletion of logical devices is restricted to authorized personnel.*

Userid Controls
- *The IAO will ensure, that at a minimum, the above USER PROFILE fields are completed for each user on the system.*

Users
- *The IAO will ensure that a user profile exists for each user on the system.*
- *The IAO will ensure that all security-relevant events are audited.*

Batch Users
- *The IAO will ensure that rules exist in the RACF data base restricting surrogate processing.*

Emergency Userids
- *The IAO will ensure that emergency userids are restricted to authorized personnel and limited in duration.*

VM System Operator Userids
- *The IAO will ensure that all VM operators have assigned userids restricting, which commands they are able to enter.*

Password Guidelines
- *The IAO will ensure that password requirements are enforced.*

Password Exit Processing
- *The IAO will ensure that all exits are reviewed by FSO prior to implementation.*

Special Privilege Access
- *The IAO will restrict special privilege access to authorized personnel.*

Audit Privileges
- *The IAO will ensure that the FSO SRR team has Auditor privileges.*

File Controls
- *The IAO will ensure that file controls are enforced.*
- *The IAO will ensure that minidisk controls are enforced.*
- *The IAO will ensure that password controls are enforced on resources.*

Volume Controls
- *The IAO will ensure that all minidisks are protected in accordance with DISA requirements.*

Sensitive Utility Controls
- *The IAO will ensure that sensitive utilities and commands are password restricted.*

Console Controls
- *The IAO will ensure that all consoles are restricted to authorized personnel.*

CP Command Controls
- *The IAO will ensure that all operator commands are restricted the authorized personnel.*
- *The IAO will ensure that the CP DIAL and MSG commands are restricted and audited prior to their logging on.*

Security Administrators, Security Group Managers, and Directory Managers
- *The IAO will ensure that Security Administration is restricted to authorized personnel.*
- *The IAO will ensure that Security Group Administration is restricted to authorized personnel.*
- *The IAO will ensure that Directory Administration is restricted to authorized personnel.*

This page is intentionally left blank.