UNISYS

SECURITY TECHNICAL IMPLEMENTATION GUIDE

Version 7, Release 1

28 July 2005

Developed by DISA for the DOD

This page is intentionally left blank.

TABLE OF CONTENTS

SECTION **PAGE**

LIST OF TABLES

TABLES **PAGE**

TABLE OF FIGURES

SUMMARY OF CHANGES

Changes made since the previous release of the Unisys STIG (Version 6, Release 1, dated 22 July 2003) are listed below for the Unisys STIG, Version 7, Release 0.1 (dated 15 April 2005).

GENERAL CHANGES:

Added Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code to all policy bullets.

Changed all Form 41 and DISA Form 41 references to SAAR (System Authorization Access Request) except in the first occurrence.

Replaced Form 41 with DD Form 2875.

All bold emphasis removed from the text throughout this document.

All policy bullets have been rewritten to include the position of the individual responsible.

Marked ALN specific requirements and DISA site specific requirements.

Removed all references to Alternate Information Assurance Officer (AIAO).

All bulleted requirements that are actually exceptions to another requirement are removed and for this release will be treated as exceptions in the checklist.

Removed all references to DECC San Antonio as it no longer processes Unisys workloads.

Removed all references to DECC-Detachment Jacksonville as it no longer processes Unisys workloads.

Removed all references to Navy Civilian Personnel as it has been migrated to another platform.

Changed all references for SRR-NT Toolkit to SRR Manager Toolkit.

Removed all references to the size, shape and type of tapes used.

Removed UP (Univac Publication) from the front of all Unisys manual numbers as the designation is no longer used.

Attributed the development of utilities to SSO Montgomery where appropriate.

Removed all references to Vendor Integrity Statement(VIS).

SECTION 1. INTRODUCTION

Section completely rewritten to accommodate new Section 1 requirements.

SECTION 1.1 Background

Derived from old Section 1.9 Processing Environment. Added reference to ALN and DISA history.

Added a definition of System Administrator (SA) that reflects the definition found in DODI 8500.2 section 5.11 and stated this is what is meant by SA in this STIG.

Section 1.3 Scope

Derived from old section 1.3 Scope.

Section 1.7 Security Administration.

Removed section.

Section 1.14 Security Awareness and Training.

Removed section.

SECTION 2. UNISYS OPERATING SYSTEM INTEGRITY

Large portions of this section have been reworded or removed.

Section 2.1 Security Report Generation and Review

Derived from old section 1.8. Rewritten removing requirement to use SRR Tool kit, made more generic.

Section 2.2.2 Unisys Operating System Security Design

Derived from old section 1.11.

Section 2.2.3 Sotware Integrity

Removed NIAP requirement.

Section 2.2.3.3.2 SIMAN Environment Settings

Added settings for HMP IX 8.1 and above.

Section 2.2.3.4 GEN Tags

Removed last sentence prior to Table 1.

Added configuration values for HMP IX 8.1 where appropriate in Table 1 and 2.

Section 2.2.3.4.1 Tip Session Control

New section.

Section 2.2.3.5 Government Warning Message

Removed sample warning message.

Section 2.3 System Control Requirements

Removed section.

Section 2.4 Continuity of Operations Processing

Removed section.

Section 2.4 Security Patches and Obsolete Software.

New section.

Section 2.5 Joint Task Force Global Network Operations-Computer Emergency Response Team.

New Section.

Section 2.6 Inadvertent Classified Processing

Renumbered from 2.4.3.

Section 3 Access Controls

Section 3.1.2 Investigation Requirements

Section removed.

Section 3.1.2.3 Batch Only Userids.

Removed specific directions for filling out SAAR.

Section 3.1.3 User Information Requirements

Removed specific directions for filling out SAAR.

Section 3.1.3.2 Deactivating Userids

Removed note about Unisys allowing deletion of userids in HMP IX 7.0 as Unisys removed the ability in HMP IX 7.1

Added note stating that JX$$0000*00. is a file supplied by SSO Montgomery to sites supported by SSO Montgomery.

Section 3.1.3.4 Rehosting Userids

Added note stating rehosting is a procedure used by sites supported by SSO Montgomery.

Section 3.1.3.8 System Userids

List entry “c” significant rewrite to accommodate the “Unencrypted File Transfer Protocol (FTP) and Telnet” white paper.

List entry “d” added.

Section 3.1.3.9 Standard Userids

Added an exception for the new CAMS system.

Section 3.1.5.1 Common System Userids

Added new common userids to tables.

Section 3.1.5.3 System or Hard-coded Demand Userids

Changed the DPS profile to profile 5 with SSBYCOMP.

Section 3.1.6 Userids For Troubleshooting Problems

Section removed.

Section 3.1.6.3.5 Extended Password Settings for FTP Userids

Changed section name to FTP Userids.

Removed all references to acknowledgement of risk letters.

Section 3.1.7 Temporary Access Userids

Section removed.

Section 3.1.8 Permanent Userid Access

Section removed.

Section 3.1.6 Password Controls

Added HMP IX 7.0 and above requirements.

Section 3.1.6.5 Extended Password Settings for FTP userids.

Rewritten to accommodate updated FTP guidance.

Section 3.4.8 Attaching ACRs

Modified to state profile 1 or 2 can attach an ACR to a file and profile 1 security administrator can attach an ACR to a userid.

Section 4 Management Of The Unisys System Security Environment

Section 4.1.3 Backup Frequency and Offsite Storage

Section removed.

Section 4.5 Reinitializing SACRD$

Added warning that this does not work on HMP IX 7.0 or later.

Section 5 DATABASE MANAGEMENT UTILITIES

Section 5.6.1 Application Group Names

New table for Table 30.

Section 5.6.4 Securing UREP Configuration Entity with UREP Groups

New section.

Section 6 MASS STORAGE MANAGEMENT

No significant changes.

Section 7 TAPE MANAGEMENT/AUTOMATED CARTRIDGE SILO UTILITIES

Removed reference to CSC 2R6.

Added changes for CSC level 4R1.

Section 7.2.4.2 Input Tape Bypass Messages

Removed list of known exceptions to automatic refusal and required the sites to develop and maintain their own list.

Section 7.4.3 DNMC CSC Parameter file

Section delete as DNMC no longer has a system.

Section 8 SYSTEM PROCESSORS

Section 8.1.1 Overview

Added RKY T,B <ALN or ELC> keyin to Table 31.

Section 8.3 FTP and Telnet

Added additional information from the FTP and Telnet White Paper.

Section 8.3 TAS FTP

Section renumbered and renamed 8.3.1 TAS FTP – ALN.

Added note dealing with TAS selection of only the first account number found on a userid that is allowed multiple accounts.

Section 8.4 Virtual FTP Userids

Section number has been changed to 8.3.2.

Removed reference to DISA memo 9 August 2000.

Section 8.4.3 Securing the DDP Log and Trace Files

Added instructions on how to find the qualifier for the files.

Section 8.6 Print Viewing Utilities

Moved to section 12.7 Print Viewing Utilities.

Section 8.8.4 Additional MAPPER Identification And Authentication – DNMC Sites

Deleted this section as there are no DNMC MAPPER application sites left.

Section 8.9.1 Securing Sightline and Torch Files – ALN and DFAS-IN Sites

Section number now 8.7.1

Deleted file DATAMETRICS*PMS-CMyy.

Add file DATAMETRICS*TORCH.

Section 8.9.2 Securing Sightline and Torch Files – DNMC

Section delete.

Section 8.11.3 DPS Password File – DNMC and DFAS-IN

Section is now 8.9.3 DPS Password File – DFAS-IN.

Last paragraph dealing with DPS as the primary identification and authorization entity. TIP Session Control is required and is the primary identification and authorization entity on the system. This paragraph is obsolete.

Last bullet deleted as it dealt with DPS as the primary identification and authorization entity.

Section 9 THE SCHEDULER

Section 9.3.1 Site Scheduler Security Profiles

Removed restriction to the number of users authorized at this level. Any number can be assigned if IAM approves. Synchronized this change with the rest of Section 9.

Section 10 WebTS

Section reworded to state that there will be no web server specific documentation in this STIG.

Section 11 TELECOMUNICATIONS SECURITY

Added warnings for discontinuance of support by Unisys for Telcon and CMS 1100.

Section 12 SYSTEM PRINT UTILITIES

Section 12.1.2.3 SEND Statement

Second bullet, changed “name” to “destination application name”.

Section 12.3 QTPIE

Section name changed to QTPIE – ALN.

Section 12.5 AB Utilities and Routing Tables

Name changed to AB Utilities and Routing Tables - ALN

Section 12.6.1.2 Userid Requirements

In the note, last paragraph before bullets, change account to userid.

Section 12.6.2.1 System Requirements

Changed to generic Windows and removed redundant STIG compliance.

Section 12.6.2.1.2 Mail Requirements

Section removed.

Section 12.6.2.1.2 Print Requirements

Change will to should and removed bullet.

Section 12.6.2.1.3 DEPCON Configuration

Deleted the sentence “The following parameters will be configured.”

Section 13 SOFTWARE DEVELOPMENT

Section 13.1

Reworded to better clarify.

Section 14 UNISYS SECURITY READINESS REVIEW PROCEDURES

Section Removed.

APPENDIX A RELATED PUBLICATIONS

Publications added and removed.

Version numbers and dates for STIGs changed to “current version”

APPENDIX B GLOSSARY OF ACRONYMS AND TERMS

Many changes made review.

APPENDIX C ACCESS AND LOCATION NUMBER INFORMATION

Bulleted policy items removed.

Site and AIS tables delete, html reference to Montgomery site for current tables left.

Consolidated Air Force military and civilian personnel system deleted.

APPENDIX C.2.1 Userid Parameters

Subsection b last sentence HQ SSG/PM is changed to SSO Montgomery.

APPENDIX C.2.1.1 Format

Sub paragraph a deleted and phrase "For all other non-CAMS userids," from subparagraph b.

APPENDIX C.9

Section obsolete and deleted as it deals with Navy Civilian Personnel which is no longer on a Unisys platform.

APPENDIX D. DNMC SITE SPECIFIC INFORMATION

Site and AIS tables delete, html reference to Montgomery site for current tables left.

APPENDIX D.3 Alternate Runids

Remove all references to DECC-Detachment San Diego and Infoquest.

APPENDIX E. DFAS-IN SITE SPECIFIC INFORMATION

APPENDIX E.1 DFAS-IN Naming Standards

Deleted subparagraph b and removed the subparagraph a designation from the remaining paragraph.

APPENDIX E.1.1 DECC-Detachment Indianapolis

Section deleted.

APPENDIX E.1.2 DFAS-Indianapolis

Added Table 48.

APPENDIX F. INADVERTENT CLASSIFIED PROCESSING PROCEDURES

Name now INADVERTENT CLASSIFIED PROCESSING PROCEDURES – ALN.

Multiple changes from SSO Montgomery.

APPENDIX G SAMPLE SECURITY LETTERS

Section removed.

APPENDIX G. SIMAN

No significant changes.

APPENDIX I DOD CERT BULLETINS

Section removed.

APPENDIX J VCTS REPORTS

Section removed.

APPENDIX K USER ACCESS INFORMATION MEMO

Section removed.

1. INTRODUCTION

This document will define the minimum requirements, standards, controls, options and procedures that have to be in place for the Unisys Executive and standard system software to meet MAC II sensitive compliance as discribed in the DODI 8500.2. Individual sites may implement additional security measures as deemed necessary

1.1 Background

There exists a large amount of DOD transaction processing workload which is accomplished on Unisys OS2200-based mainframe systems or the ClearPath IX-based enterprise servers. The Unisys Executive, or operating system, can provide a MAC II sensitive compliance. The operating system, as released from Unisys, provides extensive controls to ensure integrity of the operating environment. Unisys has developed documentation and procedures to assist in enforcing this integrity.

The original target audience for this Security Technical Impementation Guide (STIG) was DISA facilities using the Access and Location Number (ALN) modification of the standard Unisys software. As a consequence, this STIG contains many ALN specific policies, procedures and settings.

DODI 8500.2 paragraph 5.11 Privileged User with AI responsibilities (e.g., System Administrator) defines the responsibilities and duties for a System Administrator(SA). This STIG, when it uses the term SA, will be referring to an individual who's position fulfills this set of duties and responsibilities.

It should be noted that FSO support for the STIGs, Checklists, and Tools is only available to DOD Customers.

1.2 Authority

DOD Directive 8500.1 requires that "all IA and IA-enabled IT products incorporated into DOD information systems shall be configured in accordance with DOD-approved security configuration guidelines" and tasks DISA to "develop and provide security configuration guidance for IA and IA-enabled IT products in coordination with Director, NSA." This document is provided under the authority of DOD Directive 8500.1.

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.

1.3 Scope

This document applies to all DOD-owned and/or administered Unisys systems controlled by DOD sites, Systems Support Offices (SSOs), and other organizations, hereinafter referred to simply as sites. The requirements set forth in this document are for the Unisys hardware (U2200 mainframes or ClearPath IX enterprise servers), Executive, and standard system software (all software not written or procured by individual AISs) hereinafter referred to simply as Unisys. Security measures implemented by AISs may augment, but not circumvent, Executive security controls. The security exposures outside the scope just defined (i.e., network infrastructure, personnel security, etc.) are not addressed in this document. As pointed out previously, this STIG still contains many ALN specific policies, procedures and settings. If a requirement is marked as ALN specific or DISA site specific then it is required only for ALN or DISA sites.

1.4 Writing Conventions

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

A reference that uses "**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 will adhere to the instruction as written. Only an extension issued by the Designated Approving Authority (DAA) will table this requirement. The extension will normally have an expiration date, and does not relieve the IAO from continuing their efforts to satisfy 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. Nevertheless, all reasonable attempts to meet this criterion will be made.

For each italicized policy bullet, the text will be preceded by parentheses containing the italicized Short Description Identifier (SDID), which corresponds to an item on the checklist and the severity code of the bulleted item. An example of this will be as follows "(*G111: CAT II*). "If the item presently has no Potential Discrepancy Item (PDI), or the PDI is being developed, it will contain a preliminary severity code and "N/A" for the SDID (i.e., "*[N/A: CAT III]*").

1.5 Vulnerability Severity Code Definitions

Category I	Vulnerabilities that allow an attacker immediate access into a machine, allow superuser access, or bypass a firewall.
Category II	Vulnerabilities that provide information that have a high potential of giving access to an intruder.
Category III	Vulnerabilities that provide information that potentially could lead to compromise.
Category IV	Vulnerabilities, when resolved, will prevent the possibility of degraded security.

Table 1-1. Vulnerability Severity Code Definitions

1.6 STIG Distribution

Parties within the DOD and Federal Government's computing environments can 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 http://iase.disa.mil/.

1.7 Document Revisions

Comments or proposed revisions to this document should be sent via e-mail to fso_spt@disa.mil. DISA FSO will coordinate all change requests with the relevant DOD organizations before inclusion in this document.

This page is intentionally left blank

2. UNISYS OPERATING SYSTEM INTEGRITY

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

2.1 Security Report Generation and Review

The IAO will proactively pursue security issues. Passive scanning of the security environment (reacting to blatant security violations) is inadequate. This presents a requirement to actively review the system security posture for potential security weaknesses.

- *(A104.010.00: CAT II) The IAO will regularly review the system security posture for potential security weaknesses.*

2.2 System Level Integrity

System level integrity is comprised of protecting hardware and software resources.

2.2.1 Hardware Integrity

Every operating environment is composed of hardware resources. These include facilities such as central processing units (CPUs), instruction processors (IPs), disk storage devices, tapes, consoles, printers, and communication devices. Currently, sites utilize U2200 mainframe systems or ClearPath enterprise servers for Unisys processing.

When handled improperly, these components can create exposures within the operating environment that cannot be controlled with any software process. For instance, the system console can be used to perform unrestricted keyins to up or down devices, stop the system, or modify the operating system.

This document is not written attempting to address the resolution of the integrity of the hardware environment. Access controls will be designed and implemented as part of the physical security plan for the site. The concept of identification and authentication will be employed as the principal mechanism for controlling access to these hardware resources.

2.2.2 Unisys Operating System Security Design

The Unisys Executive is tightly linked to the hardware platform it is executing on and provides security mechanisms for all Interfaces that control the hardware. All entities, including users and processes, which perform actions, are defined as subjects. All entities acted upon (files, tapes, hardware, userids, resources, etc.) are defined as objects. The Executive provides for MAC II sensitive level control over subject-object interaction via Interface and Privilege combinations as well as other access controls specific to individual features. To implement this MAC II sensitive level control, Security Option 1 (SECOPT1) will be configured in the operating system.

- *(S104.150.00: CAT I) The IAO will ensure Security Option 1 is configured in the Unisys operating system.*

2.2.3 Software Integrity

The *OS2200 Security Planning and Administration Reference Manual* (7831-0307) outlines the philosophy of the Unisys Operating System security architecture. This manual was superseded by the interactive document *Security Administration for ClearPath OS 2200 Help* (7862 1760) in release HMP IX 6.1 and all subsequent releases. Controlling integrity exposures is the responsibility of individual system subjects. The Unisys Executive and the accompanying standard system software provided by Unisys provide tight integrity controls when properly configured. It is accepted that some sites may deviate from commercial-off-the-shelf (COTS) system software and products with the introduction of local code changes to support individual requirements. Only authorized system software and products will be installed on the system.

To facilitate maintaining operating system integrity, the following general guidelines will be followed:

a. SOLAR and COMUS are the current standard Unisys system software installation processors. The use of SOLAR is increasingly common, but COMUS is still used for some installations. All products with the capability of being installed via COMUS or SOLAR will be installed and maintained via that method to ensure control and tracking of maintenance and changes. In either case, the SYS$*DATA$.CO$INSTALL$/COMUS$ element will contain a list of all SOLAR/COMUS installed products.

b. Products that cannot be installed via COMUS or SOLAR will be installed and maintained using procedures that will ensure proper control and tracking of changes. These procedures may include the use of the Base Level Integrated Support System (BLISS), SETUP and COPY,G tapes, and supporting release documentation and instructions.

c. All products that bypass normal Executive subject/object validation checks will be certified to ensure system integrity is not compromised.

d. All system software administered and/or installed by site personnel will be secured from modification or destruction by unauthorized personnel. This may be accomplished through the use of any of the Unisys Discretionary Access Control (DAC) mechanisms identified throughout *Section 3, Access Controls*, in this document. As stipulated above, only authorized system software and products will be installed on the system.

The guidelines defined in the rest of this STIG assume a Unisys Operating System level of HMP IX 6.1 unless otherwise noted.

- *(S103.550.00: CAT II) The IAO will ensure the security attributes associated with system software files are not modified or removed.*

- *(S103.564.00: CAT II) The IAO will ensure only authorized system software and products is installed on the system.*

2.2.3.1 Interfaces

Interfaces, formerly known as Executive Requests (ERs), are system calls that programs make to the operating system. These Interfaces provide services in the form of input/output operations, authentication, allocation and validation of resources, etc.

For sites that have access to the source release software, the Exec contains a list, generated in Exec element SSINIT, that identifies secured and enforced Interfaces. All Interfaces listed in SSINIT are secured. Secured Interfaces appear in the SIMAN screens that list the Interfaces that can be given to a userid. The site IAO can secure additional Interfaces, causing them to appear in the SIMAN screen, but this will be done with the coordination of the SSO Montgomery Security Office.

Secured Interfaces can be ENFORCED, ALWAYS ENFORCED, or UNENFORCED. As expected, ALWAYS ENFORCED Interfaces cannot be UNENFORCED. The site IAO can UNENFORCE Interfaces that are ENFORCED and vice versa; however for DISA sites, this will be done with the coordination of the SSO Montgomery Security Office. The statuses of initially secured and enforced Interfaces are identified in the *OS2200 Security Planning and Administration Reference Manual (7831 0307).* The IAO will ensure the minimum enforcement of Interfaces, as detailed in *Section 3.1.8.7, Secured Interfaces*, of the STIG, is not altered.

- *(S104.140.00: CAT II) The IAO will ensure security related Executive Interfaces are secured on the system.*

2.2.3.2 Executive Privileges

Executive Privileges are used to secure Executive Interfaces and act as validation mechanisms for processors. For instance, consider an interface that allows a user to bypass tape validation. This interface will be useless unless the executing process also has a corresponding privilege to activate that interface. Similarly, certain Interfaces may allow more functionality when called by a subject possessing a broader range of privileges.

For sites that have access to the source release software, the Exec contains a list, generated in Exec element SSINIT, that identifies secured and enforced Executive Privileges. All Privileges listed in SSINIT are secured. Secured Privileges appear in the SIMAN screens that list the Privileges that can be given to a userid. The site IAO can secure additional Privileges, causing them to appear in the SIMAN screen; this will be done with the coordination of the SSO Montgomery Security Office.

Secured Privileges can be ENFORCED, ALWAYS ENFORCED, or UNENFORCED. ALWAYS ENFORCED Privileges cannot be UNENFORCED. The site IAO can UNENFORCE Interfaces that are ENFORCED and vice versa; however, this will be done with the coordination of the SSO Montgomery Security Office. At the current time, most Privileges are ALWAYS ENFORCED or ENFORCED. There are only two Privileges that are not enforced and they are SSTIPSENDMSG and SSTIPGETMSG. The statuses of initially secured and enforced Privileges are identified in the *OS2200 Security Planning and Administration Reference Manual*

(7831 0307). The IAO will ensure the minimum enforcement of Privileges, as detailed in *Section 3.1.8.8 Secured Privileges*, of this STIG is not altered.

- *(S104.140.00: CAT II) The IAO will ensure security related Executive Privileges are secured on the system.*

2.2.3.3 SIMAN

2.2.3.3.1 Overview

Prior to the implementation of "Security for the 21st Century", a major modification to Unisys system security first introduced in general release HMP IX 7.0, the Site Management Complex (SIMAN) is the sole interface to the Unisys Operating System security system. SIMAN provides both a full screen and syntactical interface to allow setup and modification of the system environment, security environment, userids, accounts, etc.

With the release of HMPIX 7.0, Security Administration for ClearPath OS2200 (SecAdmin) was included as an alternative to SIMAN for the maintenance of the security system. Since the settings controlled by both products are the same and SIMAN being the legacy approach, information given here will remain SIMAN specific until SecAdmin is in wider use. Significant features of "Security for the 21st Century" will be noted but cannot be used on general release systems prior to HMPIX 7.0.

2.2.3.3.2 SIMAN Environment Settings

Only the Master userid and SIMAN administrator userids will be allowed to update the SIMAN environment. The following SIMAN environment settings will be configured on all site systems:

Accounting and resource control (ON)
Enable quota set usage (ON)
Enable Account information screen (ON or OFF)
User identification and maintenance (ON)
Extended security and access control (ON)
Enable user information screen (ON or OFF)
Account usage restricted to specified userids (ON)
Verify userids under accounts (ON)
Verify accounts under userids (ON)
Disable userid validation (OFF)
Notify console for undefined userid (ON), Display to user (OFF)
Notify console for invalid password (ON), Display to user (OFF)
Maximum days of inactivity (35)
Maximum invalid passwords (3)
Maximum times password-expired notice may be ignored (0)

For release HMP IX 8.1 the following settings where added to the SIMAN environment settings.

Traditional Authentication Allowed (OFF)

Retain Clear Text Passwords (OFF)
Open Session Control (OFF)

NOTE: On the Default Application Access Screen, since it is easy to fail to remove access to default application groups, "no application groups will be selected". Normally access to application groups will only be granted on a userid by userid basis.

- *(S103.490.00: CAT I) The SA will ensure only the Master userid and SIMAN administrator userids are allowed to update the SIMAN environment.*

- *(S104.130.00: CAT II) The SA will ensure the SIMAN environment is properly configured on the system.*

2.2.3.4 GEN Tags

When the Unisys Executive is generated (GENNED), input parameters are derived from many files and elements. Site-definable parameters are known as GEN tags. It has been determined that as a minimum, certain GEN tags have to be set to specific values to meet the MAC II sensitive level security specifications. Refer to *Table 2-1. GEN Tag Specifications~~Table 2-1. GEN Tag Specifications~~~~Table 2-1. GEN Tag Specifications~~*, for a list of GEN tags and their required settings. GEN tags SECURITY_OPT_1_CTRL and EXERR_054_FOR_ALAT will always be set to TRUE. On the DFAS-IN (Indianapolis) domain, the GEN tag FILES_PRIVATE_BY_ACCOUNT is authorized a setting of TRUE. There is code within the DFAS-IN (Indianapolis) applications that requires this parameter to be set to TRUE for the applications to work correctly.

The system GEN tag RESIDUE_CLEAR setting of FALSE is for performance reasons. If it is set to TRUE this will not be a finding but the site may suffer from sever performance degradation.

LONG TAG NAME	*SHORT TAG NAME*	*VALUE [brackets 8.1 value]*
QUOTA_LEVEL	ACCNTON	Greater than 0
ACCNTG_CLASS_LOGGED	LOGACCTON	TRUE
CONSOLE_CLASS_LOGGED	LOGCONSOLEON	TRUE
EXERR_054_FOR_ALAT	ALATXR	TRUE
FIXED_MS_FILE_CLASS_LOGGED	LOGFIXMSON	TRUE
LOG_FILE_HDR_CLASS_LOGGED	LOGFILEHDRON	TRUE
REJECT_OPTION_CONFLICTS	REJCONFLTOPT	FALSE
SYSTEM_HISTORY_CLASS_LOGGED	LOGSYSHISTON	TRUE
AUTOMATIC_TAPE_LABELING	TLAUTO	TRUE or 1
DEFAULT_MAX_DAYS_PASSWORD	MAXPASSDAY	90
DEFAULT_MIN_DAYS_PASSWORD	MINPASSDAY	1
DELAYED_SIGN_ON_SOLICITATION	DELAYSOL	FALSE
EBCDIC_TAPE_LABELS	TLEBCDIC	0
FILES_PRIVATE_BY_ACCOUNT (DISA and ALN Requirement)	SSPBP	FALSE or 0
MAX_SIGN_ON_ATTEMPTS	MAXATMP	3
MIN_PASSWORD_LENGTH	MINPASSLEN	6 [>= 8 <= 18]
MAX_PASSWORD_LENGTH	MAXPASSLEN	[>= MINPASSLEN <= 18]
PRELABELED_TAPES_REQUIRED	TLSIMP	TRUE
TAPE_ACCESS_RESTRICT_BY_ACCOUNT	TPOWN	FALSE
TSS_FILE_VERSION	TSS$VER	01(TAG DOES NOT EXIST AFTER LEVEL 7.0)
NPE_CONTROL	NPECTRL	1
RESIDUE_CLEAR	RESDUCLR	FALSE
SECURITY_OPT_1_CTRL	(none)	TRUE
SRSF_SYS_HIGH;	SRFHGH	FALSE
OPERATOR_ASSIST_UNDEF_ACCOUNT	RESTRICT	TRUE

Table 2-1. GEN Tag Specifications

NOTE: TSS_FILE_VERSION (TSS$VER) is no longer used in HMP IX 7.0 and above.

The following GEN tags should be set to the values indicated in *Table 2-2. Recommended GEN Tag Specifications*~~*Table 2-2. Recommended GEN Tag Specifications*~~~~*Table 2-2. Recommended GEN Tag Specifications*~~. These values are not required because extensive testing of existing applications would be required to verify that these setting do not break a currently working application.

LONG TAG NAME	*SHORT TAG NAME*	*VALUE [brackets 8.1 value]*
SRSF_SYS_HIGH	SRFHGH	TRUE
TIP_FILE_SECURITY	TFSEC	TRUE
OWNED_FILE _READ_WRITE_KEYS	OWNEDRWKEY	[TRUE]
SUBSYSTEM_ENTRY_PROTECTION	SSPROTECT	TRUE
COMPOOL_DISABLED	CMPDIS	TRUE

Table 2-2. Recommended GEN Tag Specifications

- *(S104.150.00: CAT I) The IAO will ensure the GEN Tag SECURITY_OPT_1_CTRL is set to TRUE.*

- *(S104.160.00: CAT I) The IAO will ensure the GEN Tag EXERR_054_FOR_ALAT is set to TRUE.*

- *(S104.170.00: CAT II) The IAO will ensure the GEN Tag QUOTA_LEVEL is set greater than zero (0).*

- *(S104.170.00: CAT II) The IAO will ensure all other security related GEN Tags are set to the required values.*

NOTE: The DFAS-IN (Indianapolis) domain is authorized to set the tag FILES_PRIVATE_BY_ACCOUNT to a value of TRUE.

2.2.3.4.1 TIP Session Control.

Transaction Processing (TIP) Session Control will be configured on for all application groups.

- *(S103.590.00: CAT II) The IAO will ensure TIP Session Control is configured on for all application groups.*

2.2.3.5 Government Warning Message

In accordance with CJCSM 6510.01 dated March 25, 2003, the system will present the standard government warning message prior to sign-on solicitation on TIP, Demand, and FTP sessions. The log-on notice and consent banner, as a minimum, must advise users of the following:

a. The system is a DOD system.

b. The system is subject to monitoring.

c. Monitoring is authorized in accordance with applicable laws and regulations and conducted for purposes of systems management and protection, protection against improper or unauthorized use or access, and verification of applicable security features or procedures.

d. Use of the system constitutes consent to monitoring.

e. This system is for authorized US government use only.

The warning banner will also be displayed after a successful log-on and will remain displayed on the user's screen until a keystroke is entered. This serves as an auditable event that the banner could be read.

- *(S103.070.00: CAT II) The IAO will ensure the Standard Warning Message regarding authorized use of computers is displayed prior to sign-on solicitation or after sign-on completion on TIP, Demand, and FTP sessions.*

- *(S103.072.00: CAT III) The IAO will ensure the Standard Warning Message regarding authorized use of computers is displayed prior to sign-on solicitation on TIP, Demand, and FTP sessions.*

- *(S103.074.00: CAT III) The IAO will ensure the warning banner contains the five points required by CJCSM 6510.01 dated March 25, 2003.*

- *(S103.076.00: CAT III) The IAO will ensure the warning banner is displayed after a successful log-on and remains displayed on the user's screen until a keystroke is entered.*

2.3 Data Level Integrity

It is the responsibility of the respective application and system software developers (including vendor provided software) to certify that there is no malicious code in the software that is released to operational locations. DISA sites supported by SSO Montgomery will not add programs to system software or library files released by SSO Montgomery since this invalidates the SSO Montgomery security certification. If a site has a need for certain system-type programs, they will present this requirement to the site Configuration Control Board, test and certify these programs, and then load these programs to a site unique system file. Depending on the capabilities of the software, the site will implement appropriate security controls on this file.

It is the responsibility of the data owner to ensure released software is not modified in a manner that can corrupt the integrity of owned data or interfere in the verification of owned data (for example, databases).

The site is responsible for implementing written procedures to ensure that all media (disk and tape) leaving the site is degaussed, erased, randomly overwritten via a disc prep, or reformatted prior to salvage or off-site maintenance, or otherwise rendered unreadable.

- *(S103.560.00: CAT II) The SA or IAO will ensure unauthorized programs are not added to system software or library files or the site CCB.*

- *(A102.250.00: CAT II) The IAO will ensure written procedures exist to ensure all unclassified tapes, disks, and other storage media is cleared prior to off-site maintenance or salvage.*

- *(A102.260.00: CAT II) The IAO will ensure written procedures exist to ensure all classified tapes, disks, and other storage media, if applicable, are rendered unreadable by approved methods prior to off-site maintenance or salvage.*

2.4 Security Patches and Unsupported software

The SAs and IAOs should regularly check Unisys support web sites for information on new security patches that are applicable to their site. All applicable security patches will be applied to the system. A security patch is deemed applicable if the product is installed, even if it is not used or is disabled.

FSO does not test or approve patches or service packs. It is the site's responsibility to test vendor patches within their test environment.

The SAs and IAOs will ensure that obsolete system software is removed from the system and that there exist a plan to upgrade to newer releases of software prior to the date Unisys drops security patch support for a release level.

- *(N/A: CAT I) The IAO or SA will ensure all security related patches supplied by Unisys are located, applied and tested.*

- *(N/A: CAT I) The IAO or SA will ensure unsupported system software is removed or upgraded prior to a vendor dropping support.*

- *(N/A: CAT II) The IAO will ensure the site has a formal migration plan for removing or upgrading OS systems prior to the date the vendor drops security patch support.*

2.5 Joint Task Force Global Network Operations-Computer Emergency Response Team

The Joint Task Force Global Network Netdefense (JTF-GNO) is the approved DOD source for vulnerability updates. The World Wide Web address is www.cert.mil. The site will set up a policy to ensure that JTF-GNO bulletins are being implemented in a timely fashion.

- *(A105.030.00: CAT I) The IAO will ensure JTF-GNO bulletins are being implemented in a timely fashion.*

2.6 Inadvertent Classified Processing

The site will have procedures for use in case of the introduction of classified information into the system. While this is a rare situation, it has occurred in the past. For instance, B2 pilots entering classified information as part of their flight plan. These procedures will encompass system isolation, disk scrubbing, and validation. Generalized procedures are provided at *Appendix F, Inadvertent Classified Processing Procedures*, and may be tailored for a site's specific requirements or situation.

- *(A102.240.00: CAT II) The IAO will ensure there are written procedures for handling the introduction of classified material into the system.*

3. ACCESS CONTROLS

This section discusses discretionary access control (DAC) and the identification and authentication (I&A) criteria necessary to ensure that access to system resources is effectively managed and controlled for the Unisys system.

3.1 Userid Controls

Every action performed on a Unisys system is accomplished with a userid or an agent of a userid. Every time a file is created, modified, assigned, written to, or deleted, it was done by a userid. A userid links an action to a specific user. A standard userid is defined as having a certain set of characteristics. This is simplified by the user profile system, as outlined in *Section 3.1.8, User Profile System*, in this document.

Each userid that exists on the system will be used by one and only one person. The security requirements as outlined in *DOD 8500.2* prohibit sharing of userids. Sharing of userids prevents positive identification of user actions.

- *(S104.710.00: CAT II) The IAO will ensure group and shared userids are not used on the system.*

3.1.1 Userid Access Request Forms

The System Authorization Access Request (SAAR), DD Form 2875 dated MAY 2004, or an equivalent form, will be used when assigning userids to new users. If previous forms are not equivalent to the SAAR or if no form exists on file for current users, a new SAAR will be completed. This applies to contractor personnel as well. The original SAAR can be kept at the level of the authorizing agent, IAO, TASO or other locally specified position; however, the IAO will ensure these forms are readily available if requested.

- *(A102.020.00: CAT III) The IAO will ensure all users submit a System Authorization Access Request (SAAR), DD Form 2875 dated MAY 2004, (or equivalent form) for access to DOD information systems. .*

- *(S104.010.00: CAT II) The IAO will ensure all SAARs or their equivalent forms are available if requested.*

3.1.2 Individual Accountability of Users

All users will have unique userids for accessing the system. The IAO will have accurate and readily available information to tie each userid on the system to a specific individual or process. At a minimum, a copy of the individual's SAAR or grandfathered access form will be available within four hours of a request for information. At the discretion of the IAO, TASO, or other locally designated personnel, the copy of the SAAR or grandfathered access form can have all but the last four of the individual's Social Security Number blacked out. Do not alter the original SAAR. The IAO will be cognizant of the applications, developers, and customer supported sites running on the system. The IAO will also maintain current information records on all

userids/subadministrators that the IAO directly administers. As a minimum, this will include all data on the SAAR

- *(S104.010.00: CAT II) The IAO will have accurate and readily available information to tie a userid to a specific individual or process.*

- *(A101.030.00: CAT II) The IAO will be cognizant of the applications, developers, and customer supported sites running on the system.*

- *(A102.050.00: CAT II) The IAO will maintain current information records on all userids/subadministrators the IAO directly administers.*

3.1.2.1 Operator Userids

All operators that need to have access to the system outside the console area (reference *Section 3.1.8.11, Unisys User Profile Distribution Guidelines)* will have unique userids.

- *(S101.010.00: CAT II) The IAO will ensure each operator who needs access to the system outside the console area has a unique userid.*

3.1.2.2 TIP Userids.

All TIP users will be authenticated to single user granularity. This includes userids used for both TIP session control and/or application identification and authentication.

- *(S103.590.00: CAT I) The IAO will ensure each TIP user has a unique userid.*

3.1.2.3 Batch Only Userids

If a userid is for production use and will only be used to run batch jobs, it will be restricted to batch access only via the SIMAN record. As per Section *3.1.3 User Information Requirements* the site will document this userid(s) on a SAAR.

The form will include the following information.

- The system name
- How long the userid will be required (if permanent, indicate this fact)
- Name, location, and work phone of a point of contact within the organization serviced by the userid
- Identify the activity wanting the data.
- Identify the data being accessed.

- *(A102.070.00 and S104.110.00: CAT III) The SA will ensure standard userids used to start batch jobs on the system are limited to batch only access.*

- *(A102.020.00: CAT II) The IAO will ensure standard userids used to start batch jobs on the system are documented on a SAAR in accordance with this STIG.*

3.1.2.4 Change in User Access Requirements

The IAO will document and implement a procedure to ensure that the implementer of the procedure is informed of a user's transfer, retirement, administrative action or extended absence so the userid can be disabled. This document will encompass userid deactivation procedures (see *Section 3.1.4.2*, Deactivating Userids), removal or modification of ACRs that reference the userid (see *Section 3.4.1.3.1 Userid*) and, if necessary, removal/reassignment of files that are owned by the userid.

- *(A102.100.00: CAT II) The IAO will document and implement a procedure to ensure prompt notification of a user's transfer, retirement, administrative action, or extended absence so the userid can be disabled.*

- *(A102.110.00: CAT II) The SA will ensure ACRs on the system that contain hard-coded userid names in the condition field are updated when the userid is disabled or deactivated.*

3.1.3 User Information Requirements

The System Authorization Access Request (SAAR) will be used for all users (a person or an application) accessing applications running on DOD owned or operated platforms

- *(A102.020.00: CAT III) The IAO will ensure the DD Form 2875 is used as the System Authorization Access Request (SAAR) for all users (person or application) accessing applications running on DOD owned or operated platforms.*

3.1.3.1 Creating Userids

The IAO creates userids for the system, as required by users, to perform only those tasks required by the users to accomplish their mission. The IAO uses the SIMAN processor to install and administer userids.

3.1.3.2 Deactivating Userids

Once the user no longer requires access to the system, the userid is deactivated, disabled, or assigned to another user. Due to limitations in the way the SACRD$ security file is updated, userids will not be deleted. If a userid were to be deleted it would remain in the SACRD$ file flagged as deleted and could never be reused. To properly deactivate a userid, the IAO will use the runstream JX$$0000*00.PROFILE/DACT. This runstream removes the TIP and Batch run modes, sets the Demand mode with an @FIN in the control image, and re-profiles the userid to a Profile 9. These actions render the userid unusable since it cannot be used to sign on to the system. Reference *Section 3.1.4.2, Deactivating Userids*, for more information.

NOTE: The JX$$0000*00. file is provided DISA sites supported by SSO Montgomery by SSO Montgomery. If the user does not have access to this file they will need to manually perform the actions performed by this runstream.

3.1.3.3 Recycling Userids

Since userids will not be deleted (see *Section 3.1.3.2, Deactivating Userids*), and there are only so many combinations available for standard userids, they will be recycled. Once a person no longer requires system access, their userid will be deactivated (see *Section 3.1.4.2, Deactivating Userids*). Later, when a userid meeting the same standard format is required by a user, the IAO can recycle one of the userids that have been deactivated. Re-profiling the userid to the proper profile (normally a Profile 9); verifying the account information for the userid; changing the password, and assigning it to the new user will accomplish this.

3.1.3.4 Rehosting Userids

If a workload migration or consolidation requires the rehosting of userids from one site platform to another, there are two important steps to take following the successful completion of the rehost. The first step is to ensure the IAO deactivates all userids that have been rehosted. Reference *Section 3.1.4.2,* Deactivating Userids, for more information. The second step is for the IAO to delete any accounts that are no longer needed because of the rehost effort. Deleting the account will remove all userids that were under that account. If there are a handful of userids that still need to have access to the account following the rehost, purge the account, and reenter those few userids that need to have access to the account. This will ensure rehosted userids do not accidentally gain access to their old host platform.

NOTE: Rehosting userids is a process used by sites supported by SSO Montgomery.

3.1.3.5 Use of the Master and SIMAN Administrator Userids

The Master userid will only be used by a single IAO. A copy of the Master userid will be secured in a safe place. No other individual will have access to the Master userid. The other IAOs will be given administrator userids for use in performing daily userid administrative functions such as password resets and profile updates.

In no case will any personnel other than appointed IAOs have access to SIMAN administrator userids. The Master userid and SIMAN administrator userids will not have access to batch mode. Only the Master userid and SIMAN administrator userids will be allowed to update the SIMAN environment.

SIMAN subadministrator userids will only be issued to personnel performing IAO duties at a site or remote sites.

- *(S101.020.00: CAT I) The IAO will ensure the Master userid is only be used by a single IAO.*
- *(S104.020.00: CAT I) The IAO will ensure the Master userid and IAO userids do not have access to batch mode.*
- *(S104.490.00: CAT I) The IAO will ensure only the Master userid and IAO userids are allowed to update the SIMAN environment.*

3.1.3.6 Securing the Master Userid

The password for the Master userid will be stored in a sealed envelope in a safe or a secure location where only the security office has access, in cases of emergency. When an emergency requires backup personnel to use the Master userid, the password is signed out of the safe and used to perform the necessary function. When the IAO is again available, the password will be reset and stored in the safe for future use. The IAO will maintain a log to record emergency access situations involving the Master userid.

3.1.3.7 Securing the Subadministrator Userid

In no case will any personnel other than appointed IAOs or SAs have access to SIMAN subadministrator userids. The password for the subadministrator userid will be stored in a secure location where only the security office has access, in cases of emergency. This secure location can be a locked drawer, locked file cabinet, or safe. When an emergency requires backup personnel to use the subadministrator userid, the password is signed out of the secure location and used to perform the necessary function. When the IAO/SA with subadministrator privileges is again available, the password will be reset and stored in the secure location for future use. The IAO/SA with subadminister privileges will maintain a log to record emergency access situations involving the subadministrator userid. An alternate solution for emergencies would be to simply call the IAO/SA with administrator privileges and request a reset of the subadministrator's password for use by the alternate IAO/SA. When the original IAO/SA returns, again notify the IAO with administrator privileges to reset the subadministrator's password for exclusive use by the original IAO. If there are multiple IAOs/SAs who need access to the subadministrator userid (e.g., a site running a day and a swing shift), then the primary IAO/SA will change the password, give the subadministrator userid to the alternate IAO/SA, and annotate the date and time of transfer in the security log. The alternate IAO/SA will immediately change the password once in possession of the subadministrator userid. After the shift is over, the alternate IAO/SA will repeat the procedure and transfer the subadministrator userid back to the primary. Accountability to a single individual is the key requirement in this process and the security log will reflect all transfers of this userid. Since the password may be changed frequently, the subadministrator userid used in this manner is allowed to have a minimum password expiration of zero days.

- *(S102.020.00: CAT III) All IAOs/SAs involved in the transfer will maintain a security log to record emergency and other transfers of the subadministrator userid from the primary IAO/SA to an alternate IAO/SA.*

3.1.3.8 System Userids

Some userids do not belong to any particular user. These userids are needed by the operating system, system support software, or by particular COTS products in order for the system to operate properly. These userids may be installed by the EXEC, product installation runs, or other means. Since these userids belong to the system, they will be considered "application userids and will be documented on a SAAR as required in 3.1.3 User Information Requirements. This additional documentation will be required of all new system userids or any system userids that have changes in functional use, or changes in privileges and interfaces allowed. Since these

userids will be considered owned by the IAO, they may all be documented with a single SAAR. Additionally, individual service-specific applications may require one of these userids because the AIS has hard-coded a userid into their software. The following should be noted:

a. The Exec or system userids are owned by the Security Officer, are well documented (see *Section 3.1.5, System Userids*), and cause immediate problems when deleted. If any of these userids are deleted, the best recovery option is to reload the security files from a time before the userids were deleted.

b. Application developers will work to remove hard-coded userids from application software because this violates the positive user identification aspect of an MAC II sensitive security system. The IAO will have a list of all hard-coded userids required for the applications on their system. Known hard-coded application userids are listed in the service-specific appendices. If one of these userids is deleted, the problem may not surface for some time. By the time it is discovered, the site may no longer have any security tapes that have this userid. Even if the site has these tapes, they will be required to reload the tapes and then redo all security changes made in SIMAN since that time.

c. FTP automated program-to-program userids need a SAAR since they are application userids. The IAO will document these userids, the specific application and organization that is using them, and a point of contact for these userids. The extended expiration password setting will not exceed 365 days and the password will be changed at a minimum of every 365 days. If subadministrators own these FTP userids, then they will also need a maximum password setting of 365 days.

d. Application Userids. These userids are used by applications to communicate between different systems. An example would be a userid used by an application running on a web server on a separate system to access the databases on the Unisys system. These userids will be documented on a SAAR. These passwords will be unique to each application pair. If they use passwords as authenticators they the password will be changed at a minimum every 365 days.

   An application pair will be considered the unique application running on a unique system and the application running on the Unisys system. An example would be a web browser on system A connecting to an application running on Unisys system C would use a different application userid than a web browser running on system B connecting to the same application running on the Unisys system C.

- *(A102.020.00: CAT III) The IAO will ensure all system userids are documented as application userids.*

3.1.3.9 Standard Userids

For DISA sites, Unisys systems will have standard userids (among the few exceptions is the site IAO's userid, which is not standardized in order to make it more difficult to guess). Reference the appropriate appendix in this manual for service-specific userid standards. At a minimum, the site needs to be able to identify at a glance the location of a userid and whether it belongs to a

site person or a functional user. Each site will use their assigned site code in the first two – three positions (as appropriate) of all site userids. The site codes are provided in the service specific appendices.

The CAMS system will not be required to enforce the userid naming requirements found in this system.

- *(S104.200.00: CAT III) For DISA sites, the IAO will enforce the userid standard established in the appropriate service specific appendix except for userids on the CAMS system.*

- *(S104.200.00: CAT III) For DISA sites, the IAO will ensure site userids have the site code assigned to that particular site as identified in the service specific appendix except for userids on the CAMS system.*

3.1.3.9.1 Reasons to Standardize

A userid-naming standard was established for the following reasons:

a. Contingency Processing and site Workload Balancing. A userid standard eliminates duplication of userid names across all DISA Unisys platforms. This allows workloads to be moved from one system to another or from one site to another without having to worry about userid duplication.

b. Identification. A userid standard allows the Security Officer (or anyone else, for that matter) at the site to identify at least the user's location at a glance.

c. Convenience. A userid standard eliminates some of the inconveniences associated with having userids that are more than six characters long (consider the truncated run-IDs shown at the console). A maximum userid length of six characters is recommended.

d. Administration. A base with hundreds of userids can spend a lot of time in userid management alone. Standard userids make it easier for the security officer to manage them properly.

e. Stacked Base Workloads. A userid standard that is strictly followed, whether or not it is the same as another service, will simplify the eventual migration to a unified standard. Workload migrations may take place to allow AIS workload consolidations (such as the formation of the consolidated accounting and finance Field Organizations), to balance the workload on various platforms across the sites, for contingency processing, or to accomplish other mission requirements. Non-unique system userids (such as DPS) will not conflict because they are already used on all platforms across the fleet. It is highly undesirable for duplication among the userids that are used by the functional users. Standard userids will ensure uniqueness across the DOD Unisys environment.

3.1.3.9.2 Guidelines for Assigning Standard Userids

Sometimes it is unclear what the standard userid name will be for a particular user, especially if that user performs functions for more than one AIS. The following guidelines may help in making these decisions:

a. Use the ALN or service-specific site code that is appropriate for where the user is physically located. For example, if a person in the Systems Support Office Montgomery requires a permanent userid on one of the ALN systems at DECC Ogden, use the base code GA (the site code for SSO Montgomery). If that same SSO person needs a userid on one of the DNMC systems at SMC Oklahoma City, the same base code of GA would be appropriate. Thus, an individual would have a single Unisys userid for use throughout the DISA. Field Organization personnel accessing a Field Organization system will use the Field Organization site code. Field Organization personnel accessing an Air Force base-level system will use the Field Organization site code and the base-level AIS code. For example, if a Dayton Field Organization BQ user signs on to Robins AFB's Supply, the userid will be DTGVxx. Air Force base-level personnel accessing a Field Organization system will use as their site code the Air Force site where they are physically located. For example, if a Robins AFB user signs into BQ at the Dayton Field Organization, this user will have a userid named ROBQxx.

b. Use the same userid for all DOD Unisys systems accessed by the user. If an individual has the requirement to have a userid on multiple systems (most if not all site technical personnel fall into this category), use the same userid name on all the systems he or she has access, This guideline will also be used if site or CDA personnel require access to multiple sites. Within DOD, an individual needs to have the same Unisys userid DOD-wide.

c. Minimum requirements for userid naming conventions are as follows:

    1. Will be able to distinguish site users from application users, including same base users. Each site will use their assigned site code in the first two or three positions (as appropriate) of all site userids. The site codes are provided in the service specific appendices.

    2. Be consistent in using the applicable standards that have been established for the sites particular service.

3.1.3.10 Guidelines for Protecting Userids

Most userid names need no protection beyond that given to any sensitive unclassified information contained on the system, but site personnel (who tend to have higher privilege userids) will not actively disseminate their userid names outside the site.

3.1.3.11 Userid Parameters

It has been determined that certain userid parameters will be regulated in order to maintain a level of security compliant with MAC II sensitive level security and to maintain a standard security environment across all DOD Unisys platforms. These requirements follow.

3.1.3.11.1 General Parameters

The following userid parameters will be set on all userids assigned to individual users (these do not necessarily apply to system userids):

a. All userids will have a security record (ACCESS screen).

b. All userids will have the disable userid feature implemented with 35 days in the Maximum Days of Inactivity field, three in the Maximum Invalid Passwords field, and zero in the Maximum Times Password-Expired Notice May Be Ignored field (ACCESS screen). One exception to this rule is that the Master and SIMAN Administrator userids will have a value of zero in the Maximum Days Of Inactivity field, a value of zero in the Maximum Invalid Password field, and a value of zero in the Maximum Times Password-Expired Notice May Be Ignored field. If the Master or SIMAN Administrator userids are ever disabled, these userids cannot be easily recovered. In addition, CAMS and SBSS userids are authorized to have 65 days in the Maximum Days of Inactivity field.

c. On the SECURITY screen, place an asterisk in the fields for userid record access being Private and User to create only unowned files.

d. For all functional userids, on the SUBSYSTM screen, blank all of the fields except the one labeled Can only read Executive GRS. This applies to subadministrator userids as well.

- *(S104.614.00: CAT II) The SA will ensure all userids have a security record.*
- *(S104.620.00: CAT II) The SA will ensure no userid, except documented exceptions, has "maximum days of inactivity" set to a value greater than thirty–five.*
- *(S104.630.00: CAT II) The SA will ensure no userid, except documented exceptions, has the SIMAN Disable Userid feature disabled by having "maximum days of inactivity" set to zero.*
- *(S104.640.00: CAT II) The SA will ensure no userid, except documented exceptions, has " invalid password attempts" set greater than three.*
- *(S104.650.00: CAT II) The SA will ensure no userid, except documented exceptions, has the SIMAN Disable Userid feature disabled by having "invalid password attempts" set to zero.*
- *(N/A: CAT II) The SA will ensure all userid, except documented exceptions, have " password notices may be ignored" set to zero.*

- *(S104.616.00: CAT II) The SA will ensure all userids have a record access of Private set.*

- *(N/A: CAT II) For DISA sites, the SA will ensure all userids has "User to Create Only Unowned Files" set.*

- *(N/A: CAT II) The SA will ensure all userids, except documented exceptions do not have "User to Create Only Unowned Files" set.*

- *(S104.618.00: CAT II) The SA will ensure all functional userids have "Can only read Executive GRS" set in the SUBSYSTM screen.*

3.1.3.11.2 Project-ID Requirements

Refer to the appropriate service-specific appendix for more information concerning project-ID requirements. This is especially important for the sites using the ALN operating system since it allows a user to obtain exempt ALN status.

For ALN:

- *(S104.340.00: CAT II) The SA will ensure non-exempt users, except where documented, are not allowed to enter their project-ID at sign-on time.*

NOTE: Users with a valid need are a documented exception.

- *(S104.330.00: CAT II) The SA will ensure non-exempt users, except where documented, are restricted to a specific list of project-Ids*

- *(S103.310.00: CAT II) The SA will ensure non-exempt users does not have an exempt project-ID in their userid record.*

3.1.3.11.3 Account Requirements

The majority of functional users will not be able to enter an account at sign-on time, and will be restricted to a list of accounts. This reduces the risk that they could gain access to an account that they are not registered to use. This is especially important in a fee-for-service environment. In rare cases where application users require access to more than five accounts, it is acceptable to set the Account May Be User Entered flag. This requirement will be justified, documented, and approved by the site IAO.

- *(S104.350.00: CAT III) The SA will ensure functional users who require access to less than five accounts do not have the ability to enter an account at sign on time.*

For ALN:

- *(S104.320.00: CAT II) Non-exempt users, except where documented, does not have an exempt account in their userid record.*

3.1.3.11.4 Terminal Time Out Requirements

The terminal time out requirements are as follows:

a. The systems are set to terminate or lock out a user session after 15 minutes of inactivity. If the session is locked out rather than terminated, a mechanism will be implemented that requires user identification and authentication before the connection is unlocked. The lockout mechanism will not be under the sole direct control of the end user.

b. A system's default time for lock out or session termination may be lengthened at the discretion of the IAM to 30 minutes. The IAM will maintain documentation for each system with a time out adjusted beyond the 15 minute limit and provide justification to explain the basis for this decision.

c. The IAO may set selected userids to have a time out of up to 60 minutes in order to complete critical reports or transactions without timing out. Each exception will meet the following criteria:

   1. The time out exception cannot exceed 60 minutes.

   2. The IAM will document the requirement and mitigating controls.

   3. The requirement will be revalidated whenever a new IAM is assigned or new domains are installed for those requiring access to the new domains.

d. In many situations, a hierarchy of lockout and time out parameters may be appropriate. For example, a site may choose to set a 15 minute standard for terminal lockouts implemented through the system controls or terminal screen protections, supplemented with a 60 minute time out.

- *(S104.380.00: CAT II) The IAM will document an extended system-wide default terminal time out.*

- *(S104.380.00: CAT II) The SA will ensure userids, except where documented, have their terminal time out set in to fifteen minutes.*

- *(S104.390.00: CAT II) The SA will ensure userids, except where documented, do not have the ability to disable their terminal time out.*

3.1.3.11.4.1 Application Specific Time Out Requirements – Internal Controls

The following application time out requirements fall under the guidelines outlined in *Section 3.1.3.11.4, Terminal Time Out Requirements*:

a. The Core Automated Maintenance System (CAMS), System Code FS, is an event-oriented system and transactions entered into the database are a result of some activity in the aircraft maintenance environment. CAMS terminals need to be available to the CAMS users as long as aircraft maintenance is being performed in order to receive maintenance work orders. Once a CAMS transaction (TIP) user has logged on to the system, the CAMS application software verifies that the userid is configured in the CAMS internal security matrix. All CAMS PID numbers are subject to the internal CAMS time out feature. If a CAMS terminal is not used for more than the specified amount of time (usually 15 minutes), the CAMS application locks the terminal and does not accept further input. The terminal connection to the host remains open so that work orders and other output from the system can still be routed to that terminal. Before further input can be made from the terminal, the user will completely sign off the system and back on. A CAMS user may also place the terminal in a "receive only" mode by entering an IDLE command to the CAMS application. Once a terminal is placed in IDLE mode, it will only be allowed to receive, print, or delete maintenance notifications queued to that terminal. If any other transactions are input from the terminal while in IDLE mode, CAMS will close the terminal.

   All CAMS TIP Profile 9 userids are granted a 780 minute (13 hour) time out as long as the CAMS internal application time out is set to 15 minutes (or 30 minutes if that is the approved system time out).

NOTE: These userids will be TIP only; they will not have access to demand mode. If individual userids (via PID numbers) need their internal application time out set to longer than 15 minutes (or 30 minutes if that is the approved system time out), they need a letter documenting the userids, PID numbers, and the mitigating controls in place. Requests for an internal time out of greater than 60 minutes will not be approved. A routine has been provided to the site IAOs to periodically check the CAMS internal application time out for compliance. The IAO will run this audit routine at least quarterly on all CAMS databases if this 780 minute (13-hour) time out is implemented.

b. The Standard Base Supply System (SBSS), System Code GV, has an application feature that supports the existence of TIP output only userids. These userids are configured in the SBSS database and can only receive output. They cannot be used to input transactions to the SBSS database or used to initiate interactive sessions.

   All SBSS TIP "Output only" Profile 9 userids are granted a 540 minute (9 hour) time out. These Profile 9 TIP userids are granted a 540 minute (9 hour) terminal time out. A routine has been provided to the site IAO so these userids can be audited. Any violations of this policy will result in only the userid involved to be restricted with a 15 minute time out (or 30 minutes if that is the approved system time out).

3.1.3.11.4.2 Application Specific Time Out Requirements – External Controls

These application specific time out requirements have an approved extension on file; however, each site AIS manager will document all userids with the extended time out, and the external mitigating controls that have been implemented by the end users, or, the acceptance of risk by the site AIS manager.

a. The Mission Capable (MICAP) Automated Sourcing System (MASS), System code GW, TIP userids. According to the AIS manager for MASS, enforced time-outs on these TIP userids degrade the sourcing process to unacceptable standards because of the unsolicited output being directed to the MASS terminals for sourcing status. To make the MASS time out policy easier to enforce and track, the MICAP userids that need an extended time out will have GW in positions 3 – 4 of their userid and will only have GW project-ID(s) and account(s) identified in their userid record.

   The MASS (GW) TIP Profile 9 userids are granted a 540 minute (9 hour) terminal time out with a letter from the site MASS AIS manager (usually the Chief of Supply) stating that they accept all data integrity and processing risks associated with the extended time out, and a list of all userids to be extended. This list will not be very large (maybe 200) depending on the size of the site. To make the MASS time out policy easier to enforce and track, the MICAP userids that need an extended time out will have GW in positions 3 – 4 of their userid and will only have GW project-ID(s) and account(s) identified in their userid record.

b. The SBSS Remote Processing Station (RPS) Function 057 Terminal. This terminal serves as the prime PID of the SBSS application and controls the SBSS application, up/down flags, SBSS crossovers, and is used by console operators to monitor the system. If this terminal is signed off for any reason, the SBSS application is inaccessible by any SBSS user. For this reason, the Demand userid used to sign on to the SBSS RPS 057 terminal is authorized to be signed on 7 days a week, 24 hours a day with appropriate documentation for the userid, the RPS 057 terminal-ID, and the policies and procedures as stated in the following paragraph. Shift supervisors will be responsible for all actions performed with this userid, and will take over this responsibility during shift changes by logging it on the RPS Shift Changeover Log. This userid will be a Profile 5 with Demand/Batch/TIP, TERMRUN$, and EZLOAD capabilities. This userid will NOT have access to QLP with Update, IQU, or DBE processors. At consolidated supply squadrons only, this userid is also allowed access to the Automated Reset Process (ARP) Program, Section 8.2.1Automated Reset Process Program. Terminal-IDs ending in 57 will normally be the terminal-ID that will be signed on with this userid 7 days a week, 24 hours a day.

   The Demand userid used to sign on to the SBSS RPS 057 terminal can be signed on 7 days a week, 24 hours a day. The SBSS RPS 057 terminal will be in a controlled area and the individual responsible for all actions performed by this userid will be documented in the RPS Shift Changeover Log. This userid will be a Profile 5 with Demand/Batch/TIP, TERMRUN$, and EZLOAD capabilities. This userid will NOT have access to QLP with Update, IQU, or DBE processors. At consolidated supply

squadrons only, this userid is also allowed access to the Automated Reset Process (ARP) Program, Section 8.2.1Automated Reset Process Program.

c. Other SBSS RPS Demand userids may have an extended time out because the time out of these userids could adversely impact weapon system support. This time out will be sufficient to cover a single shift of operations.

   Other SBSS RPS Demand userids are granted a 540 minute (9 hour) terminal time out if documented with, a list of the userids to be extended, and the mitigating controls that will be in place.

d. Supply Asset Tracking System (SATS) Userids. SATS communicates with the SBSS by using two InfoConnect paths. The SBSS recognizes these paths as terminals with function numbers 01803 and 01804. SATS sends Transaction Identification Codes (TRICs) REC/TIN/FCS/1SI transactions to the SBSS using function number 01803. The SBSS inline programs use flag 001-SATS-FLAG and if equal to Y sends ISU/MSI/TIN/SHP/A5J/DOR output documents to function 01804 instead of applicable warehouse terminals. The unique mission and functionality of SATS makes a 15 or 30 minute time out period impractical and can potentially disrupt supply operations. SATS terminals should be configured as type equipment 21 (non-bar-coded). The SATS userids that are used to sign on to these terminals will be TIP/Batch only and may be granted a terminal time out of 480 minutes (8 hours). The increased risks that an 8-hour terminal time out can potentially bring will require all field units using SATS to accomplish the following:

   The SATS userids will be TIP/Batch only userids and will be assigned standard userid names for both input and output functions for the sole purpose of maintaining the SATS/SBSS interface. The userids will be configured as follows:

   Positions 1-2 (base name) e.g., GU Gunter
   Positions 3-4 (system code GV)
   Positions 5-6 = SI for SATS input, and SO for SATS output

   The SATS userids are granted a terminal time out of 480 minutes (8 hours).

   Base Supply managers will be responsible for reviewing and changing SATS passwords every 90 days and will also function as the system administrators for the SATS server as well as the SATS/SBSS interface workstation. They will ensure SATS/SBSS interface workstations are located in designated controlled areas that only authorized personnel may access. They will maintain a SATS history log within the SATS server for a minimum of one year to comply with DOD audit requirements. Finally, they will ensure password protected screensavers are installed on all SATS/SBSS interface workstations.

e. The CAMS Host Database Manager's (DBM's) Demand userids may have an extended time out because the time out of these userids could adversely impact weapon system support. This time out will be sufficient to cover a single shift of operations.

   The CAMS Host DBM Demand userids are granted a 780 minute (13-hour) terminal time out if documented with, a list of the userids to be extended, and the mitigating controls that will be in place.

f. The Command Budget Automated System (CBAS) TIP Profile 9 userid may have an extended time out because the time out of these userids in MAPPER can cause critical delays in the generation and submission of financial reports.

   The CBAS TIP Profile 9 userids are granted a 240 minute (4-hour) terminal time out.

3.1.4 Assigning Userids

Because of the regionalization concept, the IAO may perform the userid assignment himself or delegate this function to IAOs at remote sites. In the latter situation, the IAOs at individual sites will install userids as required for their site, and forward pertinent security information to the IAO at the site. The IAO then adds the user to the appropriate account(s). Because only the IAOs at the site can update accounts, there is no threat of IAOs at the remote site adding userids to accounts without the knowledge of the IAO.

a. Before the IAO assigns a permanent userid (as opposed to a temporary userid as in *Section Temporary Access Userids*), to a new user, the IAO will obtain a properly filled out SAAR (or its equivalent) and add this data to their list of active users for their system. Determine which of the security profiles in *Section 3.1.8.2, Standard Security Profiles*, is appropriate for the new user. It is DOD policy that each user fills out a SAAR or equivalent form, and that the IAO retains this form for as long as the userid is assigned to that user. For userids assigned by the site IAO, the site IAO will retain these records. For userids assigned by IAOs at a remote site, the IAO at the remote site or TASO (if delegated by the IAO at the remote site) will retain these records. Local or service-level policy may also dictate that the end user, the end user's supervisor, the end user's TASO, or the Base Security Officer will be required to retain a copy of this form as well. The main point for IAOs is that the IAO will be able to identify (either directly or through an IAO on a remote site or TASO) the identity of any userid that is active on any system he or she has the responsibility to maintain.

b. The IAO will maintain a list of active userids for each system (arranged alphabetically by AIS code) so that userids can be tracked as well as recycled more easily. Further, it is highly recommended that this data be kept in some type of database or file at the IAO's PC.

c. If there are no unassigned userids for the appropriate application, install a new one. If there is an existing unassigned userid for the application, tailor the settings in that userid

for the new user, give it an initial password (using documented password construction rules), re-enable the userid, and then assign it to the new user. These steps are explained below.

d. All userid authorizations will be revalidated on a yearly basis. The date of the last revalidation should be added to the original userid request form.

NOTE: If the list of current users of a system is maintained on-line, the revalidation dates may be entered into the on-line record instead of (or in addition to) the userid request form.

3.1.4.1 Installing New Userids

Once the pool of userids available for recycling for a given site and application is exhausted, a new userid will have to be installed. The installation or creation of a new userid is outlined in the sections below.

3.1.4.1.1 Installing a New Userid Record in SIMAN

These procedures are tailored for use as a step-by-step instruction for the Security Officers. These steps may be modified to suit individual site requirements.

The first step is to create the userid record in accordance with the correct service standards. This step can be accomplished by using the Master userid, by an IAO or SA with SIMAN administrator privileges, or by an SA with SIMAN subadministrator privileges. Be aware of ownership issues when deciding who will install the userid. The individual who will be performing the majority of maintenance on the userid will perform the installation. These steps assume the use of SIMAN in full-screen mode. Note that all of these steps can be performed in SIMAN batch mode as well.

a. Decide on a userid name using the appropriate service specific naming convention, as outlined in the appendices of this document.

b. To install the userid in SIMAN, enter @SIMAN 1,2. This will bring the user to the userid installation screen. Enter the userid to be installed. The user may enter more than one and they will all be alike. Do not install TIP-only users and Demand users at the same time. Although not required, the user may be able to save time and effort by finding an existing userid from the same site and AIS as the userid the site wants to install and typing that userid name in the SETUP user information LIKE user [_____] field at the bottom of the screen. Transmit.

NOTE: Do not use an IAO userid as the LIKE userid unless the site requires the creation of an administrator or a subadministrator userid.

c. On the next screen, assuming theuserid is enabled the INFO screen in SIMAN, user information can be entered here. Enter the user's name, work phone, and any other applicable information. There is not a requirement to use this screen, but every Security Officer will maintain a current list of the active users of the Security Officer's system,

including all the information specified on this screen if the Security Officer does not keep a copy of the SAAR. Transmit.

d. On the ACCESS screen, make sure the userid has a security record. Most of the userids created will only need Batch and TIP access, and the Security Officerwill minimize the number of userids that can establish a Demand session on the system. Transmit.

e. On this screen, the initial password will need to be changed otherwise, it will automatically be set to A. Do not use the same initial password for all users or any single group of users. Be sure to follow documented password construction rules even for the initial password.

f. On the SECURITY screen, put an asterisk in the field labeled User to Create Only Unowned Files. There are some problems associated with file ownership when reloading owned files during a 4-13 boot. Do not give the user any ACRs, since the Security Officer will own all ACRs on the system. Transmit.

g. On the SUBSYSTEM screen, give the user Can Only Read Executive GRS only. This applies to subadministrators as well. Transmit.

h. On the first SESSION screen, give the user time out values according to the guidelines in *Section 3.1.3.11.4, Terminal Time Out Requirements*. Remove the ability for the user to disable terminal time out checking. The run image will always be system generated. Only authorized select site Profile 2 userids will have the ability to enter their own run image. Only DNMC userids are authorized to have an alternate run-ID and they will comply with the guidelines specified in *Appendix D.3, System and Application Software – DNMC*. If unauthorized users enter their own run image or have an alternate run-ID, they could spoof other run-IDs or give themselves higher system scheduling priority.

i. On the second SESSION screen, fill the first two fields with nines (“9”). These are maximum time and maximum pages. Give the user the appropriate project-ID(s) and accounts for their application. Ensure the project-ID restricted field is enforced if the site is running the ALN operating system. Do not place an @SIMAN in the Control Image field of any userid (even subadministrator userids). If a userid is compromised, an @SIMAN in the control image may allow someone unauthorized access or knowledge of this processor, especially if the userid involved is a subadministrator userid.

j. At this point, continue paging through the userid record configuring each field, but save time and effort by using the security profile runstreams instead. Press the HOME key and enter COMMIT,X to install the userid and exit SIMAN. Use the information in *Section 3.1.8.2,* Standard Security Profiles, to determine what profile the new user falls under. Remember that it is very important to give a user the least amount of power required (the lower the profile number is, the more power the user has) for the user to do his or her job. From the Demand prompt, type the following command to start a job that will customize the userid just created:

@ADD JX$$0000*00.PROFILE-x
Where x is the security profile for the new user (2 through 9 inclusive)

This job will prompt for a userid, and then kick off a SIMAN Batch run to update that userid to the security profile requested. Be sure that END SIMAN 4R3 0 ERRORS appears after the job runs. This message confirms that the changes to the userid were made successfully. Of course, there is no runstream to make a userid a Profile 1, because very few Profile 1 userids will be required. The profile runstreams will update the CONS level, console keyin groups, console message groups, Interfaces, and Privileges for a particular userid. If a user falls between profiles, run the lesser profile runstream against the userid first, then manually add the higher level CONS level and Keyins, Interfaces and Privileges.

k. If the userid has a need for a CONS mode different from the normal in his or her security profile, manually update the level of CONS through SIMAN. Remember that CONS privileges are very powerful and will be restricted to only those individuals that need to have them in order to do their job. The FULL, DISPLAY, and RESPONSE levels of CONS are the most dangerous, and ACTIVATED RESPONSE level CONS will never be assigned to a userid unless it is logged by the IAO in the security event log. RESPONSE CONS is limited to Profile 1 and 2 userids.

- *(S104.670.00: CAT II) For DISA sites, the SA will ensure only authorized select site Profile 2 userids have the ability to enter their own run image.*

- *(S104.680.00,: CAT II) For DISA sites, the SA will ensure only authorized userids have an alternate run-ID.*

- *(S104.690.00: CAT II) For DISA sites, the SA will ensure for DNMC userids authorized to have an alternate run-ID the alternate runid is the last four or five characters of the userid.*

- *(S104.700.00: CAT II) For DISA sites, the SA will ensure for DNMC userids authorized to have an alternate run-ID the alternate runid is unique within the system.*

- *(S104.120.00: CAT I) The SA will ensure userids do not have activated response CONS mode.*

- *(S104.124.00: CAT I) The SA will ensure RESPONSE CONS are limited to Profile 1 and 2 userids.*

3.1.4.1.2 Entering a New Userid Under an Account in SIMAN

The second step in this process is to add that userid name to the account(s) listed in the userid record, and this step can only be accomplished by the Master userid/Account, which is owned by the site IAO.

NOTE: There is an Exec local-code change available to allow all SIMAN administrators under the Master Account to perform account maintenance. Contact the SSO Montgomery for more information.

a. Sign on to the system with the Security Officer userid and the Master Account (the one with which updates other accounts). Enter SIMAN Batch mode to insert the userid under the account. SIMAN Batch mode is much faster than the screens when updating accounts.

```
@SIMAN,B
UPDATE ACCOUNT = aaaaaaaa ADD USER = uuuuuu ;
                              or
UPDATE ACCOUNT = aaaaaaaa ADD USER = uuuuuu,vvvvvv,wwwwww ;
@EOF
```

Where aaaaaa is the desired account and uuuuuu, vvvvvv, and wwwwww are userids to be added to that particular account.

WARNING! Keep track of how many userids are under a particular account, and never put more than 900 userids under an account. This problem and workaround are documented in Unisys Problem List Entry (PLE) 17869779.

b. The userid is now fully functional. If this user works in an application that has its' own internal security mechanisms, this userid will have to be added to that AIS security database before it will be operational for that application.

3.1.4.2 Deactivating Userids

If a user no longer requires access to the system, the IAO will be notified so that the userid that was assigned to the individual can be deactivated. The IAO will deactivate the userid by removing the TIP and Batch run modes, setting the Demand run mode with an @FIN in the control image, and re-profiling the userid to a Profile 9.

To deactivate a userid, the IAO will type the following from a demand mode session:

```
@ADD JX$$0000*00.PROFILE/DACT
```

This job will prompt for a userid, then kick off a SIMAN Batch run to update that userid to the security profile requested. Be sure that END SIMAN 4R3 0 ERRORS appears after the job runs. This message confirms that the changes to the userid were made successfully.

- *(S104.580.00: CAT II) The IAO will deactivate a userid when notified the user no longer requires access.*

3.1.4.3 Disabling/Enabling Userids

3.1.4.3.1 Disabling Userids

All IAOs will ensure the SIMAN Disable Userid Feature is correctly implemented. This is accomplished by ensuring the Maximum Days of Inactivity and Maximum Invalid Password Attempts fields are set to the required values. Reference *Section 3.1.4.6, Implementing the SIMAN Disable Userid Feature*, on details on how to properly implement the SIMAN Disable Feature. At times, the IAO may want to temporarily disable a userid. To disable a userid in SIMAN, the IAO can type the following from a demand mode session:

```
@SIMAN,B
UPD USE=XXXXXX     DIS_USE ; where XXXXXX is the userid
@EOF
```

3.1.4.3.2 Enabling Userids

If the SIMAN disable feature is correctly implemented, a userid may become disabled. Reasons for a userid to become disabled are as follows:

1. The user has not signed on within the period specified in the Maximum Days of Inactivity field.

2. The user has entered more invalid password attempts than allowed by the Maximum Invalid Password Attempts field.

3. The userid has been disabled by a SIMAN Administrator or subadministrator.

If the TASO, or IAO is notified by a user that his/her userid has become disabled, the TASO or IAO will verify the identify of the individual by validating the individual's SAAR before any attempt is made to enable the userid. This will prevent unauthorized individuals from gaining access to the system. After the individual's identity is verified, the TASO can execute the Automated Reset Process (ARP) Program, 8.2.1 Automated Reset Process Program, (if used) or an IAO can type the following from a demand mode session:

```
@SIMAN,B
UPD USE=XXXXXX     ENA_USE ;
@EOF
```

NOTE: SIMAN is a single thread processor and goes through a security record one field at a time. If a userid is disabled because of multiple reasons (for example, maximum days of inactivity and maximum invalid password attempts); this userid would have to be enabled twice.

- *(S104.650.00: CAT II) The IAO will ensure no userid, except documented exceptions, have the SIMAN Disable Userid feature disabled by having "invalid password attempts" set to zero.*

- *(S104.654.00: CAT II) The SA will ensure users identity is verified before their userids are enabled.*

3.1.4.4 Dormant and Never Signed On Userids

The IAO will periodically review the SRR Toolkit report and identify dormant userids that have been inactive on a system for over 35 days (65 days if CAMS or SBSS is processed). The IAO will determine why the userid was not properly disabled and correct the problem. The IAO will also periodically review the SRR Toolkit reports and identify userids that have never signed on to the system. Userids that have never signed on can be system userids (which can usually be disabled) or userids that are being improperly staged by an IAO or subadministrator. If userids appear to be staged, the IAO will contact the individual installing these userids and brief the individual on the proper assignment of new userids. If these userids cannot be immediately assigned, they will be deactivated.

- *(S104.580.00: CAT II) The IAO will identify userids are dormant and implement the appropriate corrective actions.*

- *(S104.570.00: CAT II) The IAO will identify userids are installed but never signed on to the system and implement appropriate corrective actions.*

3.1.4.5 Recycling Existing Userids

The recycling of an existing unassigned userid can be a one or two step process very similar to installing a new userid, and is outlined in the sections below.

3.1.4.5.1 Modifying an Existing Userid Record in SIMAN

The first step is to modify the existing userid record in SIMAN with the correct parameters for the AIS that will use the userid. This step can be accomplished by using the Master userid, by an IAO with SIMAN administrator privileges, or by an IAO that has SIMAN subadministrator privileges.

a. Select an available unassigned standard format userid for the particular application needed.

b. To update or modify the userid to fit the user it will be assigned to, enter @SIMAN 1,3 from a Demand session. This will bring the user to the userid modification screen. Enter the userid to be modified. Transmit.

c. On the next screen, one can enter user information. Enter the user's name, work phone, and any other applicable information. It is not required to use this screen, but every Security Officer will maintain a current list of the active users of the Security Officer's system, including the information specified on this screen if the Security Officer does not keep a copy of the SAAR. Transmit.

d. On the ACCESS screen, make sure the userid has a security record as well as access to required run modes (Demand, Batch, or TIP). Most userids for functional users will only need Batch and TIP access, and l minimize the number of userids that can establish a Demand session on the system. Transmit.

e. On this screen, the user will set the initial password for the userid. Do not take the system default password, which is always A. Do not use the same password for all users or any single group of users. Be sure to follow documented password construction rules even for the initial password.

f. On the SECURITY screen, put an asterisk in the field labeled User to Create Only Unowned Files. There are some problems associated with file ownership when reloading owned files during a 4-13 boot. Do not give the user any ACRs, since the Security Officer will own all ACRs on the system. Transmit.

g. On the SUBSYSTEM screen, give the user Can Only Read Executive GRS only. This applies to subadministrators as well. Transmit.

h. On the first SESSION screen, give the user time out values in accordance with the guidelines provided in *Section 3.1.3.11.4, Terminal Time Out Requirements*, in this document. The run image will be system generated. Only authorized site Profile 2 userids will have the ability to enter their own run image. Only DNMC userids are authorized to have an alternate run-ID and they will comply with the guidelines specified in *Appendix D.2 System and Application Software – DNMC.* If unauthorized users enter their own run image or have an alternate run-ID, they could spoof other run-IDs or give themselves higher system scheduling priority.

i. On the second SESSION screen, fill the first two fields (maximum time and maximum pages) with nines. Give the user the appropriate project-ID(s) and account(s). Ensure the "project-ID restricted" field is enforced if the site is running the ALN operating system. Do not place an @SIMAN in the Control Image field of any userid (including subadministrator userids). If a userid is compromised, an @SIMAN in the control image may allow someone unauthorized access or knowledge of this processor, especially if the userid involved is a subadministrator userid.

j. At this point, continue paging through the userid record configuring each field, but save time and effort by using the security profile runstreams instead. Press the HOME key and enter COMMIT,X to save the changes you have made to the userid record thus far and exit SIMAN. Use the information in *Section 3.1.8.2,* Standard Security Profiles, to determine what profile the new user falls under. Remember that it is very important to give a user the least amount of power required (the lower the profile number is, the more power the user has) for that user to do his or her job. Type the following command to start a job that will customize the userid selected:

    @ADD JX$$0000*00.PROFILE-x
    (Where x is the security profile for the new user (2 through 9 inclusive)

This job will prompt for a userid, then kick off a SIMAN Batch run to update that userid to the security profile requested. Be sure that "END SIMAN 4nRnn 0 ERRORS" appears after the job runs. This message confirms that the changes to the userid were made successfully. Of course, there is no runstream to make a userid a Profile 1, because very few Profile 1 userids will be required at a site. The profile runstreams will update the CONS level, console keyin groups, console message groups, Interfaces, and Privileges for a particular userid.

k. If the userid has a need for a CONS mode different from the norm in his or her security profile, manually update the level of CONS through SIMAN. Remember that CONS privileges are very powerful and will be restricted to only those individuals that need to have them in order to do their job. The FULL, DISPLAY, and RESPONSE levels of CONS are the most dangerous, and the ACTIVATED RESPONSE level of CONS will never be assigned to any userid unless it is logged by the IAO in the security event log. The RESPONSE level of CONS is restricted to Profile 1 and 2 users only.

- *(S104.670.00: CAT II) The SA will ensure only authorized site Profile 2 userids have the ability to enter their own run image.*
- *(S104.680.00,: CAT II) The SA will ensure only authorized userids have an alternate run-ID.*
- *(S104.690.00: CAT II) The SA will ensure for DNMC userids authorized to have an alternate run-ID the alternate runid is the last four or five characters of the userid.*
- *(S104.700.00: CAT II) The SA will ensure for DNMC userids authorized to have an alternate run-ID the alternate runid is unique within the system.*
- *(S104.660.00: CAT II) The SA will ensure userids do not have an @SIMAN in their control image.*
- *(S104.120.00: CAT I) The SA will ensure userids do not have ACTIVATED RESPONSE CONS mode.*
- *(S104.124.00: CAT I) The SA will ensure RESPONSE CONS is limited to Profile 1 and 2 userids.*

3.1.4.5.2 Entering a Recycled Userid Under an Account in SIMAN

The second step in this process is to add the userid from the previous step under the account(s) listed in the userid record. This step can only be accomplished by the Master userid/Account, which belongs to the site IAO or, if a local code change has been applied to SIMAN, a SIMAN administrator under the Master Account

a. Sign on to the system with the Security Officer userid and the Master Account (the one you update other accounts with). Enter SIMAN Batch mode to insert the userid under the account. SIMAN Batch mode is much faster than the screens when updating accounts.

```
@SIMAN,B
UPDATE ACCOUNT = aaaaaaaa ADD USER = uuuuuu ;
                              or
UPDATE ACCOUNT = aaaaaaaa ADD USER = uuuuuu,vvvvvv,wwwwww ;
@EOF
```

Where aaaaaa is the desired account and uuuuuu, vvvvvv, and wwwwww are userids to be added to that particular account.

WARNING! Keep track of how many userids are under a particular shred of an account, and never put more than 900 userids under an account. If this threshold is exceeded, problems are likely to occur with security files. This problem and workaround are documented in Unisys Problem List Entry (PLE) 17869779.

b. The userid is now functional. If this user works in an application that has its' own internal security mechanisms, this userid will have to be added to that AIS security database before it will be fully operational.

3.1.4.6 Implementing the SIMAN Disable Userid Feature

The IAO will properly implement the SIMAN Disable Userid feature. There are two SIMAN fields in every userid record associated with this feature. The first controls how many days of inactivity will pass before that particular userid is automatically disabled by the system. This field will be set to 35 days for all userids on the system except CAMS and SBSS userids, SIMAN Administrators, and the Master userid. All CAMS and SBSS userids are authorized to have this field set to 65 days. SIMAN Administrators and the Master userid are authorized to have this field set to zero days. The second data field controls how many consecutive invalid sign-on attempts a userid can have before the userid will be disabled by the system. This field will be set to three for all userids on the system except SIMAN Administrators, the Master userid, and selected system Demand RSI userids. SIMAN Administrators and the Master userid are authorized to have this field set to zero. Since only the SIMAN Administrators can modify the Master userid, if these userids became disabled the only way to recover them would be to reboot the system and reload the security files from a backup set. For more detailed information on this feature, refer to the SIMAN manual. Selected system Demand RSI userids (reference *Section 3.1.5.4,* Configured Demand Remote Site Interface Userids) are authorized to have this field set to zero. This prevents anyone from intentionally disabling these userids to disrupt computer processing.

NOTE: This feature in SIMAN does not remove the requirement for a procedure to be put in place to ensure the Security Officer is notified whenever a user no longer needs or is no longer authorized access to the system. This could be because the user is leaving, separating from the service, changed duties, or had a clearance revoked or some other reason. If a user no longer requires access to the system, the userid that was assigned to

the individual will be deactivated (reference *Section 3.1.4.2*, Deactivating Userids) until the userid is reassigned.

There are several security utilities outlined in the Unisys Security Integrated Toolkit (USIT) Software User Manual. Please reference that document for information on various tools available to assist the IAO in performing their duties.

- *(S104.630.00: CAT II) The SA will ensure no userid, except documented exceptions, and has the SIMAN Disable Userid feature disabled by having "maximum days of inactivity" set to zero.*

- *(S104.620.00: CAT II) The SA will ensure all userids, except documented exceptions, and has the maximum days of inactivity field set to 35 days.*

- *(S104.640.00: CAT II) The SA will ensure all userids, except documented exceptions, and has a setting of three in the maximum invalid password attempts field.*

- *(S104.650.00: CAT II) The SA will ensure no userid, except documented exceptions, and has the SIMAN Disable Userid feature disabled by having "invalid password attempts" set to zero.*

3.1.4.7 Deleting Userids

Userids will never be deleted, since once they are deleted they cannot be reinstalled to a userid of the same name. Due to the nature of the SACRD$ security file, once a userid is deleted, it is irrecoverable by any means short of an initialization of the SACRD$ file, or a reload of the system security files. The proper way to delete a userid involves taking Extended Security down, deleting the userid, and then bringing Extended Security back up. This procedure deletes the TSS$ record for the userid without deleting the SACRD$ record, but since there are multiple opportunities to make a mistake or forget a step, it is much safer simply to disable or deactivate the userid instead. This procedure will not work on system levels HMP IX 7.0 and above. Userids will not be deleted on these systems.

3.1.4.8 Changing Ownership

Userids will normally be owned by the Administrator or Subadministrator that installs them. If you change the userid of the Administrator or Subadministrator at a site or the userids are rehosted to a different site Subadministrator; the userids formerly owned will now need to be updated to reflect the new owner's userid. The procedures documented below will change ownership of a userid.

```
@SIMAN,B
UPD USE=XXXXXX    OWN=YYYYYY ;
@EOF
```

Where XXXXXX is the userid to be updated and YYYYYY is the Subadministrator's userid.

3.1.5 System Userids

Many sites have default userid/password combinations installed on their system that would be easy for an intruder to exploit and use to do damage to the system or its data. Some of the userids listed below are quite powerful and could therefore cause significant harm if compromised. The Security Officer will perform the steps listed below in order to prevent these most obvious and easily fixed security breaches.

3.1.5.1 Common System Userids

These userids will be found on most, if not all, Unisys domains. If a userid is not mandatory, this means that an equivalent userid may be installed to replace the original. If the userid is mandatory, some piece of software will not work unless it can use that exact userid.

USERID	*MANDATORY*		*PURPOSE*
	Y/N	*SERVICE*	
-ASIS-	Y	SYSTEM	Needed to own FLEX Fixed-Gate subsystem file. No run modes; can be disabled.
CATS	N	ALN	Userid for Computer Assisted Training.
-CHAMELEON-	Y	SYSTEM	Needed to own various Fixed-Gate subsystem file and other DATA$ files. No run modes; can be disabled.
-CIFS-ADMIN- (Batch Only)	Y	SYSTEM	Needed to own CIFS Fixed-Gate subsystem file. Batch mode only; can be disabled.
-CMS1100- or -CMS-SUBSYS-	Y	SYSTEM	Needed to own CMS Fixed-Gate subsystem file. No run modes; can be disabled.
-COMAPI-	Y	SYSTEM	Needed to own COMAPI Fixed-Gate subsystem file. No run modes; can be disabled.
COM-SYSTEM-H	N	SYSTEM	Needed for Session Control Exec. No run modes; can be disabled.
COM-SYSTEM-L	N	SYSTEM	Needed for Session Control Exec. No run modes; can be disabled.
-CPCOMMSS- or -CPCOMM-SS	Y	SYSTEM	Needed to own CPComm Fixed-Gate subsystem file. No run modes; can be disabled.
-CPFTP- or -FTP-SUBSYS-	Y	SYSTEM	Needed to own cpFTP Fixed-Gate subsystem file. No run modes; can be disabled.
DCFS	N	ALN	Needed for Pseudo Processing. Batch only.
-DDP-PPC-	Y	SYSTEM	Needed to own DDP Fixed-Gate subsystem file. Batch mode only; can be disabled.
DPS/DPSSYS	Y	SYSTEM	Required for privileged DPS software commands.
-DPS-	Y	SYSTEM	Needed to own DPS Fixed-Gate subsystem file. No run modes; can be disabled.
EXEC8 **	Y	SYSTEM	Needed to operate the system. No TSS$ record.
-EXPIPE-	Y	SYSTEM	Needed to own Expipe Fixed-Gate subsystem file. No run modes; can be disabled.
GAJT00	Y	SYSTEM	Used by SSO Montgomery personnel to transfer Release Tapes via the DDP TXFR process. Batch only, can be disabled.
GUJXFG	Y	SYSTEM	Needed to own Fixed-Gate subsystem file. No run modes; can be disabled.
-HTPIC-2200-	Y	SYSTEM	Needed to own OS 2200 High-Performance Transaction Processing Interconnect Fixed Gate subsystem file. No run modes, can be disabled

USERID	*MANDATORY*		*PURPOSE*
	Y/N	*SERVICE*	
-INFOACCESS-	Y	SYSTEM	Needed to own INFOAccess Fixed-Gate subsystem file. No run modes; can be disabled.
INSTALLATION **	Y	SYSTEM	Needed to boot the system. No TSS$ record.
IPF or DDP	Y	SYSTEM	Demand RSI userid. Needed to run DDP.
IQUMAS	N	ALN	Needed for IQU Processor.
MASTER	N	DNMC	Original DNMC Security Officer's userid
--MEDIAMGR--	Y	SYSTEM	Needed to own Media Manager Fixed-Gate file. No run modes, can be disabled.
-MQS2200- or -MQS-	Y	SYSTEM	Needed to own MQ Series Fixed-Gate subsystem file. Batch mode only; can be disabled.
-NTSI-	Y	SYSTEM	Needed to own NTSI Fixed Gate subsystem file. No run modes, can be disabled
-OPE-TP-	Y	SYSTEM	Needed to own OPE-TP Fixed-Gate subsystem file. No run modes; can be disabled.
-OSI-DIR-	Y	SYSTEM	Needed to own OSI-DIR Fixed-Gate subsystem file. No run modes; can be disabled.
-OSI-TP-	Y	ALN & DFAS-IN	Needed to own OSI-TP Fixed-Gate subsystem file. No run modes; can be disabled.
-OTM-	Y	SYSTEM	Needed to own OLTP-TM2200 Fixed-Gate subsystem file. No run modes; can be disabled.
QUIKST	Y	SYSTEM	Demand RSI userid. Needed for NJZMON Processor.
SECOFF	N	ALN & DFAS-IN	ALN & DFAS-IN Security Officer's userid.
SECURITY	N	SYSTEM	Allows initial access to NMS (TELCON).
-SQL-NET-	Y	SYSTEM	Needed to own SQL Fixed-Gate subsystem file. No run modes; can be disabled.
SSC-SSQM	Y	SYSTEM	Used by HQ SSG/SW personnel to transfer Release Tapes via the DDP TXFR process. Batch only, can be disabled.
STAR	N	ALN	Needed for STAR label printer.
-SX2200-	N	SYSTEM	Obsolete. Used to own SX2200 Fixed-Gate subsystem file. No run modes; can be disabled.
TIPOUTPUT	N	SYSTEM	Needed for Session Control Exec. No run modes; can be disabled.
-TTW-	Y	SYSTEM	Needed to own TTW Fixed-Gate subsystem file. No run modes; can be disabled.

USERID	*MANDATORY*		*PURPOSE*
	Y/N	*SERVICE*	
-UDS01-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS02-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS03-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS04-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS05-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS06-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS07-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS08-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS09-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS10-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS11-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS12-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS13-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS14-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.

USERID	*MANDATORY*		*PURPOSE*
	Y/N	*SERVICE*	
-UDS15-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UDS16-	Y	SYSTEM	Needed to own UDS Control Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
-UNIACCESS-	Y	SYSTEM	Needed to own UniAccess ODBC Fixed-Gate subsystem file. Batch on active applications only; can be disabled.
UOSS	Y	SYSTEM	Needed for Unattended Operations, can be disabled.
VTHSRV	Y	SYSTEM	Demand RSI userid. Used by Virtual Tape Software.
xxEZ00	Y	SYSTEM	Demand RSI userid. Used to start jobs by EZLOAD (xx is the local ALN site code, such as GU for SMC Montgomery).
xxJF00	Y	SYSTEM	Demand RSI userid. Used to start jobs by Scheduler (xx is the local ALN site code, such as GU for Montgomery).
xxJSTM	Y	SYSTEM	Needed for Shared Library System (xx is the local ALN site code).
** ***NOTE:*** *Prior to HMP IX 7.0, the EXEC and INSTALLATION userids need to have a SACRD$ record but will never have a TSS$ record during normal operation of the machine. These userids are very powerful and can bypass most of the security mechanisms offered by the Exec.* *In HMP IX 7.0 and above, there is no longer separate TSS$ and SACRD$ files, all userid security information is kept in the SEC@USERID$ file. Therefore, the EXEC and INSTALLATION userids will appear in all security record maintenance utilities but cannot be modified or deleted.*			

Table 2-3. Common System Userids

3.1.5.2 Obsolete Userids

These userids will no longer be on the system. They will be disabled. If they are still being used, create equally powerful standard userids and then disable the originals.

ASET	SPERRY	CMSRSI
CDTS	UNIVAC	ACFBAT
CMS	USAF	RETRIEVALS
VALCHG	SMXX6P	DCFS

- *(S104.210.00: CAT II) The IAO will ensure obsolete, pre-installed, standard userids do not exist on the system or are disabled.*

3.1.5.3 System or Hard-coded Demand Userids

The system or hard-coded application userids listed below will be kept on the system but need their passwords changed from the default after installation. Change the passwords as per *Section 3.1.6.3.4, Changing Passwords*. The DPS userid will be set up as a Profile 5 userid with SSBYCOMP. The STAR userid appears to be used at selected sites for site unique requirements and IQUMAS does not appear to needed by IQU.

STAR
IQUMAS
DPS

- *(S103.500.00: CAT I) The IAO will ensure standard, pre-installed userids on the system are secured properly.*

- *(S104.220.00: CAT III) The IAO will ensure the DPS userid is set up as a Profile 5 userid.*

3.1.5.4 Configured Demand Remote Site Interface Userids

These Demand Remote Site Interface (RSI) userids are cross-referenced to a configuration file, and are required for a product to work properly.

a. QUIKST. This Demand RSI userid is used for QuickStart (NJZMON). This userid will be set up as a Profile 3 with STRTZOPT, IMMEDST, Display CONS, and as a minimum, the SYMCTL, TIPGRP, and RNCNT1 console keyin groups. This userid is authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, and zero invalid password attempts. The runstream PROFILE/QUIKST in file JX$$0000*00 can be used to update this userid with the correct privileges. To change the password for QUIKST, first change the QUIKST password as per *Section 3.1.6.3.4, Changing Passwords*. Note that when signing on to Demand, QUIKST will send an outstanding message to the operator. Have the operator answer: GO. To change the password in the QS database, perform the following steps with the Security Officer's userid in demand mode:

   @QSBLD
   DEMAND QUIKST/<password> G99999
   EXIT

   Start QuickStart (ST QSRUN,,,<account>/<userid>).

b. IPFDDP, IPF, or DDP. This Demand RSI userid is used to start the file transfer jobs for DDP-FJT and will be set up as a Profile 5. This userid is authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, zero invalid password attempts, and System or User Enter Run Image. The System or User Entered Run Image is a requirement for the Virtual FTP userids. This userid is not needed to use the IPF editor. To change this password, first change the password in SIMAN as per *Section 3.1.6.3.4, Changing Passwords*, and then change it in the configuration file (usually DDP*CS$CONFIG) using SYS$LIB$*DDP-PPC.CSUPDT. All SSO Montgomery releases require the SSWRSUBDAC privilege to execute the secured CSUPDT processor.

c. Scheduler Userid. This Demand RSI userid is used to start jobs for Scheduler. The runstream PROFILE/SCHED in file JX$$0000*00 can be used to update this userid with the correct privileges. The Scheduler userid will be set up as a Profile 3 with STRTZOPT and IMMEDST privileges. This userid will also be account and project-ID enforced. This userid is authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, and zero invalid password attempts. To change this password, first change the password in SIMAN as per *Section 3.1.6.3.4, Changing Passwords*, and then change it in The Scheduler by using the SET USER command (assuming Scheduler is up).

d. Virtual Tape Handler Userid. The Virtual Tape Handler (VTH) software uses a Demand RSI userid to manage VTH activities. This userid is called VTHSRV and is installed when VTH is implemented. The runstream PROFILE/VTHSRV in file JX$$0000*00 can be used to update this userid with the correct privileges. This userid is authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, and zero invalid password attempts. To change this password, first change the password in SIMAN as per *Section 3.1.6.3.4, Changing Passwords*, and then change it in the configuration file using VTCNFG. The user will need to have the Bypass Ownership and Bypass ACR privileges to use VTCNFG.

e. EZLOAD Userid. This Demand RSI userid is used to start jobs on behalf of users who are executing the EZLOAD processor. This Demand RSI userid allows authorized users to quickly reload files from 9840 cartridge tapes that were created by FAS with the Fast Access Tape feature. This userid is call xxEZ00 (xx is the ALN site code). The runstream PROFILE/EZLOAD in file JX$$0000*00 can be used to update this userid with the correct privileges. The userid will be set up as a Profile 5 with the STRTZOPT privilege and RNCNT1 keyin group. This userid will have access to demand mode only and will be account and project-ID enforced. This userid is authorized to have up to 365 maximum password days, time out disabled, and zero invalid password attempts. To change this password, the Security Officer should first change the password in SIMAN as per *Section 3.1.6.3.4, Changing Passwords*, and then change it in the EZLOAD database by performing a @EZLOAD ACCESS. From the main menu, select Change Master (Option 1). Next, complete all fields and clear the "X" in the XMIT field and hit transmit. To complete the fields, first enter the Master Userid, FAS Directory tape device (e.g., u47L, HIS98, etc), FAS Backup tape device, number of days to retain EZLOAD data, Batch userid (normally the System Standard Batch userid), EZLOAD RSI userid created above with the PROFILE/EZLOAD, and EZLOAD RSI password.

- *(S104.230.00: CAT III) The SA will ensure the QUIKST userid is set up as a Profile 3 userid with the STRTZOPT and IMMEDST privileges.*

- *(S104.240.00: CAT III) The SA will ensure the IPFDDP, DDP, or IPF are be set up as a Profile 5 userid.*

- *(S104.250.00: CAT III) The SA will ensure the Scheduler userid is set up as a Profile 3 userid with STRTZOPT and IMMEDST privileges.*

- *(S104.260.00: CAT III) For DISA sites, the SA will ensure the VTHSRV userid is set up as a PROFILE/VTHSRV userid.*

- *(N/A: CAT III) For DISA sites, the SA will ensure the EZLOAD userid is set up as a PROFILE/EZLOAD userid.*

3.1.5.5 Shared Library System Userid

The Shared Library System (SLS) software uses a Demand userid in the automated TIF merge process. This userid is called xxJSTM (xx is the ALN site code) and is installed when SLS is implemented. This userid will be set up as a PROFILE/TAPE userid. The Shared Library System userid is authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, and zero invalid password attempts. To change this password, first change the password in SIMAN as per *Section 3.1.6.3.4, Changing Passwords*, and then update the SYSLIB*STRPARM.ATIFMRG element using the instructions outlined in the SLS implementation procedures. If this is an ALN site, will need to have the Bypass Ownership and Bypass ACR privileges to use SLSCNFG.

- *(N/A: CAT II) For DISA sites, The SA will ensure the Shared Library System userid is set up as a PROFILE/TAPE userid.*

3.1.5.6 Software Release Tape Transfer Userids

The Air Force HQ Standard Systems Group (HQ SSG) and SSO Montgomery personnel utilize the DDP-FJT Tape Transfer Processor, TXFR, to initiate tape-to-tape transfers of approved software releases to certain OS2200 hosts. Two specific userids have been assigned to these organizations for this process. The userid SSC-SSQM is assigned to HQ SSG Configuration Management and the userid GAJT00 is assigned to SSO Montgomery. DDP-FJT Tape Transfer userids will be set up as a Profile 8 userid with Batch only access and disabled. These userids are authorized access to an ALN exempt account.

- *(S104.270.00: CAT III) The SA will ensure the DDP-FJT Tape Transfer userid is set up as a Profile 8 userid with only batch access and disabled.*

3.1.5.7 Unattended Operations Support Software Userid

The Unattended Operations Support Software (UOSS) userid is used to start jobs identified in the UOSS control file for unattended operations. This userid will be set up with a Profile 2 to allow STRTZOPT (Start Run at System High) and IMMEDST (Immediate Start) privileges. This userid will be set up as a Profile 2 userid with Response CONS; SYMCTL, RUNSTA, and RNCNT1 console keyin groups; and the ability to user enter a run image.

- *(S104.274.00: CAT III) The SA will ensure the UOSS userid is set up as a Profile 2 userid with Response CONS; SYMCTL, RUNSTA, and RNCNT1 console keyin groups; and the ability to user enter a run image.*

3.1.5.8 Network Management System Userid

SECURITY or TELCON is the default Network Management System (NMS) password. There is no userid in SIMAN. To change the NMS password from its released default, refer to the following steps:

```
$$OPEN NMSC
IDE P <default password>
IDE P <default password  N <new password>
```

- *(A103.030.00: CAT II) The Network or Systems Administrator will ensure the NMS password is changed from the default.*

3.1.5.9 Transparent Userids

These are userids controlled by the EXEC. They require no effort to maintain and will not be altered.

a. Session Control Userids. These userids are COM-SYSTEM-L, COM-SYSTEM-H, and TIPOUTPUT. They will not have any run modes, will be disabled, and cannot be used by anyone other than the system. They are used when TIP Session Control is configured.

b. EXEC Userids. These userids are EXEC8 and INSTALLATION (or an alternate overhead userid). These two userids are created automatically during a SACRD$ initialization. They both are Profile 1 userids (all Privileges) but have no accompanying TSS$ records. Because there are no TSS$ records, they cannot be used by anyone other than the system. Do not create a TSS$ record for these userids without the coordination of SSO Montgomery. In system level HMP IX 7.0 and above there is no longer a separate SACRD$ file. All userid security information is contained in the SEC@USERID$ file. THEREFORE, EXEC8 an INSTALLATION will appear in all userid maintenance utilities but cannot be modified or deleted.

c. Fixed Gate Subsystem Userids. These userids are installed for the purpose of acting as owner userids for the various fixed gate subsystems in the environment. The following userids will be disabled, with Batch mode only (-DDP-PPC-, -CIFS-ADMIN-, and -MQS2200-). The -UDSxx- userids will be disabled, and only the -UDSxx- that support active application groups will be allowed access to Batch mode. All other Fixed Gate Subsystem userids will be disabled with no run modes.

HMP FIXED GATE SUBSYSTEM USERIDS		
GUJXFG	-OPE-TP-	-UDS07-
-ASIS-	-OSI-DIR-	-UDS08-
-CHAMELEON-	-OSI-TP-	-UDS09-
-CIFS-ADMIN- (Batch Only)	-OTM-	-UDS10-
-CMS1100-	-SQL-NET-	-UDS11-
-COMAPI-	-SX2200-	-UDS12-
-CPCOMMSS-	-TTW-	-UDS13-
-CPFTP-	-UDS01-	-UDS14-
-DDP-PPC- (Batch Only)	-UDS02-	-UDS15-
-DPS-	-UDS03-	-UDS16-
-EXPIPE-	-UDS04-	-UNIACCESS-
-INFOACCESS-	-UDS05-	--MEDIAMGR--
-MQS2200- (Batch Only)	-UDS06-	-CMS-SUBSYS-
-FTP-SUBSYS	-CPCOMM-SS	-HTPIC-2200
-MQS-	-NTSI-	-OPE-

Table 3-2. Fixed Gate Subsystem Userids

- *(S104.280.00: CAT III) The IAO will ensure Session Control userids do not have any run modes and are disabled.*

- *(S104.300.00: CAT I) The IAO will ensure in system levels below HMP IX 7.0 the EXEC userids (EXEC8 and INSTALLATION) do not have TSS$FILE records, only SACRD$ records.*

- *(S104.290.00: CAT II) The IAO will ensure all Fixed Gate Subsystem userids, except where noted, do not have any run modes and are disabled.*

3.1.5.10 Master Userid

The default Master userid for Unisys systems is GEN-tag dependent. The Master userid belongs to the site IAO for that system. Therefore, throughout this document the terms Master userid and Security Officer's userid refer to the same userid. The Master userid is the most powerful userid on the system, so protect it as much as possible. The Master userid requires extra protection. If it is even suspected that anyone knows the password for the Master userid, change the password. To secure the Master userid, perform the following steps:

a. Create a new userid like SECOFF using the SIMAN processor. Do not follow standard userid naming conventions when naming it. Make the new userid an Administrator in SIMAN, and make sure that this userid is a Profile 1 with the highest level of power and privilege possible. Select a standard account name to use as the new master account. Install it via SIMAN and make sure that the Master userid is registered under this new master account. The site IAO may select any standard format account name to use, but make sure the alternate site IAOs know the current Master userid and Master account, but not the password. The password will be secured as outlined in the next section. Use SIMAN to change the Master userid and Master account (reference *7831 0661, SIMAN Administration and Operations Guide*) to the userid and account just created.

b. Do not delete the old SECOFF userid from SIMAN, but do change the password. Access to Batch mode will be removed from the new Master userid just created. Unlike the Subadministrator userids, the Master userid can give a userid access to Batch even though the Master userid does not have the Batch access field set. However, SIMAN Subadministrators need to have access to Batch in order to install userids with access to Batch. Put the passwords for the new Administrator userid and for SECOFF into a sealed and marked envelope and place it in the site unit safe or a secure location that only the security office may access. Whenever either of these passwords is changed, update/replace the copy in the safe. The purpose for taking this step is to ensure that in an emergency situation, the site management can get access to the Master userid.

c. Perform some additional steps to make the new Administrator userid the true Security Officer userid in the TSS$ and SACRD$ files. Please contact SSO Montgomery for guidance in performing this step. Both the new Master userid that have been created and the backup administrator userid (which will usually be SECOFF) will be configured as the most powerful userids on the system. Remember that SIMAN Administrator userids will not have access to batch mode. SIMAN Administrators will have all the Interfaces, Privileges, CONS keyins and message groups, and Response CONS. On the SUBSYSTEM screen in SIMAN, it is very important that both these userids be configured as follows:

Subsystem Parameters for SECOFF screen name: SUBSYSTEM

System Control Designators:
[*] Allow Gates Built by this Subsystem to Disable Quantum Timer
[*] Allow Gates Built by this Subsystem to Defer Interrupts

Processor Privilege:
[*] Can Write Executive GRS in Addition to Ones Below
[_] Absolute Addressing in Basic Mode and Read GRS
[_] Can Only Read Executive GRS

Access Privilege:
[*] Kernel [_] Shell [_] Trusted

Subsystem Sharing Level:
[*] SYSTEM – Subsystem accessible across system
[_] APPLICATION – Subsystem accessible throughout application
[ ] RUN – Subsystem accessible throughout the duration of run

Table 3-3. SIMAN Subsystem Screen

- *(S104.020.00: CAT I) The IAO will ensure the Master userid and userids with SIMAN Administrators privilege do not have access to batch mode.*

3.1.5.11 Subadministrator Userids for IAOs

Non-site personnel performing userid administration functions need to be implemented as SIMAN Subadministrators, not Administrators. In a decentralized security environment, the site IAO delegates most of the routine userid administration duties to IAOs at the remote sites. Since an IAO at one remote site would not need the capability to create or modify userids for another remote site at the same site, the IAOs at the remote site are configured as basically a modified Profile 3/4 userid with extra security Privileges and SIMAN Subadministrator status. A Subadministrator in SIMAN can only modify userids owned by that Subadministrator userid. Unlike the Master Userid or IAO with administrator privileges, the IAO's Subadministrator userid will be given access to TIP, Demand, and Batch. The reason for this is that a SIMAN Subadministrator has to possess a characteristic (in this case access to Batch mode) before that userid can install or modify another userid and give it that characteristic. A special profile runstream has been added to the JX$$0000*00 file to assist in configuring IAO, with subadministrator privileges, userids. To use it, install the basic userid to be used by the IAO, and then type the following from a demand mode session (as the Master userid):

@ADD JX$$0000*00.PROFILE/SUB

This runstream will prompt the user to enter the name of the IAO userid, and then configure it correctly for an IAO with subadministrator privileges. Before using this runstream to modify an existing IAO, with subadministrator privileges, userid, check and make sure that the userids being administered by that IAO do not have any Interfaces (ERs), privileges, CONS level, or any other userid characteristic that is not included in the PROFILE/SUB runstream. If the modified IAO with subadministrator privileges userid has less power than any of the userids being administered, the IAO userid will not be able to access the more powerful userids, even if they are owned by the IAO.
Subadministrators will have the following attributes:

Minimum Clearance level:	0
Maximum Clearance level:	0
Run Modes:	Batch, Demand, TIP
The user will have a security record:	Yes
Quantum Timer	Disabled
Defer Interrupts	Disabled
Processor Privilege:	Can Only Read Executive GRS
Access Privilege:	Ordinary (None)
Record Access	Private
System Control Designator:	None
Subsystem Sharing Level:	None
Min Password days:	0
Max Password days:	90 – Can be 365 if authorized FTP userids are owned by the subadministrator
Max days inactivity:	35 – Can be 65 days if administrating CAMS or SBSS userids

Max invalid login attempts:	3
Time Out (Initial and Maximum):	For example: 780 if administrating CAMS userids; 540 for SBSS; or else 15 minutes or the system wide time out value
Record Access:	Private
File Creation:	User to Create Only Unowned Files
Console Mode:	Display or Lower
The following Interfaces (ERs):	IOAID$, RSI$, TERMRUN$, RLP$, TPLOG$, PB$CON, FCREG$, RT$PSI, TRTIM$, FS$UTF, CONNECTTIP, VTPUR
The following Keyins:	GENSTA, RUNSTA, LOGGIN, DATKEY
Display access to the following message groups:	SYSMSG, IOMSG, RSICOM, HDWCON, USER4, USER5, USER6, USER7, TPMSG, DSKMSG, PRTMSG
The following Privileges:	MODRECCL, CRESECRD, MODSPFLG, SETGAP, MODRUNCL, FASHNDL, TIPGET, TIPSEND, SSSSCALLANY, ABSDVASG, MSCONRET, SSMMGRILES1, MODINTPR, EXTACQUR, DREG, MODSECRD, SMOQUE, LEVEL$, MOUNTAPE, FILDELET, MODRECOO
In all cases, it is important that the subadministrators be restricted to a defined list of accounts on the ACCESS screen. This list will be limited to those accounts used by the customers at that site. Because the IAO is the only person performing account maintenance, this measure further reduces the risk of improper billing of customers. In an ALN environment, the subadministrator will also be restricted to a defined list of project-IDs on the ACCESS screen. The accounts and project-IDs that are available for a subadministrator's use will only consist of valid accounts and project-IDs.	

Table 3-4. Subadministrator Configuration

- *(S104.060.00: CAT II) For DISA sites, the SA will ensure a subadministrator's configuration matches the profile specified in this STIG.*

- *(S104.070.00: CAT II) The SA will ensure subadministrators are be restricted to the accounts they can assign to userids.*

- *(S104.080.00: CAT II) The SA will ensure the list of accounts available to a subadministrator consist of valid accounts.*

For ALN:

- *(S104.090.00: CAT II) The SA will ensure subadministrators are restricted to the project-IDs they can assign to userids.*

- *(S104.100.00: CAT II) The SA will ensure the list of project-IDs available to a subadministrator consist of valid project-IDs.*

3.1.6 Password Controls

Passwords are currently the only key securing userid access to the system. As such, password management is a critical issue.

3.1.6.1 Requirements

Some of the material for this section was drawn and adapted from the National Computer Security Center publication, *Password Management Guideline*. Personnel having a need for a more complete explanation need to consult that publication for further details, with the understanding that the password management strategy on the Unisys systems is somewhat constrained by the Unisys operating system. The fundamental security objectives for password systems are:

a. Individual Accountability. First, individual accountability is the key to securing and controlling any computer system. Second, there is a need for authentication. Without authentication, user identification has no credibility.

b. Password Vulnerabilities. Passwords are vulnerable to compromise due to five essential aspects of the password system:

   1. A password will be initially assigned to a user when installed on the system.

   2. A user's password will be changed periodically.

   3. The system will maintain a "password database."

   4. Users need to remember their passwords.

   5. Users will enter their passwords into the system through a terminal at login time.

c. Password Protection. Although the system may process only sensitive unclassified information, the data will still be protected from unauthorized access. Even though a password is unclassified, the user will protect his or her password from disclosure to any other person. Passwords that are used in AISs that operate in the System High Security Mode will not be classified, but will be protected as "For Official Use Only" information.

d. Password Requirements. Password systems used to control access to IT systems that process or handle classified or other sensitive information need to assure:

   1. Individual Identification. To uniquely determine the name for each and every person using the system.

   2. Authentication. The absolute verification of the user's claimed identity.

   3. Password Privacy. To the extent possible, the system will protect the password database as sensitive information. There will not be any files on the system

containing userids and their passwords that can be accessed by unauthorized personnel.

4. Passwords on DOD Unisys systems will be six characters, eight characters in system level HMP IX 7.0 and above, long. The minimum password expiration will be one day and the maximum password expiration will be 90 days. Only documented exceptions in this STIG can deviate from these settings.

5. Passwords in system levels below HMP IX 7.0 will be a combination of alphanumeric, non-repeating, non-consecutive characters. SSO Montgomery released a local code change, which enforces these password construction rules, to all ALN, DNMC, and DFAS-IN (Indianapolis) sites in April 2000. Password construction rules will be included in the Security Features User Guide (SFUG).

6. Passwords in system level HMP IX 7.0 and above will be a combination of upper case characters, lower cases characters, numeric characters, and special characters (A-Z, a-z, 0-9, and all special characters except a slash, comma, semi-colon, period, asterisk, and pound sign). The characters will be non-repeating and non-consecutive.

- *(S103.860.00: CAT II) The IAO will ensure userid/password combinations are adequately secured from access by unauthorized personnel.*

- *(S103.410.00: CAT II) The SA will ensure all users, except documented exceptions, have a minimum password expiration of one day.*

- *(S104.400.00: CAT II) The SA will ensure all users, except documented exceptions, have a maximum password expiration of 90 days.*

3.1.6.2 Password Use

A password will be solicited for each userid at the time system log-on is attempted. Such passwords will authenticate authorized users to the system.

a. TIP and Demand processing. In order to sign on into TIP or Demand mode, the user will enter a userid and password. The Executive will only allow passwords exactly six (eight to eighteen characters in system level HMP IX 7.0 and above) characters long. The password will consist of a combination of alphanumeric and special characters (A-Z, 0-9, and all special characters except a slash, comma, semi-colon, period, asterisk, and pound sign, in HMP IX 7.0 and above the range a-z has been added).

NOTE: SIMAN will not accept the semi-colon as a password in SIMAN batch mode; and although SIMAN will accept a period, asterisk, and pound sign, using these characters in the password or the SIMAN Information screen causes problems in the SECMERGE/SIMAN software and will not be used. The userid and password are not case sensitive prior to HMP IX 7.0, and the password will not contain consecutive or repeating characters.

b. Batch processing. For batch or remote batch processing (e.g., ST or @START runs), the userid is not needed in the runstream. Also, the password for that userid will not be in the runstream. Remote batch runs emulating a card reader (e.g., runstreams that are submitted using the DDP-FJT SUBMIT command via IPF, DDPFJT batch command interface, or DDPFJT menu interface) require a valid userid and password. The files containing the runstreams that are used in the DDP-FJT SUBMIT runs will be protected with an ACR, and the userid within the card reader simulated runstream will have a run mode of Batch only.

c. Files. File passwords (read or write keys), if needed, will be entered on the @ASG or @CAT control command.

d. NMS. The NMS password controls access to the Network Management System. This allows a user to UP and DOWN lines, communicate directly to the DCP, etc. There is no userid.

e. Terminal passwords. Some terminals (like the PWT 120) require a password just to use the terminal, offering another level of protection. There are also products available to provide password protection for PCs. Use of such features, if available, is actively encouraged.

f. DPS passwords. The DPS processor has a password database. Do not assign a userid in the DPS password file the same password as the userid has in SIMAN.

- *(S103.860.00: CAT I) The IAO will ensure files containing the runstreams are used in the DDP-FJT SUBMIT runs are protected with an ACR, and the userid within the card reader simulated runstream have a run mode of Batch only.*

- *(S103.470.00: CAT I) The IAO will ensure the password identified for a userid in the DPS password file is not the same password is assigned to the userid in SIMAN.*

3.1.6.3 Password Management

The IAO will assign userids and passwords for use by users. Once the userid and password are issued, the user will manage the password after the initial sign-on. The end user of the userid/password will be instructed to sign on immediately upon receipt of the initial userid/password in order to minimize the vulnerability of the initial password to compromise.

- *(A102.090.00: CAT II) The IAO will develop written procedures to ensure user passwords are changed to a random value at install, deactivation, and reset time.*

3.1.6.3.1 Assigning Passwords

In an environment where the IAO is collocated with the users of the system, the IAO will assign and distribute passwords in a controlled manner as determined by local site procedures. In a decentralized security environment, the local IAOs will usually handle password assignment and distribution since they are physically located at the same remote site as the end user. The site

IAO is still updated as far as userid usage is concerned since only the site IAO can update accounts directly. In either case, controlled password distribution to individual users will establish a positive audit trail and will prevent inadvertent release of passwords to unauthorized users. In a centralized security environment, the site IAO will establish a secure and reliable method for transmitting initial or reset passwords to an end user or TASO. A recommended procedure is to have a small, trusted list of TASOs that can be identified by voice recognition. Transmit the passwords to these TASOs and force the user to sign on immediately and change this initial password.

3.1.6.3.2 Password Generation

If an algorithm is used to generate a password for a user at userid creation or reassignment, the password will be randomly generated. No duplication of generated passwords will occur. Passwords will not be drawn from a pool of passwords in such a way that the same password may be assigned to more than one user. Generated passwords will be alphanumeric case sensitive with non-repeating characters.

3.1.6.3.3 Password Construction Rules

SSO Montgomery has put in local code so a user will use the following password construction rules when changing his/her password:

a. The password must be six characters in length. Eight characters in length in system level HMP IX 7.0 and above.

b. The password will consist of a combination of alphanumeric and special characters (A-Z, 0-9, and all special characters except a slash, comma, semi-colon, period, asterisk, and pound sign, the range of a-z was added in HMP IX 7.0 and above).

NOTE: SIMAN will not accept the semi-colon as a password in SIMAN batch mode; and although SIMAN will accept a period, asterisk, and pound sign, using these characters in the password or the SIMAN Information screen causes problems in the SECMERGE software and should not be used.

c. The userid and password are not case sensitive prior to system level HMP IX 7.0, and the password cannot contain consecutive or repeating characters.

3.1.6.3.4 Changing Passwords

The IAO, end user, or operating system will change a password when:

a. The IAO is notified by a TASO that an individual having knowledge of a password has been transferred, discharged, or reassigned.

b. An individual’s security clearance has been administratively reduced or suspended.

c. The password has not been changed in the last 90 days. In SIMAN, the field that controls the minimum number of days that need to pass before a password can be changed will be set to one day, and the field that controls the maximum allowable period before the system will force a user to change his or her password will be set to 90 days. The Demand RSI userids identified in *Section 3.1.5.4, Configured Demand Remote Site Interface (RSI) Userids*, are authorized to have up to 365 days of inactivity, 365 maximum password days, time out disabled, and zero invalid password attempts.

d. Release tapes are released from the source (HQ SSG, CDA, Vendor, etc.) containing *generic* passwords.

- *(S104.410.00: CAT II) The SA will ensure all users, except documented exceptions, have a minimum password expiration of one day.*

- *(S104.400.00: CAT II) The SA will ensure all users, except documented exceptions, have a maximum password expiration of 90 days.*

3.1.6.3.5 FTP Userids

It is recognized that production problems may occur if passwords for userids that perform File Transfer Protocol (FTP) data transfers as part of an automated program-to-program interface expire within the 90-day time period specified above. For FTP userids used for automated program-to-program interfaces is acceptable to establish FTP logons with extended expiration password settings if mitigating controls are in place and the data owner has been apprised of the risks, and has officially documented and acknowledged those risks. The maximum password setting allowed for these FTP only userids is 365 days. The password change should be synchronized with the client process at a convenient time prior to its expiration to avoid the interruption of a production cycle. If subadministrators own these FTP userids, then they will also need a maximum password setting of 365 days

a. As a mitigating control, the script owner will ensure that all scripts, JCL, ECL, programs, and/or data files containing one or more userid/password pairs are secured. In addition, the script owner is responsible for the scripts, JCL, ECL, programs, and/or data files and will restrict access to the files to the fewest practical number of personnel. At any time, either DOD or the other organization involved with this interface can review the procedures used by the script owner to ensure this mitigating control is properly implemented.

b. The use of FTP and other file transfer methods require the userid/password and application data to be transmitted to/from the host system in clear text, across unsecured communication lines. While some data transfer tools (such as Connect Direct: NDM) can encrypt the data from point of source to destination, not all data transfer tools do. This increases the potential for compromise by various means (e.g., a sniffer program). The primary risk to the data source is disclosure of data to unauthorized persons, and the primary risk to the data destination is interception and modification of data by an unauthorized person. There is no direct mitigating control for this risk, but the office responsible for installation and configuration of the userid used for this interface will

ensure that the userid is configured with the lowest privilege level possible in order to limit the damage that it can do if compromised.

c. The compromise of the userid/password and/or application data could remain undetected for a long period of time. The password for this data transfer userid expiration can be set for up to 365 days on Unisys domains. A procedure will be developed and implemented, in coordination with the customer, to manually change the password at least every 365 days or when an administrator with knowledge of the password leaves. The use of an extended expiration password increases the window of exposure to the system in the event that the userid and password are compromised. This risk can be mitigated by periodic password changes even if the password is set to never expire automatically. The script owner and the office responsible for installation and configuration of the userid will ensure that the password length and construction meet or exceed DOD standards as stated in the appropriate STIG.

- *(S102.014.00: CAT II) The SA will ensure the maximum allowable password setting for FTP userids used for system to system transfes up to 365 days.*

- *(S102.014.00: CAT II) The IAO or SA will ensure procedures are developed and implemented, in coordination with the customer, to manually change the password at least every 365 days or when an administrator with knowledge of the password leaves.*

3.1.6.3.6 Password Change Methods

There are several ways to change the password for a userid. This will be done in addition to any password changes within any configuration files associated with the userid.

3.1.6.3.6.1 Password Change by User

A user may change their password only if the current password is known, and users are limited to a maximum of one password change per day. The example below is the only approved method of changing a user's password. Since the @@PASSWD command is logged in it entirety and could be found within the system log, SSO Montgomery has implemented local code that disables the @@PASSWD command.

Enter your userid/password and clearance level: (system)

<userid>/<old password>/<new password> (user)

This will change the password in the systems security database.

- *(A101.060.00: CAT III) The IAO will ensure users do not use the @@PASSWD command to change their password.*

3.1.6.3.6.2 Password Change by Security Officer

The Security Officer may change the password in SIMAN.

```
@SIMAN,B
UPDATE USER = <userid> PASSWORD = <new password>  ;
@EOF
```

The first time someone signs on with this userid, the system will ask for a new password again. Therefore, allow users to enter their own new passwords. For system userids that have passwords that have to match an entry in a configuration file, use SIMAN to change the password to something simple like "TMP010". Then immediately sign on with the userid as follows:

Enter your userid/password and clearance level:	(system)
<userid>/<old password> ("TMP010")	(user)
Your password has expired. Enter your new password:	(system)
<new password>	(user)
Your password has been replaced.	

3.1.6.3.6.3 Passwords changed by the TASO

SSO Montgomery released an Automated Reset Process (ARP) Program that allows authorized Terminal Area Security Officers (TASOs) to change a userid's password, Section *8.2.1* Automated Reset Process Program. All TASOs utilizing the ARP program will verify the identity of userids being entered against the individual's SAAR. The IAOs will verify that only authorized TASOs have access to the Q shred AIS accounts. The IAOs will maintain a list or documentation of authorized TASOs who have access to the ARP program. This list will contain the TASO's name, userid, organization, phone number, and authorized Q shred AIS account.

- *(S103.856.00: CAT II) The IAO will ensure only authorized TASOs and IAOs have access to the respective Q shred accounts.*

- *(S103.854.00: CAT III) The IAOs will maintain a list of authorized TASOs who have access to the ARP program. This list contains the TASO's name, userid, organization, phone number, and authorized Q shred AIS account.*

3.1.7 Console Mode

3.1.7.1 General Requirements

Console mode, more commonly known as CONS mode, allows a Demand user to emulate some or all of the functions of the systems operator. If the user has DISPLAY or RESPONSE level CONS, he or she has access to operator keyins and can view unsolicited messages, as they would appear on the operator's console. This is also known as scrolling CONS. If the user has FULL or lower CONS, he or she will have access to keyins only. The level of CONS, as well as keyin groups and message groups within the CONS level, determines access. Some of these keyins are very dangerous if misused, and others can be detrimental to system performance if they are overused. Because of this, it is important to ensure the correct level of CONS is assigned to a specific user profile. Even relatively low levels of CONS access are a security risk, but this needs to be balanced against the timesaving and convenience of CONS mode. Exceptions or deviations will be justified and documented by the IAO.

- *(S103.360.00: CAT II) The IAO will ensure users, except where documented, do not have access to CONS levels beyond specified in their security profile.*

3.1.7.1.1 Using CONS Keyins

Normally, there are two ways of entering CONS keyins. The first is by entering @@CONS. The user is now in CONS mode and can enter keyins in the same manner as an operator. The second means is by entering @@CONS <keyin>. The keyin is accepted by the system, but the user is not actually in CONS mode. If the keyin generates a read-and-reply message, the message is redirected to the operator and is not seen by the user.

3.1.7.1.2 Scrolling CONS

In order to enter scrolling CONS, the user needs to have a CONS level of either DISPLAY or RESPONSE. The user enters @@CONS and then can see all unsolicited operator messages, for which they have message groups indicated, as they are generated. This gives the user a way to watch jobs start and "fin.", users sign on, etc. Some sites may have a program called @CONS, which also places authorized users in scrolling CONS. However, scrolling CONS has a direct and detrimental effect on system performance (since the system will send all console messages to all terminals that are in scrolling CONS), and will be severely restricted outside the site. See *Section 3.1.7.1, General Requirements*, for more detailed guidance on giving scrolling CONS to non-site users.

3.1.7.1.3 Full CONS

It should be noted that Full CONS has almost the same power as Display CONS and is therefore very dangerous. Many people incorrectly assume that only Display and Response CONS need to be secured.

3.1.7.1.4 Activated Response CONS

If a user has RESPONSE CONS mode and has an R set in any or all of the message groups (third CONSOLE screen in the SIMAN userid record), that user will intercept messages meant for the operator whenever he or she enters CONS mode. This is called ACTIVATED RESPONSE CONS mode, and is extremely dangerous, since a user with this level of CONS takes over the system console from the operator.

NOTE: Only the messages controlled by the activated message groups will be intercepted by the user. Only one user may be in ACTIVATED RESPONSE mode per console message group. Operators will not see these messages at all. Normal users in scrolling CONS will still be able to view the messages. Therefore, no userid on a site or remote system will have ACTIVATED RESPONSE CONS.

- *(S104.120.00: CAT I) The SA will ensure userids do not have ACTIVATED RESPONSE CONS.*

3.1.7.1.5 Entering CONS

A user enters @@CONS and is now in CONS mode. While the user is in CONS mode, any commands not starting with @ or @@ are assumed to be CONS commands.

3.1.7.1.6 Exiting CONS

In order to exit CONS mode, the user enters either @@END CONS or @@END. Any unanswered read-and-reply messages waiting on the user will be redirected to the operator to answer. Any response message groups will be routed back to the operator.

3.1.7.2 Keyin Groups

CONS keyins are broken down into groups. If a user has access to a particular group, that user can perform any of the keyins in that group, as long as the level of CONS allows that keyin. In other words, if a user can do a TM keyin (terminal message), he or she can also do a TB keyin (terminal broadcast). However, if the user has FULL CONS mode and can do an E keyin, he or she cannot do an II keyin, since this keyin is restricted to a userid with RESPONSE level CONS.

3.1.7.2.1 Keyin Groups and CONS Mode

The following tables show which keyins are usable within each keyin group and which keyins are usable within each console mode. The operator has more keyins available. These are the ones available to users. (Refer to the *SIMAN Administration and End User Guide, 7831 0661, Table 5-1.*)

KEYIN GROUP	*BASIC*	*LIMITED*	*FULL*	*DISPLAY*	*RESPONSE*
CMBRLD					RL
COMMUN		TM	TB, TM	TB, TM	HK, HM, TB, TM
DATKEY	D**	D**	D	D	D
DEBUGS			AR, CJ, DJ, IT, SJ	AR, CJ, DJ, IT, SJ	BP, C, DU, FC, IOPHFL, IT, $!
DEVCNT			CTL, DN, MD, RD, RV, UP	CTL, DN, MD, RD, RV, UP	CTL, DN, MD, RD, RV, PL, UP
GENSTA	MU	MU, FS, SS	EU, FF, FS, MU, SS	EU, FF, FS, MU, SS	EU, FF, FS, MU, SS
LOGGIN	LG*	LG*	LG	LG	LG
MSGREC			MR	MR	MR
MSTCNT			DC, EX, FA, IN, MS, MV, PM, PR, SH, SU, TU, UD, UL	DC, EX, FA IN, MS, MV, PM, PR, SH, SU, TU, UD, UL	DC, DP, EX, FA, IN, MH, MS, MV, PM, PR, RP, SH, SU, TU, UD, UL
PRFANL					SB
RNCNT1	CS*, E*, RM*	CS*, E*, RM*	B, CS, E, RM, ST	B, CS, E, RM, ST	B, CP***, CS, E, II, RM, ST
RNCNT2			X	X	X
RNCNT3			SP, RE	SP, RE	CK, RS, SP, RE
RUNSTA	RC*	BL, RC, T	BL, RC, T	BL, RC, T	BL, RC, T
SECURI					SC, SF, TS
SYMCTL	SX*, SQ*	SQ, SX*	SM, SQ, SR, SV, SX	SM, SQ, SR, SV, SX	SM, SQ, SR, SV, SX
TIPGRP		TIP	AP, AT, FB, LB, LC, TF, TIPSS, TP	AP, AT, FB, LB, LC, TF, TIPSS, TP	AP, ARCMR, FB, LB, LC, TIPSS, TP

Table 3-5. CONS Keyins within Console Modes

* These keyins apply only to the user's run.
** No update capabilities are allowed.
*** The CP keyin is no longer supported in HMP IX 7.0.

3.1.7.2.2 Dangerous Keyin Groups

The following keyin groups can be dangerous to the system and therefore will not be given to any users outside the site unless the keyin group is authorized as part of the user's profile (e.g., TIPGRP for a Profile 4 user). . These keyin groups are only the most obvious examples of dangerous keyins. Other keyin groups can also cause problems if misused. Consult *Table 3-22. Keyin Groups and Profiles*~~*Table 3-22. Keyin Groups and Profiles*~~*Table 3-22. Keyin Groups and Profiles*, for a complete list of how CONS keyins are linked to the userid security profiles. On ALN systems, the only keyin groups that may be given to users outside the site and outside their userid profile is SYMCTL (Limited CONS or lower).

On DNMC, and DFAS-IN (Indianapolis) shared production/development systems, the only keyin groups that may be given to users outside the site and outside their userid profile are SYMCTL (Limited CONS or lower), or RNCNT1 (Limited CONS or lower). The exceptions referenced above cannot be excessive and will be documented on the user's SAAR. On DNMC, and DFAS-IN (Indianapolis) shared production/development systems, if RNCNT1 (Full or Display CONS) or SYMCTL (Full or Display CONS) are required by users outside the site and outside their profile, then a request letter will be approved and on file with the IAO.

KEYIN GROUP	***DANGEROUS USAGE***
CMBRLD	RL Keyin causes a common bank to be reloaded.
DEVCNT	A user can up/down tape drives, disk drives, etc.
SYMCTL	A user can delete print files. On ALN domains, can cross ALN boundaries.
RNCNT1	Can start unauthorized jobs or terminate jobs. On ALN domains, can cross ALN boundaries.
RNCNT2	X keyins can corrupt databases. Do not use!
RNCNT3	Runs can be checkpointed and restarted.
PRFANL	Keyins can affect collection of performance data, UPS operation.
MSTCNT	Mass Storage Control Keyins; only required by site personnel.
DEBUGS	C keyins can corrupt the EXEC. $! Keyins will crash the system.
TIPGRP	A user can up/down the audit trails and application group.

Table 3-6. Dangerous CONS Key Groups

- *(S104.370.00: CAT II) The SA will ensure users, except where documented, do not have access to security related CONS keyin groups beyond those specified in their security profile.*

3.1.7.2.3 Detrimental Keyins

These keyins are not dangerous, but if used excessively or incorrectly, they may cause performance problems. If it is suspected these keyins are being abused, use Log Analyzer to determine if a solution is required.

KEYIN	***GROUP***	***PROBLEM***
SQ	SYMCTL	Degrades performance if used frequently to check print listings.

KEYIN	*GROUP*	*PROBLEM*
RC	RUNSTA	Degrades performance if used frequently to check job status.
CS	RNCNT1	A user can upgrade a job to "Deadline priority." This takes time slices away from other jobs.

Table 3-7. Detrimental Keyins

3.1.7.2.4 End User Keyins

Most Demand mode end users need these keyin groups:

GENSTA
RUNSTA
LOGGIN
DATKEY

3.1.7.2.5 Site Keyins

These keyin groups are only for use by certain profiles at the site (and for some, only at the operator's console) and are not required by the vast majority of end users. Be very careful about giving these keyin groups to anyone outside the site. On DNMC, and DFAS-IN (Indianapolis) systems, the IAO may authorize specific users access to SYMCTL (Limited CONS or lower) or RNCNT1 (Limited CONS or lower).

On ALN systems, the IAO may authorize specific users access to SYMCTL (Limited CONS or lower). This access will not be excessive and the requirement will be fully documented on the individual's SAAR. On DNMC, and DFAS-IN (Indianapolis) systems, if RNCNT1 (Full or Display CONS) or SYMCTL (Full or Display CONS) are required by users outside the site and outside their profile, then a request letter will be approved and on file with the IAO.

SECURI	CMBRLD	DEBUGS	DEVCNT	MSGREC	PRFANL
RNCNT1	RNCNT2	RNCNT3	SYMCTL	MSTCNT	

3.1.7.3 Message Groups

The operator receives messages via the message groups. Users with DISPLAY or RESPONSE CONS mode may watch these messages scroll by if they have the associated message group specified in their SIMAN userid records. The message groups control the following types of messages.

MESSAGE GROUP	*MESSAGES CONTROLLED*
SYSMSG	Normal system messages. Job messages.
IOMSG	Messages from I/O controllers.
RSICOM	Communication Messages (users signing on/off, etc.)
HDWCON	Hardware controller messages.
USER4-USER7	May be specified by a user program. Good for removing unassociated messages from normal messages.
TPMSG	Messages from tape drives.
DSKMSG	Messages from disk drives.
IPMSG	Messages from Instruction Processors
PRTMSG	Messages from system printers.

Table 3-8. Message Groups

References. Refer to ECL Programming Reference Manual, 7830 7949, for more information on CONS keyins and CONS levels. Refer to 7831 0281 and 7831 0299 for an explanation of CONS keyin use.

3.1.8 User Profile System

The following sections explain the purpose of the security profiles that have been established for the Unisys environment, give examples of their use, and outline the general procedure for determining the proper profile level for a particular user.

Sites are required to implement and adhere to the profile system outlined in the following sections; however, sites may deviate from this standard if sufficient justification exists. Deviations will be clearly documented, justified, and coordinated through the site IAO for the system involved. Significant deviation involving many userids will be coordinated with SSO Montgomery to ensure that (1) the security profiles outlined in this STIG accurately reflect the needs of the sites, and (2) any problems associated with this deviation can be worked out prior to the next Security Readiness Review, where such deviations can become findings.

- *(S104.030.00: CAT II) The IAO will ensure there is a security profile system in place to ensure the least privilege concept is enforced.*

- *(S104.040.00: CAT II) The IAO will ensure userids reflect the profile system and the distribution requirements identified in this STIG. Discrepancies between the profile and the actual access granted is justified and documented.*

- *(S104.050.00: CAT II) IAOs and SAs will follow the profile guidelines when assigning userids.*

3.1.8.1 Purpose

The purpose of the security profiles documented in this section is to assist IAO personnel in implementing the principle of least privilege in the Unisys environment. This principle states that on any computer system, a user will be given a userid with the least amount of power and

privilege required for that person to perform his or her legitimate duties. By establishing the nine general userid profiles documented in the sections below, we have made it easier and quicker for an IAO to determine the exact levels of Interfaces, Privileges, CONS level, CONS keyin groups, and accounts to assign to a user.

3.1.8.2 Standard Security Profiles

The following paragraphs list the nine standard security profiles that are used in the DOD Unisys environment. These profiles reflect the most common minimum requirements for each type of user based on that person's job. See *Section 3.1.8.12, Determining a User's Profile*, for a more detailed explanation of how to determine the proper security profile for a particular user. Modified standard security profiles have been created for IAOs with subadministrator privileges, system operators, tape librarians, and performance monitoring personnel, and that these modified profiles are outlined in *Section 3.1.12.9, Special Security Profiles,* in this section. Individuals assigned Profile 1 and 2 userids will be cleared for Information Technology (IT)-I positions and the background investigation will not be older than six years.

NOTE: ALN exempt accounts apply to sites running the ALN operating system with ALN activated.

- *(S104.420.00: CAT II) The SA will ensure users, except where documented, do not have access to clearance levels beyond those specified in their security profile.*
- *(S104.360.00: CAT II) The SA will ensure users, except where documented, do not have access to CONS levels beyond specified in their security profile.*
- *(S104.370.00 CAT II) The SA will ensure users, except where documented, do not have access to CONS keyin groups beyond those specified in their security profile.*

3.1.8.2.1 Site Security Officers

Profile:	1
Includes:	All site Security Officers and review team members. Security software developers and security quality assurance evaluators at dedicated CDA Domains. Users having this profile will be IT-I cleared.
Clearance Level:	0 through 63
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Response
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	Yes

Table 3-9. Profile 1

3.1.8.2.2 Senior Level Site Technical Personnel

Profile:	2
Includes:	Senior DBM/DBAs, Systems Analysts, and Operators (if necessary). Senior system software programmers, developers, and quality assurance evaluators at dedicated CDA Domains. Users having this profile will be IT-I cleared.
Clearance Level:	0 through 63
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Display or Response
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	Yes

Table 3-10. Profile 2

3.1.8.2.3 Site System/Surveillance Monitors

Profile:	3
Includes:	Junior DBM/DBAs, Schedulers, Senior AIS Monitors, and BLISS Release Monitors. Junior system software programmers, developers, and quality assurance evaluators at dedicated CDA Domains.
Clearance Level:	0 through 63
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Display
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	Yes

Table 3-12. Profile 3

3.1.8.2.4 Application Programmers on Dedicated CDA Domains

Profile:	4
Includes:	Junior AIS Monitors. Applications programmers on dedicated CDA Domains.
Clearance Level:	0 through 63
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Display
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	No

Table 3-13. Profile 4

3.1.8.2.5 High-level Customer DBAs/Functional Users Outside the Site

Profile:	5
Includes:	High Level Customer DBAs or Functional Users Outside the site.
Clearance Level:	0 through 0
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Display
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	No

Table 3-14. Profile 5

3.1.8.2.6 AIS Managers and Application Programmers of TIP/Database Systems on Shared Production/CDA Domains

Profile:	6
Includes:	AIS Managers and Application Programmers of TIP/Database Systems on shared Production/CDA Domains.
Clearance Level:	0 through 0
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Full
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	No

Table 3-15. Profile 6

3.1.8.2.7 AIS Managers and Application Programmers of Batch/Demand Systems on Shared Production/CDA Domains

Profile:	7
Includes:	High-Level end users. AIS Managers and Application Programmers of Batch/Demand Systems on shared Production/CDA Domains.
Clearance Level:	0 through 0
Secured Interfaces:	See Table 3-19. Interface Profile Mapping.
Secured Privileges:	See Table 3-20. Privilege Profile Mapping.
Console Mode:	Limited
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	No

Table 3-16. Profile 7

3.1.8.2.8 Functional Users with Demand Mode

Profile:	8
Includes:	General Functional User with Demand Access.
Clearance Level:	0 through 0
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	Basic
CONS Keyins	See Table 3-22. Keyin Groups and Profiles
ALN Exempt Account?	No

Table 3-17. Profile 8

3.1.8.2.9 TIP and Batch Only Users

Profile:	9
Includes:	Users with TIP and Batch Access Only; all others not identified in Profiles 1-8.
Clearance Level:	0 through 0
Secured Interfaces:	See Table 3-19. Interface Profile Mapping
Secured Privileges:	See Table 3-20. Privilege Profile Mapping
Console Mode:	None
CONS Keyins	None
ALN Exempt Account?	No

Table 3-18. Profile 9

3.1.8.3 Interfaces

The following table is a list of Interfaces and their associated profile. The interfaces with a * will be enforced under SIMAN and those with a ** will always be enforced under SIMAN.

INTERFACE NAME	***FUNCTION***	***PROFILE***								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
ABSAD$	Access to Downed Mass Storage	*	*							
AC$NIT	Online Initialization	*	*							
ACCNT$	Read/Write Summary Account File	*								
*AP$KEY	Step Control App Group Recovery	*	*							
*AT$KEY	Specified Audit Trail Recovery	*	*							
AUDIT$	Audit Trail Interface	*	*							
AUDIT$TRAIL	Audit Trail Call	*	*							
**BDSPT$	Down Mass Storage	*	*							
CARTTAPELIB$	Allow Use of Cart-Tape Interfaces	*	*							
CMS$REG	EXEC Register Output Queue	*	*							

INTERFACE NAME	***FUNCTION***	***PROFILE***								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
CONNECT$TIP	Connect to TIP Call	*	*	*	*	*	*	*	*	*
*DEV$INFO	Returns device info within type	*	*							
DMABT$	DMR Abort	*	*							
DNLOD$	Down-Line Loading of SSP	*								
*DUMP$SUBSYS	Dump Subsystem Call	*	*							
ERCVS$	EXEC Step Control Recovery	*	*							
*ERTRAP$	Register ER Trapping	*								
EX$CRD	EXEC Core Read	*	*							
*FCREG$	File Registration with TIP	*	*	*	*	*	*			
FS$UTF	Freespace Utility Functions	*	*	*	*	*				
**H2CON$	Host to Console Message Capability	*	*	*						
HOST$	Update RLP Port-ID Table	*	*							
HVTIP$CTRL	TPUR uses to update and get online status for HVTIP libraries	*	*	*	*	*	*			
ILES$MANAGE	ILES Management Call	*	*							
*INIT$NETWORK	Initialize NIOP data structures	*	*							
IOAID$	Arbitrary Interface Devices	*	*	*						
MCABT$	MCB Abort	*	*							
**MCODE$	Load Microcode (U11 only)	*	*							
**MODPS$	Modify Privileged State	*	*	*	*					
MQF$	Step Control Queue Item Recovery	*	*							
PB$CON	Connect to on-line System	*	*	*	*	*	*	*	*	*
PRMDB$	Enable PROMEGA (U1180)	*								
PRMGA$	Enable PROMEGA (U1180)	*								
QI$CON	Used for MCB to TIP Messaging	*	*							
*REGREP$	Return Contents of UA3-UA5	*	*							
*REGRTN$	Retrieve Contents of UA3-UA5	*	*							
RLP$	Record Lock Processor	*	*	*						
RSI$	RSI Interface	*	*	*						
RT$INT	Initialize Core Compool (CMS)	*	*							
RT$PID	Associate CMS Number to PID	*	*							
RT$PSD	Delete Resident Online Program	*	*							
RT$PSI	Init Resident Online Program	*	*	*	*					
SC$QR	Step Control Short Recovery	*	*							
SC$SR	TIP Session Recovery	*	*							
*SERVER$CTRL	Provides administrative control of the authentication server	*								
*SERVE$	EXEC Monitor Services	*	*							
*SESSION$CTRL	Create and terminate TIP sessions	*	*							
SMU$	Communicate with SMU (U1180)	*								
SUBSYS$DEACT	Subsystem Deactivate Call	*	*							

INTERFACE NAME	*FUNCTION*	*PROFILE*								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
SYSBAL$	Turn SIP On or Off	*	*	*	*					
**TERMRUN$	Dynamic Term of Batch Runs	*	*	*	*					
*TF$KEY	Init, Recover, or Defer TIP	*	*							
TIP$Q	TIP Message Queue Items	*	*							
TIP$SM	Manage a TIP Session	*	*							
TIP$TALK	TIP Termination Communication	*	*							
TIP$XMIT	Step Message Termination	*	*							
TM$SET	TIP Mem Control Init/Release	*	*							
TP$APL	TIP Automatic Recovery Control	*	*							
TPFLG$	Flagbox/Logbox Manipulation	*	*	*	*					
TPLIB$	Access Program Library	*	*							
TPLOG$	Allow TIP Logging	*	*	*	*	*	*			
*TRAPRTN$	Return Control of Trapped ER	*								
TRTIM$	Reset Maximum Time Interrupt	*	*	*	*					
UK$ONS	Core File Access	*	*							
USER$	Reserved for Future Use	*								
VT$CHG	VALTAB/VINDEX Update	*	*							
VT$PUR	VALTAB Load Control Parameters (TPUR/SUPUR Processors)	*	*	*	*	*	*			
WSFP$MANAGE	SS Working Storage file placement	*	*							

Table 3-19. Interface Profile Mapping

The interfaces listed below are required by all TIP users and are not enforced under SIMAN. In the future, we will unsecure these interfaces from SIMAN so they will not appear on the SIMAN screens. All profile runstreams have been updated and these interfaces are no longer listed in these runstreams.

INTERFACE NAME	*FUNCTION*	*PROFILE*								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
CA$ASG	Physical Compool Assign	Required by all TIP users								
CA$REL	Physical Compool Release	Required by all TIP users								
CR$PHS	Physical Compool Read	Required by all TIP users								
CS$PHS	Physical Compool Store	Required by all TIP users								
DM$FAC	DMS Facility Control	Required by all TIP users								
DM$IO	DMS 1100 I/O	Required by all TIP users								
DM$IOW	DMS 1100 I/O Wait	Required by all TIP users								

- *(S104.140.00: CAT II) The SA will ensure Interfaces are enforced or always enforced as stipulated in this STIG.*

- *(S104.440.00: CAT I) The SA will ensure users do not have access to the MODPS$ Executive Interface unless it is authorized for their security profile.*

3.1.8.4 Privileges

The following table is a list of Privileges and their associated profile. The privileges with a * will be enforced under SIMAN and privileges with a ** will always be enforced under SIMAN. Since this section covers multiple releases of the operating system, some of these privileges will not be available on the system. If there is a question check *Table 3-24. Secured Privilege Descriptions~~Table 3-24. Secured Privilege Descriptions~~~~Table 3-24. Secured Privilege Descriptions~~*.

PRIVILEGE FUNCTION	*PRIVILEGE MNEMONIC*	*PROFILE*								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Absolute Device Assignment	**ABSDVASG	*	*	*	*	*	*	*		
Bypass ACR Evaluation	*BYACR	*	*							
Bypass Clearance Level Check	*BYCL	*	*	*						
Bypass Compartment Validation	*BYCOMPMT	*	*	*						
Bypass ER MSCON$ Key Check	**BYMSCNKY	*	*	*	*					
Bypass Ownership Check	**BYOWNER	*	*							
Bypass Private File Check	**BYPRVFLC	*	*	*						
Bypass Read/Write Key Check	**BYRWKEY	*	*	*	*					
Bypass Read/Write Only Mode	**BYRWMODE	*	*	*	*					
Bypass Update of Time Last Ref	**BYTIMUPD	*	*							
Bypass Volume Label Check	**BYVOLCHK	*	*	*						
Common Bank Reload	**CBRELOAD	*	*	*	*					
ER COM$ Privileged Functions	*COM$PRV	*	*							
COMPRTMT Update Functions	*COMPALTR	*								
ER CONFIG$ Update	*CONFIG$	*	*							
Create EXEC Log Entries	*CREEXCLG	*	*							
Security Configured Cbanks	CRESCCB	*								
Security Records for Devices	CRESDEV	*								
Create Userid Security Record	*CRESECRD	*	*	*						
Security Nonconfigured Cbanks	CRESNCCB	*								
Security Records for Programs	CRESPROG	*								
Security Records for Terminals	CRESTERM	*								
Security Records for Volumes	CRESVOL	*								
Change File Backup Information	*DBACK	*	*							
COMPRTMT Decontrol Functions	*DECONTRL	*								
Delete ACRs	*DELACR	*								
Delete Unowned Records	*DELUNOWN	*	*	*						
ER MSCON$ DREG$ Function	**DREG	*	*	*	*					
Extended Acquire Function	**EXTACQUR	*	*	*	*	*	*	*		
FAS Special File Handling	*FASHNDL	*	*							
Unconditional File Delete	**FILDELET	*	*							
Immediate Initiation of Batch	*IMMEDST	*	*							
ER LEVEL$	*LEVEL$	*	*	*						
Modify Attached ACR Assoc	*MODATACR	*	*							
Change Comp Set Within Max Set	*MODCOMP	*	*							
Modify Group Name	*MODGRP	*	*	*						
Modify Group Name Out of Group	*MODGRPOG	*	*	*						
Modify Interface/Privilege Masks	*MODINTPR	*	*	*						

PRIVILEGE FUNCTION	*PRIVILEGE MNEMONIC*	*PROFILE*								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Modify Created ACR Association	*MODOBACR	*	*							
Modify Record Clearance Level	*MODRECCL	*	*	*						
Modify Unowned Records	*MODRECOO	*	*	*						
Modify Run Clearance Level	*MODRUNCL	*	*	*						
Modify Security Records	*MODSECRD	*	*	*						
Modify Special Flags	*MODSPFLG	*	*	*	*					
Modify Sym Clearance Levels	*MODSYMCL	*								
Bypass REELID Conflict Hold	*MOUNTAPE	*	*	*	*	*	*	*		
ER MSCON $DMBT Ret. Functs	**MSCONRET	*	*	*	*	*	*			
Bypass ER MSCON$ Slashing	**MSCONSLA	*	*	*	*					
Read Resident EXEC Areas	*READEXEC	*	*							
Remove File Owner	**REMOWNER	*	*							
Read/Write MCT Application	RWMCT	*								
Read/Write Unloaded File	**RWUNLFL	*	*							
General Access Perm (Bank)	*SETGAP	*	*	*						
Enable/Disable SIP Data 3	SIP3	*	*							
ER SMOQUE Privileged Functs	*SMOQUE	*	*	*	*	*	*	*	*	
Download microcode to device	**SSADHMCODE	*	*							
SSAGNAME	*SSAGNAME	*								
SSANYCALLME	SSANYCALLME	*	*	*						
SSAUTHENICAT	**SSAUTHENICAT	*								
SSBHDR1RDCHK Hdr1/read check	*SSBHDR1RDCHK	*	*							
SSBYOBJREUSE Object Reuse	*SSBYOBJREUSE	*	*							
SSBYXCKMGRTF SYS$*TIF	*SSBYXCKMGRTF	*								
SSCARTLIB Cartridge Library	*SSCARTLIB	*	*							
SSFILECACHE	*SSFILECACHE	*								
SSMASTERACCT	*SSMASTERACCT	*								
SSMHFSACCESS	SSMHFSACCESS	*	*	*	*	*	*	*	*	*
SSMHFSCREATE	SSMHFSCREATE	*	*	*	*	*				
Bypass Media Manager Security	*SSMMGRBYPASS	*								
Mmanager – Read Own Records	*SSMMGRILES1	See *Table 9, Media Manager Privileges and Capabilities*.								
Mmanager – Modify Own Records	*SSMMGRILES2	See *Table 9, Media Manager Privileges and Capabilities*.								
Mmanager – Modify ALL Records	*SSMMGRILES3	See *Table 9, Media Manager Privileges and Capabilities*.								
SSSHAREDCRED	**SSSHAREDCRED	*	*	*	*	*				
SSSHAREDWR	**SSSHAREDWR	*	*	*	*	*	*	*	*	*
SSSSCALLANY	*SSSSCALLANY	*	*	*						
SSSTUBYPASSO	**SSSTUBYPASSO	*	*							

PRIVILEGE FUNCTION	*PRIVILEGE MNEMONIC*	*PROFILE*								
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
SSSWITCHUSER	*SSSWITCHUSER	*								
SSTIPBLD	SSTIPBLD	*								
SSTIPCREDEL	SSTIPCREDEL	*	*	*	*	*	*			
SSTIPUPD	SSTIPUPD	*	*	*	*	*	*			
SSTOKEN	SSTOKEN	*								
SSWRSUBDAC Write/read DAC	*SSWRSUBDAC	*	*							
ER STAB$ Update	**STAB$UPD	*								
Start Run at System High	*STRTZOPT	*	*							
TIP Read Other Input	TIPGET	*	*	*	*					
TIP Send to Other Terminals	TIPSEND	*	*	*	*					

Table 3-20. Privilege Profile Mapping

NOTE: SSTIPBLD, SSTIPCREDEL, and SSTIPUPD are not enforced in the Unisys delivered system. They should be manually enforced and SSO Montgomery has changed them to enforced on systems they support.

- *(S104.140.00: CAT II) The SA will ensure privileges are enforced or always enforced as stipulated in this STIG.*

- *(S104.430.00: CAT II) The SA will ensure users do not have access to security bypass privileges beyond those specified in their security profile.*

- *(S104.460.00 and S104.470.00: CAT II) The SA will ensure users do not have access to STRTZOPT and IMMEDST privileges unless they are authorized for their security profile.*

- *(S104.610.00: CAT II) The SA will ensure for sites using QUIKST (NJZMON), users do not have access to the SSAGNAME privilege unless it is authorized for their security profile.*

- *(S104.450.00: CAT II) The SA will ensure users do not have access to the SSWRSUBDAC privilege unless it is authorized for their security profile.*

3.1.8.5 Media Manager Privileges

Media Manager privileges are unique in the fact that they can be combined to allow certain capabilities with STAR. The table below lists those capabilities provided with standalone and combined privileges. These rules listed after *Table 3-21* below will be applied as specified and cannot be mixed and matched without considering the cumulative effects of the combined privileges. In other words, if the standalone privilege SSMMGRILES3 is authorized for Profiles 2/3/4, one cannot combine that rule with the combination of SSMMGRILES1/2, which is also authorized for Profiles 2/3/4. This is because the combination now gives a privilege combination of SSMMGRILES1/2/3, which is only authorized for select Profile 2 userids and STAR personnel.

CAPABILITY	*ILES1*	*ILES2*	*ILES3*	*ILES1/2*	*ILES1/3*	*ILES2/3*	*ILES1/2/3*
READ OWNED	*	*	*	*	*	*	*
READALL			*	*	*	*	*
MODIFY OWNED	*	*	*		*	*	*
MODIFY ALL						*	*
CREATE					*	*	*
DIRECT I/O							*

Table 3-21. Media Manager Privileges and Capabilities

The following rules apply when assigning Media Manager privileges:

SSMMGRILES1 – Assign to Profiles 5 – 9 as a standalone privilege only. This privilege is assigned in the Profile 5/6/7/8/9 runstreams that are released by SSO Montgomery.

SSMMGRILES2 – Do not assign this privilege as a standalone privilege.

SSMMGRILES3 – Authorized for Profiles 2/3/4 as a standalone privilege. This privilege is assigned in the Profile 2/3/4 runstreams that are released by SSO Montgomery.

SSMMGRILES1/2 – Authorized for Profiles 2/3/4 at the discretion of the site.

SSMMGRILES1/3 – Authorized for Profiles 2/3.

SSMMGRILES2/3 – Authorized for Profile 2.

SSMMGRILES1/2/3 – Authorized for select Profile 2 userids and STAR personnel only.

SSMMGRILES1/2/3 and SSMMGRBYPASS – Authorized for Profile 1 userids, Standard System Batch userids, select STAR personnel, and select Profile 2 userids.

- *(S104.510.00: CAT II) The SA will ensure users do not have access to the standalone SSMMGRILES2 privilege.*
- *(S104.500.00: CAT II) The SA will ensure users do not have access to the standalone SSMMGRILES3 privilege unless it is authorized for their security profile.*
- *(S104.520.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES2 privileges unless this combination is authorized for their security profile.*
- *(S104.530.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*

- *(S104.540.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES2 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*

- *(S104.550.00: CAT II) The SA will ensure users do not have access to SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*

- *(S104.560.00: CAT II) The SA will ensure users do not have access to SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRBYPASS privileges unless this combination is authorized for their security profile.*

- *(S104.490.00: CAT II) The SA will ensure users do not have access to the SSMMGRBYPASS privilege unless it is authorized for their security profile.*

3.1.8.6 Keyin Groups

The following table provides a list of keyin groups and their associated profile:

KEYIN GROUP	***PROFILE***								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
CMBRLD	*	*	*						
COMMUN	*	*	*	*					
DATKEY	*	*	*	*	*	*	*	*	
DEBUGS	*	*							
DEVCNT	*	*	*						
GENSTA	*	*	*	*	*	*	*	*	
LOGGIN	*	*	*	*	*	*	*	*	
MSGREC	*	*	*						
MSTCNT	*	*							
PRFANL	*	*							
RNCNT1	*	*	*						
RNCNT2	*	*	*						
RNCNT3	*	*	*						
RUNSTA	*	*	*	*	*	*	*	*	
SECURI	*	*							
SYMCTL	*	*	*						
TIPGRP	*	*	*	*					

Table 3-22. Keyin Groups and Profiles

NOTE : Profiles 5, 6, and 7 can be granted COMMUN on an as needed basis.

- *(S104.370.00: CAT II) The SA will ensure Users do not have access to CONS keyin groups beyond those specified in their security profile.*

NOTE: Authorized exceptions for SYMCTL, RNCNTL, and TIPGRP will be documented as stipulated in this STIG.

3.1.8.7 Secured Interfaces

Prior to SB5, Interfaces were known as Executive Requests, or ERs. Refer to *Table 11* below for a list of Secured Interfaces and their purposes. The interfaces with a * will be enforced under SIMAN. Those interfaces with a ** will always be enforced under SIMAN.

INTERFACE	***PURPOSE***
ABSAD$	Allows access to main storage by absolute address, downed or active.
AC$NIT	Used by the TIPINIT utility program after a system boot or reboot to initialize user KONS and the VINDEX in storage.
ACCNT$	Allows SIMAN Master userid (under Master account) and designated Administrators to read from and write to the summary account file.
*AP$KEY	Invokes step control application group recovery from a program. This Interface is used with Hot-Standby.
*AT$KEY	Invokes asynchronous audit trail recovery for the specified deferred audit trail. This ER is asynchronous to allow overlapping of step control and audit control recovery processing, thereby expediting Exec recovery of the application.
AUDIT$	Provides interface with audit trail, used by utility programs, common banks.
AUDIT$TRAIL	The AUDIT$TRAIL call interface allows an external interface to write audit trail records from extended mode programs.
**BDSPT$	Bad Spot on Disk – Down Mass Storage Granule.
CA$ASG	Physical Compool Assign.
CA$REL	Physical Compool Release.
CARTTAPELIB$	Allows use of cartridge tape library interfaces.
CMS$REG	See the *Transaction Processing Administration and Operations Reference Manual*. Allows a single copy of CMS 1100 to register by using both COMPOOL and the MCB, or just the MCB or COMPOOL.
CONNECT$TIP	The CONNECT$TIP call interface allows an online batch transaction or demand/batch program to use the services of the TIP system. Shares the same bit setting as PB$CON.
CR$PHS	Physical Compool Read.
CS$PHS	Physical Compool Store.
*DEV$INFO	Returns device-specific information for devices within a device type. The DEV$INFO call interface obtains device-specific characteristics of a device that has been grouped with other devices of similar characteristics. The information returned by DEV$INFO varies by function. Functions of the DEV$INFO interface perform the following tasks: • Read the hardware-id of the device • Read the microcode revision level on the device • Read mode pages from small computer systems interface (SCSI) devices

INTERFACE	*PURPOSE*
DMABT$	Notifies Step Control that DMR processing is to be aborted. Used exclusively with DMS programs.
DM$FAC	TIP file control equivalent to the Interface FACIL$.
DM$IO	TIP file control equivalent to the Interface IO$.
DM$IOW	TIP file control equivalent to the Interface IOW$.
DNLOD$	Down-Line Load/Unload
*DUMP$SUBSYS	The DUMP$SUBSYS call interface enables a subsystem to mark itself to be included in a selective system dump.
ERCVS$	Used only by short recovery utility processors to determine the status of EXEC Step Control recovery.
*ERTRAP$	Register Interface trapping activities.
EX$CRD	EXEC Core Read.
*FCREG$	Register EXEC Files with TIP.
FS$UTF	Allows a user to create, delete, register, de-register, print, access, and update Freespace files. Used by the FREIPS processor.
HOST$	Allows access to RLP port-ID table for the XTC-TIP system. The RLPCON utility uses this to update the port-ID table.
**H2CON$	Provides a host to console message capability.
HVTIP$CTRL	The HVTIP$CTRL call interface is used by the TPUR utility for online HVTIP library maintenance and administration. HVTIP$CTRL provides a superset of the functionality provided by the ER TPLIB$. The TPUR utility calls HVTIP$CTRL to update and report the online state of HVTIP libraries.
*INIT$NETWORK	Used to initialize the structures needed to interface with a Network IOP (NIOP) device. NIOP devices require an absolute device assign in order to send and receive messages. INIT$NETWORK is then used to initialize data structures used to interface with the NIOP device.
ILES$MANAGE	The ILES$MANAGE call interface is used to notify the Exec of changes in the state of an independently linked Executive subsystem (ILES).
IOAID$	Initiates input/output for an arbitrary device.
MCABT$	Used by MCB to notify Step Control that MCB process should be aborted.
**MCODE$	Enable Loading of Micro Code.
**MODPS$	Modify Privileged State. Required to perform a SYSLIB*COMUS.CLOD. This request provides an alternative to the @ASG or @FREE of SYS$*DLOC$ with the proper keys to modify the privileged state of a run. This request sets or clears the privileged bit of cell AY in the requestor's program control table (PCT). Can be used to activate Privileges such as Bypass Private File Check and Bypass Read/Write Key Check.
MQF$	Used exclusively by MCB and DMS to provide recovery and maintenance for Step Control queue items.
PB$CON	Connect to On-line system. Allows a run such as DDPFJT or NJZMON to create a pseudo-Demand terminal.
PRMDB$	Used with the PROMEGA processor.

INTERFACE	*PURPOSE*
PRMGA$	Used with the PROMEGA processor.
QI$CON	Used for MCB to TIP messaging functions
*REGRTN$	If ERTRAP$, return contents of registers UA3/UA4/UA5 to user program.
*REGREP$	If ERTRAP$, retrieve contents of registers UA3, UA4, and UA5.
RLP$	See the *Exec Administration Reference Manual*. An alternate external interface to the record lock processor (RLP) in a Multi-Host (XTC) environment. The RLP is normally accessed by application programs through existing TIP file control interfaces. Use of the ER RLP$ is for privilege users, such as the Site Administrator or system analyst. ER RLP$ is a restricted ER to be used in conjunction with the OS 2200 security complex.
RSI$	Interface with Remote Symbiont Interface (RSI) routines.
RT$INT	Initialize Core Compool. Note that Compool and MCB are mutually exclusive.
RT$PID	EXEC CMS/PID Matrix Setup.
RT$PSD	Purges all copies of a previously initialized resident online program from main storage.
RT$PSI	Initializes resident online program.
SC$QR	Used by the short recovery processor to update Step Control storage during short recovery processing.
SC$SR	Update TIP Session Control data on mass storage after a failure.
*SERVER$CTRL	Provides administrative control of the authentication server.
*SERVE$	Allows MSCP to monitor services provided by the EXEC.
*SESSION$CTRL	Provides the ability to create and terminate open TIP sessions.
SUBSYS$DEACT	The SUBSYS$DEACT call interface provides for the deactivation of a shared subsystem. Deactivation is a prerequisite for a new version of a shared subsystem to be activated and used on a system.
SYSBAL$	Turn SIP on and off from a user program.
**TERMRUN$	Allows a program to dynamically terminate all activities associated with a specific batch run. (ALN: Needed for extended @SMOQ functions. This Interface will also allow a non-exempt @SQ user to access print files created by other users within his or her ALN.)
TF$KEY	Initialize, recover, or defer TIP from a user program. This Interface is used with Hot-Standby and is needed to run CMS1100.
TIP$Q	Used by MCB to create network/passoff/output/checkpoint msg queue items.
TIP$SM	Communicate with TIP session manager to open and/or close a TIP session.
TIP$TALK	Used by CMS1100 to relay messages between terminals and the EXEC.
TIP$XMIT	Notify Step Control of message activity or termination.
TM$SET	*Unused interface that is still marked as secure in the system. It will appear in the SIMAN displays but has no function and will not be granted to any userid other than the master userid.*
TPFLG$	Flagbox/Logbox manipulate.

INTERFACE	*PURPOSE*
TPLIB$	Allows program library activation-deactivation, bank status, and bank update.
TPLOG$	TIP Logging.
TP$APL	Allow a user program to control TIP automatic recovery.
*TRAPRTN$	If ERTRP$, return control to sequence that performed the trapped request.
TRTIM$	Reset maximum time interrupt.
UK$ONS	Core File access via user KONS request.
USER$	Reserved for future use.
VT$CHG	VALTAB/VINDEX update.
VT$PUR	Update VALTAB load control parameters. Needed to execute TPUR/SUPUR.
WSFP$MANAGE	Registers a software subsystem for working set file placement on a specified set of devices or cancels that registration.

Table 3-23. Secured Interface Descriptions

3.1.8.8 Secured Privileges

In this paragraph, the Privileges available under the current EXEC level are explained in further detail. The privileges with a * will be enforced under SIMAN. The privileges with a ** will always be enforced under SIMAN.

3.1.8.8.1 MODPS$ Privileges

Also known as DLOC$ Privileges. These privileges will be documented with an "(M)" next to them. In order for users to access these privileges, they need to have the privilege and assign the file SYS$*DLOC$ the correct keys or they need to have the privilege and the Interface MODPS$, and then perform @SYS$LIB$*COMUS.CLOD,A. Runstreams that use these Privileges will assign SYS$*DLOC$ internally or execute SYSLIB*COMUS.CLOD, A.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
ABSDVASG	**SSADID	Perform Absolute-IO Assignment – Allows a user to assign special I/O devices, printers, and online maintenance of all system peripherals.
BYACR	*SSBAFC	Bypass ACR Evaluation – Allows bypass of ACR evaluation for file access, userid security record access, and subsystem transition. SSBAFC also bypasses @START,/U validation of any ACR attached to a userid. SSBAFC does not allow bypass of the private access list.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
BYCL	*SSBYCL	Bypass Clearance Level Check – Allows bypass of clearance level validation, regardless of userid clearance level range for file access. It is recommended that the site use SSCCL with only the required range instead of SSBYCL.
BYCOMPMT	*SSBYCOMP	Bypass compartment validation within the requestor's user compartment set for file and userid record accesses. Allows any user with this privilege to pass compartment set validation for file and userid, within the user's compartment set. .
BYMSCNKY	**SSDNK	(M) Bypass MSCON$ Key Check – Allows execution of the ER MSCON$ functions without read/write keys. Under normal circumstances, a user can execute only functions 30 through 40 of MSCON$ for files with read/write keys if that user has assigned the files with the correct keys. The SSDNK privilege allows a user to execute these functions without having specified any keys at the time of file assignment.
BYOWNER	**SSBYPASSOWNR	Allows bypass of owner and ACR validations for files, users, and subsystems. Bypasses ownership and ACR validations on file assignment (owned files only), userid records, and subsystem transitions. On systems prior to HMPIX 7.0 to bypass the read-only and write-only validations on owned files, users also need the SSBKUP privilege.
BPRVFLC	**SSBPFC	(M) Bypass Private File Check – Allows bypasses project-id or account number validations. Owned files are not affected by this privilege. The SSBYPASSOWNR privilege permits bypass of ownership.
BYRWKEY	**SSBRWK	(M) Bypass Read/Write Key Check – Allows read and write of unowned files. Allows a user to read and write a file without specifying the file keys. SSBRWK cannot override the private access list for unowned files.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
BYRWMODE	**SSBKUP	(M) Bypass Read/Write Mode – Allows write into read-only files or read of write-only files. For owned files, the SSBYPASSOWNR privilege also is required to bypass read-only and write-only files. For unowned files, no other privilege is required
BYTIMUPD	**SSBYTIMUPDAT	(M) Bypass Update of Time Last Referenced – Allows bypass of recording of file reference. SSBYTIMUPDAT allows a user to bypass updating the time of last reference for cataloged file assignment.
BYVOLCHK	**SSBVOLCHK	(M) Bypass Volume Labeling – Allows bypass of volume labeling. At TVSL = 3, SSBVOLCHK allows a user to assign any tape if the user is also security privileged system-high.
CBRELOAD	**SSRLODCB	(M) Common Bank Reload – Allows a user to perform a BANK$ Interface to cause the reload of a common bank.
COM$PRV	*SSCONSOLE	COM$ Privileged Functions – Allows execution of ER KEYIN$ and privileged ER COM$ functions. It also allows ER COM$ with routing information to be sent to remote consoles with specification of run-ids for logging of console messages.
COMPALTR	*SSASCDT	Allows for compartment set creation and changes. Allows execution of all the ER SCDTA$ functions except the decontrol function. On SSO Montgomery released operating systems, a user needs to have this Privilege in order to execute a VALCHG and VALBLD functions of the VTBUTL processor. Site Technical Support personnel with Profile 2 userids are authorized to have this privilege. Other than the exception above, this privilege has no meaning on a system below SECOPT2 and it will never be given to anyone but the security officer/master userid.
CONFIG$	*SSCONFIGMGR	Allow Write of Hardware/Software Configuration – Allows write access to those parameters defining the hardware or software configuration via the CONFIG$ Interface. This Privilege is needed to run LIBLOAD/LIBSAVE and accomplish SOLAR installations.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
CREEXCLG	*SSLOGER	Create EXEC Log Entries – Allows a user to use ER SYSLOG$ to create log entries in the Unisys software products log range.
CRESCCB	SSCSCCB	Unused privilege reserved for use by Unisys.
CRESDEV	SSCSD	Unused privilege reserved for use by Unisys.
CRESECRD	*SSCSU	Unused privilege reserved for use by Unisys.
CRESNCCB	SSCSNCCB	Unused privilege reserved for use by Unisys.
CRESPROG	SSCSP	Unused privilege reserved for use by Unisys.
CRESTERM	SSCST	Unused privilege reserved for use by Unisys.
CRESVOL	SSCSV	Unused privilege reserved for use by Unisys.
DBACK	*SSDBACK	Allows user to change backup info in the MFD entry, including last backup date/time, backup tape reel #s, and removal of backup tape reel #s.
DECONTRL	*SSDECONTROL	Allows compartments to be removed from the system set. Files with these compartments are no longer protected by that compartment. Allows any user with this privilege to execute the decontrol function of ER SCDTA$. Has no meaning on systems below SECOPT2. This privilege should never be given to anyone but the security offices/master userid. .
DELACR	*SSDACR	Delete ACRs – Allows deletion of unowned ACRs. Deletion of unowned ACRs is allowed, except where the Delete access of the ACR restricts the user attempting to perform the delete. Do not give this Privilege to any functional user.
DELUNOWN	*SSDELRECNOOW	Delete Unowned Records – Allows unowned record deletion. A user can delete a record that does not have an owner. User must have the correct MAC and DAC or possess bypass privileges to make this change.
DREG	**SSDRG	(M) Performs DREG$ Function of MSCON$. SSDRG allows a user to execute the DREG$ function of ER MSCON$, and thus change the project-id and account number of the file. This change affects only the security of unowned files, because project-id and account number protection for owned files occurs with ACRs.
EXTACQUR	**SSPLACE	(M) Extended Acquire Function – Allows an EACQ$ function via the IO$ or IOW$ Interface and a FC$SSN request with the AQ function.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
FASHNDL	*SSFASSPHNDL	FAS Special File Handling – Allows FAS to restore a file when the owner of the file or the ACR does not exist on the system. FAS makes the file private to the userid of the FAS run. The security officer then should attach the correct security information to the file. Without this privilege, FAS reports an error message and does not restore the file. Do not run with this privilege as standard practice. It should be used only when the user is running at system-high (clearance level = 63 and compartment set = ALL).
FILDELET	**SSFDELE	(M) Allows unconditional unowned file deletion. SSFDELE allows a user to unconditionally delete an unowned, cataloged file. This overrides all other security constraints, including the delete attribute of ACRs attached to unowned files.
IMMEDST	*SSRUNXOPT	Allows use of the X option on started runs. Allows @START,/X or ST,/X so runs execute immediately. With this privilege, a user can specify this option on a batch @RUN card. This causes the batch run to start immediately, regardless of system holds or Batch limit.
LEVEL$	*SSLEVEL	Allows execution of privileged ER LEVEL$ functions. SSLEVEL allows a user to execute an ER LEVEL$, with the format (type-indicator, relative level).
MODATACR	*SSCHACR	Modify created ACR association. Allows modification of attached ACRs to unowned files. SSCHACR allows a user to change or remove the attached ACR association specified in an unowned file record.
MODCOMP	*SSCHCOMP	Change compartment set within the user's compartment set on files and userid records. Allows any userid with this privilege to change the compartment set associated with a file or to change a user compartment set. The change must be a subset of the caller's user compartment set. Users also need this privilege to change the "All compartment" designation in userid and file security records, as well as the SSCPF privilege, and the "ALL" capability.
MODGRP	*SSCGNM	Unused privilege reserved for use by Unisys.

SIMAN KEYWORD	***EXEC KEYWORD***	***DEFINITION***
MODGRPOG	*SSCGNMB	Unused privilege reserved for use by Unisys.
MODINTPR	*SSCPRERM	Modify ER/Privilege Mask – Allows modification of privilege and ER mask. The ERs/privileges modified must be in the requesters security record.
MODOBACR	*SSCHCACR	Definition prior to HMP IX 7.0. Allows to-be-attached ACR modification on unowned userid records. The SSCHCACR privilege allows a user to change or remove a to-be-attached ACR association in an unowned userid security record. Definition from HMP IX 7.0 and above. Allow To Be Attached ACR Association Modification. Allows a user to change or remove the Attached ACR association in a userid record.
MODRECCL	*SSCRCL	Modify Record Clearance Level – Allows clearance level change of a user or file. SSCRCL allows a user to modify the clearance level range defined for a user and the clearance level of a file. The new clearance level values must lie within the clearance level range of the user doing the modification unless the user also possesses the privilege to bypass clearance level validation (SSBYCL). If the user has both SSCRCL and SSBYCL, any clearance level change is allowed.
MODRECOO	*SSMROOC	Allows change of owners in userid and file security records: Allows a user to transfer ownership of userid security records and files, to a user whose attributes are not a subset of the attributes of the current owner, or to a user whose attributes are not a superset of the object. MAC and DAC are overridden by this privilege.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
MODRUNCL	*SSCCL	Modify Run Clearance Level – Allows bypass of clearance level validation and allows change within the users range. Allows bypass of the clearance level validation within the users clearance level range. Note that SSCCL does not bypass clearance level validation for subsystem transition. SSCCL allows a user to do an @LEV control statement to modify the executing clearance level, within the userid range. See: Specifying the Privilege to Change Run Clearance Levels (@LEV,@@LEV). Runs in a subsystem can use the @LEV control statement to modify the executing clearance level of the caller home subsystem, however, the clearance level range of the subsystem is used for evaluation. If the clearance level change passes, the clearance level change is made in the user's home system and not in the executing subsystem. Files created after an @LEV is performed are given the new clearance level value of the @LEV statement.
MODSECRD	*SSCHDR	Modify Security Records – Allows modification of unowned userid security records. SSCHDR allows a user to modify an unowned userid security record.
MODSPFLG	*SSCSPF	Modify Special Flags – Allows modification of special flags. A user with the SSCSPF privilege may set or clear any flag bit present in the special flags field of the user security record or file record. ***NOTE:*** The All Compartment designation change requires SSCHCOMP in addition to SSCSPF.
MODSYMCL	*SSSCLDTUPD	Allows change of the symbolic representation of the clearance level in the security database.
MOUNTAPE	*SSNOUNIQREEL	Allows use of B option on a tape assign. The B option sends a LOAD message for the specified reel-ID even if the reel is currently mounted.

SIMAN KEYWORD	***EXEC KEYWORD***	***DEFINITION***
MSCONRET	**SSDMBT	(M) DMBT$ and DMBTS$ Functions of MSCON$ - Allows retrieval of Master Bit Tables for DMBT$/DMBTS$ mass storage functions of MSCON$.
MSCONSLA	**SSLASH	(M) Bypass MFD$$ Slashing – Allows a user to obtain a complete copy of MFD items (including read/write keys, projects, and account numbers) using ER MSCON$.
READEXEC	*SSREADEXEC	Read Resident EXEC Areas. SSREADEXEC allows ER CONFIG$ reads through the EXEC_RELATIVE_ADDRESS configuration parameter, thus giving access to highly sensitive data. SSREADEXEC also allows access to call interfaces that retrieve information about runs and files. Specifically, Exec callers are allowed to retrieve information about all runs (INSP$RUNS), information specific to a run (INSP$RUNID), file information specific to a common name section (INSP$FILES), and information specific to a given logical device address table (LDAT) index and directory index (INSP$LDAT).
REMOWNER	**SSREMFILOWNR	Allows the user to remove the owner from a file, marking it unowned.
RWMCT	SSMCT	Unused privilege reserved for use by Unisys.
RWUNLFL	**SSBROD	(M) Allows bypass of rolled-out check. SSBROD possession at the time a rolled-out file is assigned prevents the file from being rolled in, but sets the file as read and write enabled.
SETGAP	*SSGAP	Allows extended mode level-1 banks to be created with GAP set to read. SSGAP also allows level 0 and 1 public gates to be created in extended mode. SSGAP is not meaningful for Security Level 3 common bank subsystems.
SIP3	SSSIP3	Unused privilege reserved for use by Unisys.
SMOQUE	*SSSMOQUE	SMOQUE$ Interface Privileged Functions – Allows execution of privileged ER SMOQUE$ functions. SSSMOQUE allows users to execute the change entry function and use all the restricted mode bits on an ER SMOQUE$ request. This privilege allows all queued print files to be accessed or deleted, regardless of security level.

SIMAN KEYWORD	***EXEC KEYWORD***	***DEFINITION***
SSADHMCODE	**SSADHMOCDE	Allows users to download microcode to a device via ER IOAID$.
SSAGNAME	*SSAGNAME	Allows reading of the application group name (which is considered a secured entity) by the STEP_CONTROL_APP_IDENTITY function of ER$ CONFIG$.
SSANYCALLME	SSANYCALLME	Ensures that trusted privilege validation is satisfied so that a subsystem can be called, regardless of the trusted privileges a calling subsystem may have. This privilege only has meaning for called subsystems. Its use ensures that a subsystem does not have to be assigned trusted privileges it does not need in order to be called.
SSAUTHENICAT	*SSAUTHENICAT	Allows the caller to use the following authentication CALL interfaces: SERVER$CTRL, SERVER$GET and SERVER$PUT. (First used HMP 3.0 or SB 7.0)
SSBHDR1RDCHK	*SSBHDR1RDCHK	This privilege must exist to use the SSBYOBJREUSE privilege. See the description of the SSBYOBJREUSE privilege.
SSBYOBJREUSE	*SSBYOBJREUSE	The ER IO$ and ER IOW$ locate block (LBLK$) function treats EOF marks on a tape as just another block, thus allowing the user to access beyond the software EOT and possibly gain access to data with different security attributes. This privilege allows access to areas that have not been cleared. Use of this privilege requires use of the SSBHDR1RDCHK privilege (bypass_tape_hdr1_read_ checks) which is not security relevant.
SSBYXCKMGRTF	*SSBYXCKMGRTF	Allows bypass of Exec security check to update the Media Manager ILES Tape Inventory File (TIF) (SYS$*TIF). The Media Manager still enforces who can update individual TIF records.
SSCARTLIB	*SSCARTLIB	Allows use of cartridge tape library interfaces.
SSFILECACHE	*SSFILECACHE	(M) Allows a change in the XPC caching mode of a file.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
	SSMASTERACCT	The master account privilege allows all accounting maintenance without the need to run under the Master Account. This privilege is required by administrators who must update account information for userids. (Introduced in HMP IX 7.0) SSO Montgomery has made this always enforced on systems they support.
SSMHFSACCESS	SSMHFSACCESS	Allows a userid to assign shared files. This privilege, together with the SSMHFSCREATE privilege, allows sites to control which userids have access to shared mass storage. Both SSMHFSACCESS and SSMHFSCREATE should be enforced at the same time. When not enforced, all users can access shared files. When they are enforced, a userid attempting to create, delete, or assign a shared file without the appropriate privilege will receive an error. Enforcing SSMHFSACCESS and not enforcing SSMHFSCREATE will not prevent shared file assignment. Also, enforcement of the privileges on one host does not enforce the privileges on the other hosts. Both privileges must be enforced on each host separately. Sites that do not use Quota can use SSMHFSCREATE to control shared file creation and deletion. SSMHFSACCESS can control the ability to assign shared files, regardless of whether or not Quota is used. (Introduced in HMP IX 6.0)
SSMHFSCREATE	SSMHFSCREATE	Allows shared file creation and deletion. This privilege, together with the SSMHFSACCESS privilege, allows sites to control which userids have access to shared mass storage. See the description of the SSMHFSACCESS privilege for details. (Introduced in HMP IX 6.0)

SIMAN KEYWORD	***EXEC KEYWORD***	***DEFINITION***
SSMMGRBYPASS	*SSMMGRBYPASS	Allows bypassing of the Media Manager in accordance with the Media Manager ILES BYPASS configuration parameter described in the vendors tape management system documentation. For STAR, this is 1800 enforcement.
SSMMGRILES1	*SSMMGRILES1	TIF Records can be read by their owners. Selected fields can be written. See also 3.1.8.5 Media Manager Privileges for combinations.
SSMMGRILES2	*SSMMGRILES2	TIF Records can be read and written by their owners. . See also 3.1.8.5 Media Manager Privileges for combinations.
SSMMGRILES3	*SSMMGRILES3	All TIF records can be read. Selected fields can be written. See also 3.1.8.5 Media Manager Privileges for combinations.
	SSSHAREDCRED	When this privilege is enforced, the caller must have this privilege to catalog or delete a shared TIP file. When unenforced, the system acts as if everyone has the privilege. (Introduced in HMP IX 7.0)
	SSSHAREDWR	When this privilege is enforced, the caller must have this privilege to have read/write access to shared TIP files. When unenforced, the system acts as if everyone has the privilege. (Introduced in HMP IX 7.0)
SSSSCALLANY	*SSSSCALLANY	Allows a subsystem transition to occur when the calling subsystems security attributes are not a subset of the target systems security attributes. Bypasses both mandatory and discretionary attributes.

SIMAN KEYWORD	***EXEC KEYWORD***	***DEFINITION***
SSTUBYPASSO	**SSSTUBYPASSO	Allows @START,/U or ST,U keyin of a start file not owned by the target userid. For ST,/U keyins from the physical operator console (not via @@CONS ST,/U), this privilege also allows bypass of the requirement that the userid on the ST,U keyin must have execute access to the @START file. If a default TIP userid is configured by the tip_security_userid, that userid can be given the SSSTUBYPASSO privilege just like any other userid. The SSSTUBYPASSO privilege is visible in the file SYS$*SEC@USERID$ and via ERs STAB$, SREG$, SUMOD$ and SPRNT$. (Introduced in HMP IX 6.0)
	*SSSWITCHUSER	Userids need this to switch to the security attributes of a different userid using CALL SEC$SWITCH$. Not required to switch back to the home userid. Currently used only by system software. The userid that has this privilege can switch to the security attributes of any other userid. (Introduced in HMP IX 7.0) SSO Montgomery has made this always enforced on systems they support.
	SSTIPBLD	If enforced, SSTIPBLD is required to use both the VALBLD and VALINT functions of the TIP VALTAB utility (VTBUTL) except when VALINT is used to display VALTAB entries (no output field is present). This protection is provided by VTBUTL itself, not by the Exec. If SSTIPBLD is enforced, it is also required to perform the ER VT$PUR purge and drain transaction system functions. (Introduced in HMP IX 7.0) SSO Montgomery has made this enforced on systems they support.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
	SSTIPCREDEL	If enforced, SSTIPCREDEL is required to perform functions of the TIP utilities (VTBUTL, SUPUR and TPUR) that create or delete TIP resources such as SUPUR files and HVTIP libraries. This protection is provided by these utilities, not by the Exec. If enforced, it also is required to use the VALBLD and VALINT functions of the TIP VALTAB utility (VTBUTL) except when VALINT is used to display VALTAB entries (no output field is present). (Introduced in HMP IX 7.0) SSO Montgomery has made this enforced on systems they support.
	SSTIPUPD	If enforced, SSTIPUPD is required to perform functions of the TIP utilities (VTBUTL, SUPUR and TPUR) that update TIP resources such as the VALTAB file, SUPUR files and HVTIP libraries. This protection is provided by these utilities, not by the Exec. (Introduced in HMP IX 7.0) SSO Montgomery has made this enforced on systems they support.
SSTOKEN	SSTOKEN	Allows an ER RSI$ or ER TIP$SM driver program to pass a sign-on information buffer. (First used in HMP 3.0 or SB 7.0)
SSWRSUBDAC	*SSWRSUBDAC	Allows a subsystem generating an interactivity contingency to bypass private access checking and write to a subsystem owned by a different userid. If a subsystem must bypass the private access check, this privilege is preferred over the more global SSBYPASSOWNR privilege.
STAB$UPD	**SSTABCH	STAB$ Update – Allows users to change enforcement of ERs and privileges. SSTABCH allows a user to execute the change function of ER STAB$. Read functions of ER STAB$ require no privilege.

SIMAN KEYWORD	*EXEC KEYWORD*	*DEFINITION*
STRTZOPT	*SSSTRTZOPT	Allows execution of @START,/Z by a user who has execute access to the file containing the started runstream and who also has system-high capability. SSSTRTZOPT also allows users to start other users runstreams via the remote ST keyin when the starters userid is different than the userid specified with the keyin. In the case of @START,/UZ, the userid being started must also have system-high capability. ST,/Z keyin requires no privileges, except that the userid being started must have system-high capability.
TIPGET	SSTIPGETMSG	Allows a user to read queued TIP message by using ER QI$CON, within the limits of the user's mandatory attributes. ***NOTE:*** On a Security Level 2 or higher system using TIP message security this privilege should be enforced. A runstream is provided that enforces this privilege. Only has effect on SECOPT2 and above systems.
TIPSEND	SSTIPSENDMSG	Allows a user to send TIP messages to other terminals. ***NOTE:*** On a Security Level 2 or higher system using TIP message security this privilege should be enforced. A runstream is provided that enforces this privilege. Only has effect on SECOPT2 and above systems.

Table 3-24. Secured Privilege Descriptions

3.1.8.9 Special Security Profiles

Over time, the SSO has realized that certain jobs within the sites and at the remote sites do not fall cleanly into any of the existing standard security profiles. For this reason, the following special profile runstreams have been added to the JX$$0000*00 file to make the site IAOs job easier. These special profiles are explained below.

PROFILE TITLE	*ELEMENT NAME*	*PROFILE DESCRIPTION*
Subadministrator	PROFILE/SUB	Modified Profile 3. Intended for configuring IAO with subadministor privileges userids.
STAR/Tape Mgt Personnel	PROFILE/TAPE	Modified Profile 3 with all MMGR Privileges.
System Standard Batch Userid	PROFILE/OPS	Modified Profile 2 with all MMGR and other special privileges.
High Level Tech Support Analysts	PROFILE/TECH	Modified PROFILE/OPS that excludes certain controlled Privileges.
Performance Monitor; Senior System Software Analyst	PROFILE/PERFORM	Modified Profile 2 with extra Interfaces and Privileges to be able to monitor system performance.
High-level CDA profile for DNMC domains	PROFILE/DNMC	Modified Profile 5 with RNCNT1 and SYMCTL keyin groups.

Table 3-25. Special Security Profiles

3.1.8.10 Examples of Profiles

The following are examples of what job in the DOD community matches up with each of the standard security profiles described earlier in this section. Names that appear in quotes, such as DPS, mean that there is a userid in SIMAN on each system by that exact name. The other examples are in the form of a job title or description. Examples have been drawn from different sources; so do not expect to be familiar with all of them.

Profile 1: All site IAOs and review team. Security software developer/programmer/quality assurance evaluators on a dedicated CDA domain.
"INSTALLATION" *
"EXEC8" *
**NOTE*: These userids will not have a TSS$ record.

Profile 2: Senior DBM/DBAs and Systems Analysts. Senior systems software programmers, developers, and quality assurance evaluators staff on a CDA domain.
Standard System Batch userid is a modified Profile 2.
Performance analyst is a modified Profile 2.
Operations personnel, if needed.
UOSS

Profile 3: Junior DBMs/DBAs, Senior AIS Monitors, and BLISS Userids. Junior systems software programmers, developers, quality assurance evaluators on a dedicated CDA domain. STAR/Tape Management personnel are a modified Profile 3. IAO with subadministrator privileges is a modified Profile 3.
xxJSTM
xxJF00
QUIKST
VTHSRV

Profile 4: Junior AIS Monitors. Senior AIS programmers on a dedicated CDA domain.

Profile 5: Top-level customer DBAs, CAMS Host DBM, and Supply RPS userids. Junior AIS programmers and Quality Assurance DBA Test userids on a dedicated CDA domain.
DPS, DDP, and IPF userids
DPSSYS
xxEZ00

Profile 6: High-level End Users. AIS Managers and Application Developers of TIP/DMS Systems on a shared Production/CDA domain. CDA/Quality Assurance TIP/DMS AIS Manager Test userids.

Profile 7: High-level End Users. AIS Managers and Application Developers of Batch and Demand Systems on a shared Production/CDA domain. CDA/Quality Assurance Demand and Batch AIS Manager Test userids.

Profile 8: Generic Functional Users with Demand Access. CDA/Quality Assurance Generic Demand Test userids.
CATS
SSC-SSQM
GAJT00

Profile 9: Generic Users with TIP and Batch access only. CDA/Quality Assurance Generic TIP and Batch Test userids.

3.1.8.11 Unisys User Profile Distribution Guidelines

The site IAOs will use the following user profile distribution guidelines on production systems under their control. On dedicated CDA (development and test) systems, the profile distribution guidelines listed below may not apply. On these systems, the concept of least privilege is more appropriate and the IAO will ensure all requirements are clearly documented in the individual's SAAR.

Profile 1: Profile 1 userids will be assigned to SIMAN Administrators and review team administrators only. No other site Profile 1 userids are allowed. There may be two pre-positioned Profile 1 userids with SIMAN administration capabilities for remote troubleshooting of security related problems by FAB and SSO personnel. There may also be three pre-positioned Profile 1 userids (non-SIMAN administrators) for review team members. All pre-positioned userids will be disabled when not in use.
All Profile 1 users will be IT-I cleared.

Profile 2: There may be 15 userids per system across all shifts, plus one userid per operator, if assigned.
All Profile 2 users will be IT-I cleared.

PROFILE 3 – 9 DOD users will be IT-II CLEARED.

Profile 3: There may be one userid for each site person actively administering the system. In practice, Profile 3 and 4 userids will be assigned to all remaining site personnel not assigned Profile 1 or 2 userids.

PROFILE 4-9 NON-DOD users will be IT-II or IT-III CLEARED.

Profile 4: If your site is performing software development on a dedicated CDA domain (IAW STIG guidelines outlined in *Section 13, Software Development*, each application developer will have a Profile 4 userid. A Profile 4 userid rather than a Profile 3 userid may also be assigned to site junior AIS monitors depending on the job being performed.

Profile 5: On ALN, DNMC, and DFAS-IN (Indianapolis) systems, refer to *Table 3-26, Guidelines for Percentage of Active Userids*, for active userid profile percentage guidelines.

Profile 6: On ALN, DNMC, and DFAS-IN (Indianapolis) systems refer to *Table 3-26, Guidelines for Percentage of Active Userids*, for user profile percentage guidelines.

Profile 7: On ALN, DNMC, and DFAS-IN (Indianapolis) systems refer to *Table 3-26, Guidelines for Percentage of Active Userids*, for user profile percentage guidelines.

Profile 8: A Profile 8 userid is granted access to Demand, TIP, and Batch run modes. If there is no TIP workload whatsoever virtually all non-site userids may fall into this category. On ALN, DNMC, and DFAS-IN (Indianapolis) systems, refer to *Table 3-26, Guidelines for Percentage of Active Userids*, for user profile percentage guidelines. On DNMC systems, because of the non-standard implementation of TIP session control, virtually all non-site userids fall into this category because they need to have Demand access. In order to assign a Profile 8 userid, the requirement for Demand mode access will be verified.

Profile 9: A Profile 9 userid is granted access to TIP and Batch run modes. On ALN, DNMC, and DFAS-IN (Indianapolis) systems, refer to *Table 3-26, Guidelines for Percentage of Active Userids*, for user profile percentage guidelines. Profile 9 userids will not be granted access to Demand mode.

<table>
<tr><th>USER PROFILES</th><th>DNMC & ARMY SYSTEMS PERCENTAGE OF ACTIVE USERS</th><th>DFAS-IN (INDIANAPOLIS) SYSTEMS PERCENTAGE OF ACTIVE USERS</th><th>ALN SYSTEMS PERCENTAGE OF ACTIVE USERS</th></tr>
<tr><td>5
6
7</td><td>35 % Flexible total of Profiles 5,6,7</td><td>20 % Flexible total of Profiles 5,6,7</td><td>16 % Flexible total of Profiles 5,6,7</td></tr>
<tr><td>8</td><td rowspan="2">60 % Flexible total of Profiles 8 and 9</td><td>60 % of active userids</td><td>40 % of active userids</td></tr>
<tr><td>9</td><td>15 % of active userids</td><td>40 % of active userids</td></tr>
</table>

Table 3-26. Guidelines for Percentage of Active Userids

3.1.8.12 Determining a User's Profile

The process of determining the proper security profile for a user can be difficult, and it requires judgment on the part of the IAO. An experienced IAO will understand which requests for deviation from these guidelines involve critical areas and which are less serious. The most critical rule to remember is that Profiles 1 and 2 userids are always reserved for personnel within the site and review team members. Profile 3 userids are reserved for site personnel. An exception is the IAO with subadministrator privileges position that requires a higher level of privilege in order to perform userid maintenance duties. Normally, not even the highest functional users need a security profile higher than 5, and the vast majority of functional users can perform their duties with a security Profile 8 or 9 userid. A functional user is a person whose job is tied to one or more of the application areas, such as Maintenance, Supply, Accounting & Finance, etc.

3.1.8.12.1 General Procedure for All IAOs

The steps in this section will provide a general procedure for determining a user's security profile. If you need further assistance, contact the FAB and ask for the Systems Support Office to help resolve a question. In summary, always remember that the userid profile structure is like a pyramid with many, many Profile 8 and 9 users at the base and successively fewer Profile 7, 6, 5, 4, 3, 2 and 1 userids as you move up the pyramid. You can find out how many userids of each profile are present on your system by running the Montgomery Profiler runstream (RJXD50) or the SRR Toolkit software. Both are documented in the USIT Software User Manual (SUM).

a. Using the examples in this section and a description from the user about his/her job, determine which profile best fits. Remember, do not give any functional user a Profile 1, 2, or 3 userid since these are reserved for systems personnel within the site, the IAOs with subadministrator privileges, and review team members. There are very few people in the functional user community that require access to a Profile 4 or 5 userid. If the person is a functional user and the matching profile is a 4 or 5, contact the user's supervisor to verify the job description.

b. If a user falls under two job categories with two different security profiles, that user will need the more powerful of the two profiles. Since there are only nine general security profiles and many types of jobs within the DOD user community, it sometimes happens that a user cannot perform all of his/her legitimate duties under the security profile initially assigned to them. In this case, the best approach is to require the user to identify exactly what action is required by their job but prevented by their current security profile. The user will put the request in writing and have their supervisor approve it before sending it to the Security Officer. (If e-mail is used, the user will forward the request to his or her supervisor who then forwards it to the Security Officer.) This approach helps to prevent users from pressuring the IAO to increase their profile without having a clear justification.

c. Evaluate the action that the user wants to perform. Is it an appropriate action for that type of user? If the person is not a site user, would the Privileges being requested allow that user to access areas for which they are not authorized? If the action seems unusual, verify the need to perform it with the person's supervisor. If the action to be performed is appropriate to that user, the next step is to determine what Interface, Privilege, CONS level, CONS keyin, or other userid characteristic (or combination of factors) is preventing the user from performing the action in question.

d. Find the lowest level security profile that includes the required userid characteristics. Evaluate whether it is preferable to upgrade the existing userid to the higher security profile or simply add the additional Interfaces, Privileges, etc., to the existing userid. The underlying concept here is to give a person the least powerful userid that will accomplish the required duties. The security profiles, in part, serve to prevent the IAO from having to customize every userid on the system. If the required userid characteristics are included in the next more powerful security profile than the current one, it usually makes more sense to upgrade the userid to the higher profile using the profile runstreams in the JX$$0000*00 file. This will occur when the upgrade is from a Profile 8 to a 7, or from a

6 to a 5, and so forth. However, if you would have to upgrade the userid's security profile more than a single level to include the required characteristics, you need to seriously consider manually adding only the required characteristics to the userid as an alternative. You will also be very careful when adding characteristics from security Profiles 1, 2, or 3 to a lower level userid. An example follows:

A high level functional user with a Profile 6 userid needs the capability to move and/or delete print files created by other users within his or her AIS. In order to be able to do this with the print viewing utility (@SQ, @SMOQ, etc.) the userid requires the TERMRUN$ Interface, which is normally included with Profiles 1, 2, 3, and 4 userids only. In this case, it makes much more sense to add the TERMRUN$ Interface to the existing userid than to upgrade that userid to a full Profile 4. Remember minor exceptions to standard profiles can be documented on the individual's SAAR. However, Interfaces such as TERMRUN$ will be documented on a justification letter. The IAO will maintain a copy of the justification letter.

3.1.8.12.2 Resolving Profile Conflicts

Assigning a security profile to a high level functional user or a user that outranks the IAO can be especially difficult. Often a user will feel that if they are assigned a userid with less than top level Privileges that it is a sign that the Security Officer considers them as less than trustworthy. This is not the case of course, but the Security Officer will sometimes be pressured by a user (or by management) to grant Privileges above what is outlined in the guidelines of this manual. If you receive this pressure from a person outside your chain of command, notify your site management. If you are directed by your local management to deviate from these guidelines in a way that you believe seriously affects the security of a system you are responsible for, do two things. First, write a memo for record (MFR) documenting the deviation from the STIG, and coordinate the MFR through your chain of command. The manager who ordered you to make the change should sign the MFR. Keep a copy of this coordinated document in a safe place.

3.2 Account Controls

All services use standard accounts to group users and to generate input to fee-for-service software. The format for the account names is different for each service, however. Refer to the service-specific appendices for more information.

- *(A101.040.00: CAT IV) For DISA sites, the IAO will ensure there is a documented standard account format for the system.*

- *(S104.180.00: CAT III) For DISA sites, the IAO will ensure the account standard will be followed.*

3.2.1 Account Restrictions

Application users will not be able to enter an account at sign-on time. This reduces the risk that they could gain access to an account that they are not registered under. This is especially

important in a fee-for-service environment. If a user has a valid requirement for access to more than five accounts, they will need to submit their request to the site IAO for approval. Adequate justification will be provided. Once the IAO has approved the request, the user will be allowed to enter an account. Access to ALN exempt accounts, even in this situation, will normally not be approved by the IAO.

- *(S104.350.00: CAT III) The SA will ensure functional users who require access to less than five accounts do not have the ability to enter an account at sign on time.*

- *(S104.354.00: CAT III) The IAO will ensure functional users with a valid requirement to enter more than five accounts will document this requirement in accordance with this STIG guidelines.*

For ALN:

- *(S104.320.00: CAT II) The SA will ensure non-exempt users, except where documented, does not have an exempt account in their userid record.*

3.2.2 Denying Access to Unauthorized Accounts

If the account restrictions outlined above are followed for every application userid on a system, the risk that a user will gain access to an account that he or she is not authorized to access is greatly reduced. In rare cases where users require access to more than five accounts, it is acceptable to set the Account May Be User Entered flag once the request has been approved by the IAO. There are two additional steps you need to take to reduce the risk of users accessing unauthorized accounts even further. The first step is that every time a user is issued a new userid, the accounts that the userid has access to will be verified by the IAO. This will prevent userids from having access to unauthorized accounts when the userid is reassigned. The second step is to configure your SMART Console AMS database to automatically answer the "A, E, R" console messages that are generated when a user tries to use an account to which that user does not have access. The AMS database will be set up to answer this type of message with an R, which will cause the attempt of that user to access that account to be rejected. Contact your local administrator for SMART Console to ensure that these messages are being answered automatically with an R. The sites supporting DNMC Unisys workload are exempt from the second step because the standard DNMC Unisys environment prevents the "A, E, R" message from being generated. As the DNMC environment changes, however, it will be important to reevaluate this requirement.

- *(S103.130.00: CAT II) The IAO will ensure AER account-related console messages are answered correctly.*

3.2.3 Master Account/SSMASTERACCT Privilege

There is a local code change that allows all security administrators under the Master Account to perform account maintenance. For this reason, only security administrators are authorized to be under the Master account.

In HMP IX 7.0, the privilege SSMASTERACCT allows a user to perform all account related maintenance functions without the need to be under the Master Account. Only security administrators will be granted this privilege.

- *(S103.480.00: CAT II) The SA will ensure only the Master userid and security administrators has access to the Master account* or the SSMASTERACCT privilege.

3.2.4 PRIVAC Account

The Privileged tape labeling account allows users with access to this account to label, unlabel, and access tapes not owned by them. The actual name of this account is GEN tag dependent. Non-site users will not have access to the PRIVAC account. Access to this account by site users will be restricted. If access to a site user is granted, it will be justified and documented on the user's SAAR. The system standard batch userid, which is used to start the LABELRUN job, is authorized to have access to this account.

- *(S104.190.00: CAT II) The SA will ensure non-site users does not have access to the PRIVAC account. Access to the PRIVAC account by site users are restricted and access is documented on the site user's SAAR.*

3.3 Project-ID Controls

3.3.1 Overview

Each time a user signs onto a Unisys mainframe, they are assigned a project-ID. This project-ID is assigned to them by the Security Officer when he or she creates the SIMAN record for that userid or defaults to QQQ$ if none is specified for the user. Most users will have a single project-ID, but some will have access to multiple project-IDs. When a user creates, assigns, or refers to a filename.elementname without specifying a Qualifier for that file, the system uses the project-ID that user is signed on under as the default qualifier name for the file. Project-ID formats are service-specific, so please refer to *Appendix C, Access and Location Number Information,* for more information.

3.3.2 Project-ID Controls in the ALN Environment

Please note that project-IDs have critical significance in the ALN environment, so IAOs using that environment are highly encouraged to familiarize themselves with the rules outlined in *Appendix C, Access and Location Number Information*. Specifically, application users in an ALN environment will be restricted to a list of project-IDs. In addition, they will not be allowed to enter a project-ID. This prevents a user from starting a batch run with an exempt project-ID (and making the batch run exempt) or entering an exempt project-ID at sign on time. If a user has a valid requirement to access more than five project-IDs, then all functional OPRs on the system need to concur with the request since the user does have the potential to acquire exempt status. The coordination and signature level for this letter will be handled like a request for QLP with Update. Reference *Section 5.5,* Appropriate Coordination Level for additional information.

For ALN:

- *(S104.340.00: CAT II) The IAO will ensure non-exempt users, except where documented, are not be allowed to enter their project-ID at sign on time.*

NOTE: Users with a valid need are a documented exception.

- *(S103.330.00: CAT II) The IAO will ensure non-exempt users, except where documented, are restricted to a specific list of project-IDs*

Users with a valid requirement are a documented exception.

- *(S103.310.00: CAT II) The IAO will ensure non-exempt users do not have an exempt project-ID in their userid record.*

3.4 Access Control Records

An Access Control Record (ACR) is a security record in the SACRD$ file. It is the most powerful form of object protection used on a Unisys mainframe. It can protect files and userids. ACRs are created through the SIMAN processor and are primarily used by the Security Officer to protect files that contain sensitive or volatile information.

3.4.1 Installing ACRs

An ACR will be installed using SIMAN in either screen or batch mode. An ACR may be created like another and modified before actually being created. Once an ACR is installed, it may be attached to multiple files.

3.4.1.1 Userid Requirements

In order for a user to install an ACR, his or her userid needs to have ACRs allotted in the userid record. For recovery reasons, you will use only the Security Officer's userid to create ACRs. The exception to this is system-type ACRs that are owned by Fixed Gate Subsystem userids such as CHAMELEON.

3.4.1.2 ACR Arguments

An ACR restricts access to objects based on userid, account, project-ID, time, or any combination of these. These criteria will allow or prevent access per the Type of Object Access to be Controlled. It is most common to restrict access by account, since that is a natural way to separate users according to their AIS and/or site.

3.4.1.3 Access Restrictions

These arguments determine whether a user has access to the object.

3.4.1.3.1 Userid

The userids that are allowed access may be listed and then only those users may access the object. The problem in the past with this was that ACRs couldn't be modified once they were installed. Since SB5, ACRs can be modified after they are installed, but any list of userids is subject to change over time as people change jobs, retire, etc., and the longer the list of userids, the more subject to change it becomes. For one userid or a very short list of userids, this is the best type of access restriction. For medium to long lists, it is not advisable. Procedures to handle changes to personnel (userids) will be available.

- *(A102.110.00: CAT II) The SA will ensure ACRs on the system contain hard-coded userid names in the condition field are updated when the userid is either disabled or deactivated.*

3.4.1.3.2 Account

The user may access the object only when his or her userid is under the specified account. The Security Officer controls which userids have access to these accounts and can then control which users can satisfy the ACR. This is usually the best choice for groups of users on a site system.

3.4.1.3.3 Project-ID

This is a poor method for securing files. Most users can either sign on with a choice of project-IDs, or start jobs under a different project-ID. Although this may be used as a programmatic means of ensuring that a user is under the correct project-ID, there are better ways of doing it.

3.4.1.3.4 Time

This is another poor choice for an ACR access restriction. The system date/time is subject to change by operators or privileged users. Also, a determined intruder will wait until whatever time necessary to break into a file.

3.4.1.4 Object Access

The types of object access are *read*, *write*, *delete*, *execute*, *ACR_Delete*, and *modify*. They define what type of access the user is permitted to once that user satisfies the argument. If an ACR has multiple arguments and the user falls under two or more categories, the user is granted the most amount of access from each argument.

3.4.1.4.1 Write

User can modify the object.

3.4.1.4.2 Delete

User can delete the object.

3.4.1.4.3 Execute

User can only execute from the file.

3.4.1.4.4 Read

User can read from the object. For files, assumes Execute access also.

3.4.1.4.5 ACR_Delete

Unused. Only Profile 1 userids may delete an ACR and can therefore bypass this restriction. Not valid with owned ACRs.

3.4.1.4.6 Modify

Users need to pass through this ACR before being able to modify security records. Not valid with owned ACRs.

3.4.2 ACR Ownership

When an ACR is created, it becomes owned by the userid that created it or a different owner if one is specified during ACR installation. This ownership feature cannot be bypassed and effectively changes the name of the ACR. For instance, if the userid SECOFF creates an ACR called CIVPAY, the name of the ACR will be CIVPAY owner = SECOFF. This means that multiple users can create ACRs called CIVPAY, each being distinct.

a. If the Security Officer allows a functional user to create an ACR, then the user will own that ACR. If you ever have to initialize the SACRD$ file, the runstream for recreating the ACR will make it owned by the Security Officer by default (since ownership cannot be bypassed). This causes a security mismatch on any file that had that ACR attached, since the file is still expecting the ACR that no longer exists.

b. A security mismatch causes problems when reloading files using the MFDLOD or any other FAS runstream. This typically shows up during a 4-13 boot, when you can least afford such problems.

c. Because of this, the Security Officer will make sure that no functional user creates ACRs. Most ACRs will be owned by the Security Officer's userid. If an AIS manager absolutely insists that the ACR be owned by a particular userid, that AIS manager will take full documented responsibility for its integrity and that of the files it controls.

d. Recoverable ACRs are those owned by the Security Officer and those created upon SACRD$ initialization (owned by EXEC8).

e. Unrecoverable ACRs are those owned by other userids or those that are unowned (created before the SB3 release).

3.4.3 Creating ACRs

In order to create an ACR, refer to 7831 0661, SIMAN Administration and Operations Guide. Sign on into Demand using the Security Officer's userid. There are two ways of creating ACRs. This is either through screen mode or batch mode.

a. Screen Mode. Normally batch mode is the best way of creating an ACR. It is menu driven and guides the user towards creating an ACR correctly. When creating an ACR in screen mode, the default owner is the userid of the user who is executing SIMAN. The owner field can be modified to reflect another owner. If another owner is specified, make sure this userid has remaining ACRs available. Note that the ACR like an existing ACR feature is available. If the LIKE feature is chosen, make sure to enter the correct owner. If the wrong owner is used, SIMAN will respond that the like ACR does not exist in SACRD$ or worse yet, if the like ACR selected exist SIMAN will use the wrong arguments in creating the new ACR.

b. Batch Mode. Normally, Batch Mode will be avoided. The only time you would want to use batch mode is when you are reinitializing SACRD$. The rebuild runstreams run in batch mode.

3.4.4 Displaying ACRs

When displaying ACRs in SIMAN, remember to select the correct ACR owner. SIMAN screen mode assumes your userid as the owner. SIMAN batch mode assumes no owner. To get a list of all ACRs in SIMAN, generate an ACR summary report.

3.4.5 Modifying ACRs and Recovering Deleted ACRs

ACRs can now be modified directly the way userids and accounts can be modified through SIMAN. It is also possible to recover a deleted ACR through SIMAN. Deleted ACRs are updated (as opposed to reinstalled). When you COMMIT the ACR record during update, it will be recovered.

3.4.6 Deleting ACRs

It is not necessary to delete ACRs. The only two times you will delete an ACR is when you are going to reinitialize SACRD$ or after coordinating with the SSO in Montgomery.

3.4.7 Restoring Deleted ACRs

If you do delete an ACR, and are running SB5R4 or later, you may restore deleted ACRs by editing them. When the edit is committed, the deleted flag will be cleared and the ACR restored.

3.4.8 Attaching ACRs

To attach an ACR, you need to have a Profile 1 or 2 to attach an ACR to a file and a Profile 1, Security Administrator to attach an ACR to a userid record. This may be done through either screen mode or batch mode. You may attach an ACR to a file or a userid. These are both

considered objects. An ACR may be attached to more than one object. Once an ACR is attached, a user needs to pass the arguments of the ACR in order to have access to the object. To attach an ACR to a file, the file will either be unowned or owned by the same userid that created the ACR. To attach an ACR to a userid, the userid needs to be owned by the same userid that created the ACR. Note that in both cases, this is all simplified by having the Security Officer's userid own all ACRs.

a. Screen Mode. Normally you will use screen mode to attach an ACR to an object.

b. Batch Mode. This is the method used by some AISs to attach existing ACRs to their files as they are created. A good example of this is Accounting and Finance attaching ACRs to their paycheck print files. Example SIMAN syntax:
UPDATE FILE = Q*FN. ATTACH_ACR = ACRNA ACR_OWNER = EXEC8 ;

3.4.9 Removing ACRs

To remove an ACR, your userid needs to be a Profile 1 or 2, and you need to have prior access to the object. When you remove an ACR from an object, the ACR no longer controls access to the object. Do not delete the ACR. The ACR may be attached to more than one object.

a. Screen Mode. To remove the ACR, blank out the field for the ACR and its owner. After you COMMIT, you may want to check and make sure the ACR was removed from the object.

b. Batch Mode. To remove an ACR from an object, update the object and attach no ACR. Example:

    UPDATE FILE = Q*FN. ATTACH_ACR ;

3.4.10 Bypassing ACRs

There is a SIMAN Privilege that allows you to bypass ACRs. If a userid can bypass ACRs, he or she bypasses every security restriction dealing with ACRs. This effectively grants the user all types of object access. There are no warnings to tell the user or the owner of the ACR that the ACR is being bypassed. This Privilege is given to Profiles 1 and 2. These userids belong to site personnel, and they have to get to all files on the system. Users outside the site will not be allowed to bypass ACRs and access to this privilege within the site will be restricted.

3.4.11 System/Standard ACRs

The following table lists ACRs found on most Unisys systems. There are also numerous system type ACRs, which are owned by various Fixed Gate Subsystem userids.

ACR NAME	*OWNER*	*SERVICE*	*PURPOSE*
ACRRO	EXEC8	System	Read-only System ACR installed at system initialization
ACRNA	EXEC8	System	No-Access System ACR installed at system initialization
GUJXFG	GUJXFG	ALN	ACR attached to various system files
EXEDEL	Security Officer	System	Attached to the Fixed Gate Subsystem Userids to control execute access and deactivation of subsystems owned by the Fixed Gate Subsystem userids
PUBRD	Various Fixed Gate Subsystem userids	System	Attached to Fixed Gate Subsystem and System Library files to protect and control access to these files and subsystems

Table 3-27. System/Standard ACRs

3.5 System Logging

As a minimum, the system will be configured to log all system activity for purposes of audit, investigation, and recovery.

3.5.1 ASCII Audit Trail

Disk logging of the ASCII log audit trail (ALAT) or system log file, which has a filename of SYS$*F010L1, will be configured so that the cycle threshold is high enough to accommodate the amount of data generated between backups of ALAT or system log data. ALAT or system log file save tapes will be retained at least one year (365 days).

- *(S103.090.00: CAT II) The IAO will ensure the cycle threshold on the system log file is set high enough to prevent the overwriting of data prior to backup.*

- *(S103.100.00: CAT II) The IAO will ensure the system log file save tapes are retained at least one year (365 days).*

3.5.2 TIP Audit Trail

The TIP audit trail tapes will be retained for a minimum of 30 days. Since TIP audit trail tapes are considered a multiple reel tape series or file, the VOLSCR (volume scratch) flag will be set on these tapes in STAR. This flag will ensure the specific reel (volume) is scratched 30 days after creation. If the VOLSCR flag is not set, the TIP audit trails could be scratched prematurely

as a filename. The VOLSCR flag can be automatically set by using the SYSLIB*STRPARM. AAFPARM element. In addition, TIP audit trails will be physically and logically secured. For example, TIP audit trail tapes will be kept in the computer room or in a secured off-site storage facility, and will be identified with *read-only* access in STAR. If the TIP audit trails are kept on disk, they are identified as G-option files with a Clearance Level of 63, and are secured with the ACR ACRNA. On SSO Montgomery released operating systems, the disk TIP audit trails are identified as G-option files with a Clearance Level of 0, and are secured with the ACR ACRRO. Disk TIP audit trail files will need to be periodically saved to tape via the IRU MOVE command and the save tapes (with a file name of AUDIT$0xUNT1/T2) will be retained for a minimum of 30 days. These save tapes will also be physically and logically secured.

- *(S103.080.00: CAT II) The IAO will ensure TIP audit trails tapes or disk files are retained for a minimum of 30 days.*

- *(S101.030.00: CAT II) The IAO will ensure TIP audit trails are physically and logically secured.*

3.5.3 MAPPER Audit Trail

The MAPPER audit trail tapes or disk files will be retained for a minimum of 30 days.

- *(S103.110.00: CAT II) The IAO will ensure MAPPER audit trail tapes or disk files are retained for a minimum of 30 days.*

3.5.4 Console Logs

Most system configurations provide for printed logs of all operator-console activity. These logs generally need not be secured at any higher classification than the data on the system and may be disposed of normally. However, in the case of a system initialization (4-13 boot or security initialization) or times when the CONSOL job is started, the console logs and/or SPO logs may contain authentication information in the form of userids and passwords. These logs will be stored separately in a secure manner and destroyed before being discarded. Alternatively, as long as the passwords are immediately changed on the userids that were used, the console logs and log file cycles can be treated as usual.

- *(A101.090.00: CAT II) The IAO will develop procedures to secure and destroy console logs containing system passwords.*

3.5.5 DCP Logging

All DCPs in the site network need to generate CENLOG entries identifying attempted NMS logins and remote attacks through the network. These entries or logs will be generated and retained for a minimum of 30 days. Contact the SSO if you need assistance in accomplishing this step.

- *(A103.010.00: CAT II) The SA or NA will ensure CENLOG entries are generated for all DCPs in the site network.*

- *(A103.020.00: CAT III) The IAO will ensure CENLOG entries are retained for a minimum of 30 days.*

3.6 Processor Protection Methods

There are some processors that are very powerful and potentially dangerous so no access or restricted access to these processors will be required. These processors are necessary to the function of the system. The IAO can control access to these processors by using Access Control Records (ACRs), or in some cases through security controls built into the products themselves. Typically, these ACRs exclude access based on account or exclude all access. These processors and the methods to be used in securing them are listed in *Section 8, System Processors*.

4. MANAGEMENT OF THE UNISYS SECURITY ENVIRONMENT

SIMAN provides an administrator with an interface to a number of important system areas, including userid maintenance, account maintenance, ACR maintenance, cataloged file security maintenance, quota maintenance (if implemented), the SIMAN environment configuration itself, and the overall system environment. These are generally controlled within the SYS$*TSS$FILE file, the SYS$*ACCOUNT$R1 file, and the SYS$*SACRD$ file. The data that is entered on the userid and account INFO screens are stored in the SYS$*SIMAN$INFO file. See *Figure 4-1,* below.

NOTE: TIWADS applies to sites running the ALN operating system only.

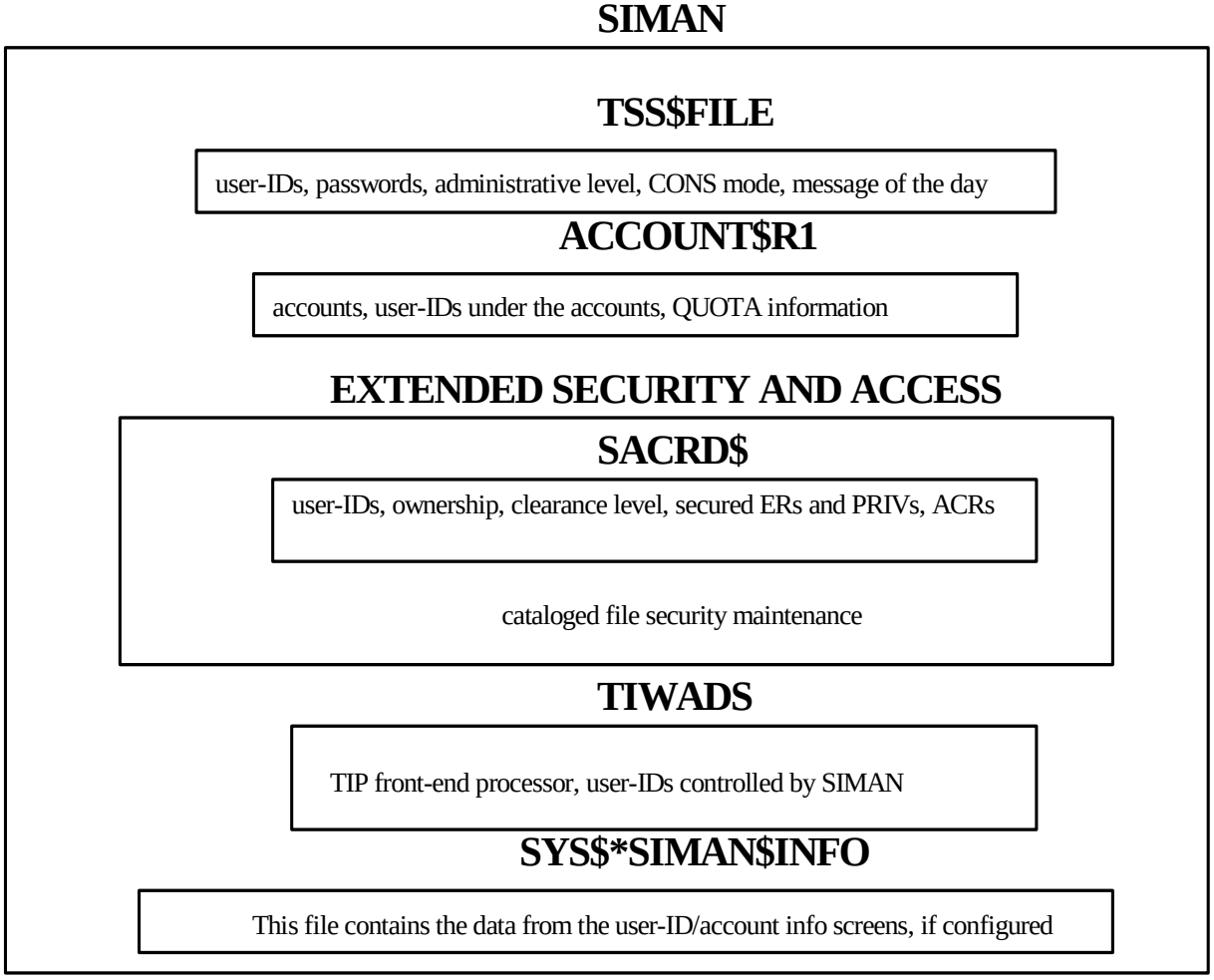

Figure 4-1. Security System Span of Control for system levels below HMP IX 7.0

General Requirements

There are four basic security files for Unisys mainframes. These are SYS$*ACCOUNT$R1, SYS$*TSS$FILE, SYS$*SACRD$, and SYS$*SIMAN$INFO. These files will be saved at least two times a week or as directed by the Security Officer, and will have a minimum retention of 14 days. If there is a loss of data, or if a Jump-Key 13 boot is done, these files will be reloaded. There is an additional ALN security file that can be saved to a tape called SECTAPE. The SECTAPE is the output tape from the Security Merge utility, which is documented in the USIT Software Users Manual. The primary reason for generating a merge tape for each site ALN system on a regular schedule is for contingency. If an entire site system is lost due to a hardware failure, natural disaster, or other reason, the workload for that host may have to be moved to another site host that already has a workload on it. Therefore, it would be necessary to merge the userids from the downed host onto the working host rather than simply loading the security files.

For system levels greater than or equal to HMP IX 7.0 the following security files will be backed up at least twice a week and will be retained for a minimum of 14 days.

SYS$*SEC@USERID$
SYS$*SEC@ACR$
SYS$*SMDTF$
SYS$*ACCOUNT$R1
SYS$*SEC@ACCTINFO

Sites running the Access and Location Number (ALN) operating system may also create the Security Merge SECTAPE file on a monthly basis.

4.1.1 Availability of Security Tapes

4.1.1.1 Created using the SV and SF keyins.

At least two cycles of the four security tapes (TSS$FILE, ACCOUNT$R1, SACRD$, and SIMAN$INFO) will be available at all times. More than two cycles are advisable to provide a more complete backup environment. Three sets or more would be ideal since at most sites this would offer multiple backups in case of a bad tape in any given tape set. Even in an environment with robotic cartridge tape silos, the three security tapes (SYS$*ACCOUNT$R1, SYS$*TSS$FILE, SYS$*SACRD$) and the Security Merge SECTAPE, if created, will be retained on tapes. The SIMAN$INFO tape can be created in the silo, if desired. To ensure these tapes cannot be inserted into the tape cartridge silos, the AUTOLIB flag in STAR will be removed on all tapes that will be used for security file backups and the Security Merge process. In addition, the system operators will never mount these tapes except upon a verified request from the site IAO. This will be documented in the Standard Operating Procedures/Instructions. Implementing a separate ‘pool’ of tapes specifically for the security file backups and the Security Merge process can best satisfy the requirements above.

4.1.1.2 Created using the SEC, SAVE keyin

At least two cycles of the four security tapes, for systems prior to HMP IX 7.0 (the TSS$ save tape, the ACCOUNT$ save tape, SACRD$SAVE, and SIMAN$INFO), or the SECTAP$, for systems HMP IX 7.0 and higher, will be available at all times. More than two cycles are advisable to provide a more complete backup environment. Three sets or more would be ideal since at most sites this would offer multiple backups in case of a bad tape in any given tape set.

If the security tapes are to be maintained within a tape silo, mitigating controls must be implemented to prevent the mounting of security tapes by an unauthorized user. The primary control is that the security file backups will be made with the SEC,SAVE command. additional mitigating controls will be in either the AMS or the use of tape pools in the tape management software. In ether case, a description of the controls should be maintained by the IAO.

- *(S103.050.00: CAT II) The IAO will ensure two cycles of the four security tapes (TSS$FILE, ACCOUNT$R1, SACRD$, and SIMAN$INFO) are available at all times.*

- *(S103.050.00: CAT II) The IAO will ensure the three security tapes created by the SV and SF keyins (SYS$*ACCOUNT$R1, SYS$*TSS$FILE, SYS$*SACRD$) are retained on tapes, if created.*

- *(S104.720.00: CAT II) The IAO will ensure the if the security tapes are made using the SV and SF keyins, AUTOLIB flag in STAR is removed on all tapes used for security file backups.*

- *(S104.720.01: CAT II) The IAO will retain documentation of the mitigating controls in place for security tapes created using the SEC,SAVE keyin and stored within a tape silo.*

- *(S103.120.00: CAT I) The IAO will ensure operators do not mount the security tapes except upon a verified request from the IAO.*

For ALN:

- *(S103.050.00: CAT II) The IAO will ensure the Security Merge SECTAPE, if created, is retained on tape.*

- *(S104.720.00: CAT II) The IAO will ensure the AUTOLIB flag in STAR is removed on tapes used to create the Security Merge SECTAPE.*

4.1.2 Physical Security

A segregated area is recommended for these tapes at the off-site storage facility so they can be quickly identified during a contingency and better controlled on a day-to-day basis. Until degaussed, all security tapes will be kept on the computer room floor, within the tape silo if appropriate mitigating controls are in place, or at the secured off-site storage facility unless removal is authorized by the IAO. These tapes will not be used as input to jobs unless under the direct supervision of the IAO. The IAO will ensure any assignment of these tapes is made on a

standalone tape drive unless they are stored within a silo with appropriate mitigating controls in place.

- *(S104.720.00: CAT II) The IAO will ensure all security tapes are kept on the computer room floor or at the secured off-site storage facility unless removal is authorized by the IAO.*

- *(S103.120.00: CAT II) The IAO will ensure security tapes are not be used as input to jobs unless under the direct supervision of the IAO.*

4.1.3 Saving Security Files

The four regular security files will be saved twice weekly, using the following keyins from the system console:

SV ,HIC40/<reel#> EXEC-8 SYS$*TSS$FILE(1)
SV ,HIC40/<reel#> EXEC-8 SYS$*ACCOUNT$R1(1)
SF HIC40/<reel#>,SACRD$
ST SAVE/SIMAN$INFO,,,<ops acct>/<ops userid>

Optionally the following keyin can be used in place of the two SV keyins and the SF keyin.

SEC,SAVE HIC40,<reel#>,14

NOTE: For all systems HMP IX 7.0 and later, only the SEC,SAVE keyin may be used and the SIMAN$INFO file no longer exists.

4.1.4 Load Sequence

In all cases, the security file sequence will be the following at boot time, if at all, before SYS starts:

SACRD$
TSS$FILE
ACCOUNT$R1

NOTE: For all systems HMP IX 7.0 and later the system controls the order of file reload.

4.1.5 SIMAN$INFO

For systems prior to HMP IX 7.0, if the user has the INFO pages configured on their system, special care needs to be taken to restore the SIMAN$INFO file during a 4-13 boot. Remember that on a 4-13 boot, when the system is initially brought up, the MFD has been initialized, so no files yet exist on the system. Since SIMAN expects the SYS$*SIMAN$INFO file to be there and it is not, any jobs which attempt to use the SIMAN processor will error until this file is loaded. For this reason, the 4-13 boot procedures have been changed so that the system will call for this file to be loaded during the boot process. However, if the SIMAN$INFO save tape is

not available to load when prompted for, significant problems will result. Therefore, make sure the site saves the SIMAN$INFO file every time the other security files are saved.

4.1.6 Securing the JX$$0000*00 File

The JX$$0000*00 file contains all the SSO Montgomery released standard security profile runstreams. To ensure these profile runstreams are protected from modification by unauthorized personnel, this file will be protected with the ACR ACRRO that is owned by EXEC8. To attach this ACR, the IAO will perform the following:

```
@SIMAN,B
UPDATE FILE = JX$$0000*00.
ATTACH_ACR = ACRRO        ACR_OWNER = EXEC8 ;
DISPLAY FILE = JX$$0000*00. ;
```

This will attach ACRRO (*read-only*) to the JX$$0000*00 file. It will then display the file. The file will show the ACR attached. If so, the only users that may update elements in the file are those with ACR bypass privileges (site personnel). All users can read or @ADD elements in the file.

- *(S103.790.00: CAT II) For DISA sites, the SA will ensure the Standard Security Profile file (JX$$0000*00) will be secured with the ACR ACRRO to protect it from modification by unauthorized personnel.*

4.2 Initializing Security Files

This will be done only at the request of the site IAO. This erases all security information in the file initialized. This also eliminates deleted userids and ACRs from the SACRD$ file. This will only be done with direct technical support from SSO Montgomery and they can be contacted through the FAB at DSN 596-5771.

4.2.1 SACRD$

To initialize the SACRD$ file, perform either a tape boot (long or short) or the SC S/1 keyin from the operator's console followed by a disk boot.

```
0-METHOD TO OBTAIN SECURITY FILE—LOAD,INIT,RECOVER      (system)
(L,I,R)
(When performing a JK 4,13 boot, there is no RECOVER option.)

0 I                                                     (operator)

0-ENTER 12-CHARACTER SECURITY OFFICER USERID             (system)
```

NOTE: The Security Officer userid does not need to be 12 characters long. This is only given as a maximum.

0 <security officer userid> (operator)

(Doing a JK 4,13 boot, will also initialize the TSS$FILE.)

4.2.2 TSS$FILE

Initializing the SACRD$ file, will allowthe system to initialize the TSS$FILE.

0-SPECIFY METHOD TO OBTAIN TSS$ FILE— INITIALIZE,RECOVER (I,R) (system)

0 I (operator)

4.2.3 ACCOUNT$R1

This may only be initialized during a boot with JK 13 set.

0-ENTER MASTER ACCOUNT (system)

0 <Master account name> (operator)

NOTE: Do not change the master account here. Use SIMAN to do that.

4.2.4 Contents of Initialized Files

After initialization, the security files will have the following information.

TSS$FILE	Security Officer's userid, as a SIMAN Administrator, with a password of SECURI, no generated @run image Pointers to the master account, with a link to the Security Officer's userid

SACRD$	Master secured ER/Privilege table Security Officer's userid, all ERs and Privileges INSTALLATION userid, all ERs and Privileges EXEC8 userid, all ERs and Privileges ACRNA ACR (no access) owned by EXEC8 ACRRO ACR (read-only) owned by EXEC8 SMDTF$ file
ACCOUNT$R1	Master account, pointers to security officer's userid

NOTE: The Master userid and Master account will match those in the TSS$FILE.

Security Officer's userid entered under the master account
Account INSTALLATION with userid INSTALLATION
Account STNDRD-ACCNT with userid STNDRD-USRID

4.3 Merging Security Files (ALN Only)

A utility is available from SSO Montgomery that will allow the IAO to merge some or all of the security environment from one system into the security environment of another system, effectively migrating one system's users to another machine. This utility is documented in the USIT SUM. The merge save tape that is created by this utility contains all of the userid, account, ACR, and quota information from the SIMAN environment, and will therefore be protected to the same extent as the primary Security Files. The merge save tape will be used if the site encounters some kind of catastrophic failure, which would require the movement of a workload onto another mainframe. In this case, it is likely that the site's workload will be moved onto another site mainframe in addition to the workload already being processed on that system. Since the users of the other system will continue to have access to that system during the time when the site's workload is being processed there, the Security Merge utility provides the best way of installing the site's SIMAN environment on this system. A merge save tape may be created at least once a month or more often as directed by the IAO, and a security merge save tape, if created, will be kept off-site for contingency purposes.

4.4 Account Messages

If a userid tries to access an unauthorized account, the operator will be asked to intervene. An unauthorized account is one where the security officer did not enter the userid under the account in SIMAN. If the operator does not allow an undefined userid or account to process, the user or runstream requesting access will get an *ILLEGAL USERID message and terminated abnormally. Please note that the DNMC Unisys environment is configured in such a way that these messages are not generated by the system. Users of this environment can skip ahead to *Section 4.5, Reinitializing SACRD$.*

4.4.1 Userid Not Under the Account

If the userid is not authorized to run under the account or if the AER message was already answered once with an A, the operator will get the following message:

0-<run-ID> USID <userid> UNDEF FOR ACCNT <account> AER

This message may be answered in one of three ways:

0 R REJECT-access denied. Job/userid will error fin.

NOTE: This will be the standard response to this message, since any other answer could give a user access to an account for which the user is not authorized.

0 E ENTER-access approved. Userid will be entered under the account.

0 A ACCEPT-access approved, but just once. The next time the userid tries to access the account, the AER message will be generated again. The userid will be added to the account for tracking purposes only. In SIMAN, the userid under the account will look the same as any others.

4.4.2 Account Does Not Exist

If the account does not exist, or if the AER message was already answered once with an A, the operator will get the following message:

0-<run-ID> UNDEF ACCT/USID <account>/<userid> AER

This message may be answered in one of three ways:

0 R REJECT-access denied. Job/userid will error fin.

NOTE: This will be the standard response to this message since any other answer could give a user access to an account for which that user is not authorized.

0 E ENTER-access approved. Account will be created. Userid will be entered under the account.

0 A ACCEPT-access approved, but just once. The next time the userid tries to access the account, the AER message will be generated again. The account is created with the userid under it. Any other userids entered under this account in any way will also get the AER message.

NOTE: SIMAN tracks the method used to create an account on the USAGE screen in the account maintenance loop. An account may be entered via the A keyin, E keyin, or by the Site Administrator.

4.5 Reinitializing SACRD$

Because of the changes in the security file structure and names, this procedure applies only to systems prior to HMP IX 7.0. There is no equivalent procedure to this with systems HMP IX 7.0 and above.

The system security files are initialized when a system is first booted. There are some situations require the starting over and reentering of userids into SIMAN. This section briefly discusses the keyins used to initialize security files but not the consequences of each step. Usually, the only security file that would be reinitialize is SACRD$. When the SACRD$ file reinitialized all userids are the, clean out of SIMAN. Please note that since SB5R4, it is possible to delete and reinstall ACRs through SIMAN, which removes the need to initialize the security files to recover an ACR. Be very careful with file ownership and ACR ownership during these procedures. These steps may take a long time and most of this is down time.

4.5.1 Impacts and Prerequisites

A security initialization is a very serious step and is not to be taken lightly. This is an all-else-fails situation and will be done with the support of the FAB and the Systems Support Office. Among the things needed is to generate beforehand are a Userid Summary Report and Cataloged File Security Summary Report from SIMAN.

4.5.2 Alternatives

Having access to a low-use Unisys system with the same Exec level as the site, load the security tapes to that system. The actual re-initialization could then be done there off-line, saved, and then reloaded to the original machine. The other system's security files would then be reloaded. Most IAOs will have to schedule the process over a weekend.

4.5.3 Procedures

The SACRD$ file is usually reinitialized when someone has deleted a critical userid or system userid and no fallback security tapes are available. Since the SB5R4 release, it is no longer necessary to reinitialize the security files to recover an important ACR. Make every attempt to reload an old SACRD$ tape from before the deletion of the userid. If you manage to find such a tape, reload it in accordance with normal site procedures. The user would then have to recreate all the changes they made to SIMAN since the day the SACRD$ file was saved. If there is no such tape, then continue with these steps.

a. Generate a Cataloged File Summary Report in SIMAN. This will show all files with an attached ACR. Print the report.

b. Save all four security files. Refer to *Section 4.1.3, Saving Security Files*, for more information on saving security files.

c. Perform a SAVALL (or BACKALL).

d. Delete all undesirable ACRs and userids from SIMAN.

e. Sign on with the Security Officer's userid.

f. Go into the SIMAN Environment and make sure that Extended Security and Access Control is set.

g. Generate an ACR Summary Report and Userid Summary Report.

```
@SIMAN,B
DIS ACR=!ALL   SYN   BRE = SECURITY*ACRS. ;
DIS USE=!ALL   SEC_ACC SEC_INF    SUB_INF
               SYN   BRE = SECURITY*USERS. ;
@EOF
```

NOTE: These files are examples. Other filenames can be used. By specifying SEC_ACC, SEC_INF, and SUB_INF, SIMAN only generates information needed to recreate the SACRD$ file.

h. Use a text editor to inspect the contents of these files. If they are empty, recheck Extended Security and Access Control.

i. Once satisfied that these files reflect the current SACRD$ environment, initialize security as discussed in *Section 4.2, Initializing Security Files*.

j. Initialize both the SACRD$ and TSS$FILE files. If the files are not initialized the TSS$FILE, the runstreams cannot create the userids.

k. Do not change the Security Officer's userid when the system asks for the 12-character Security Officer userid. This will confuse SIMAN as to which userid can update accounts.

l. Bring up CMS.

m. Reload the old ACCOUNT$R1 file.

n. Sign on with the Security Officer's userid.

o. Make sure TSS$FILE and SACRD$ file were initialized.

```
@SIMAN,B
GEN USE_SUM ;
@EOF
```

NOTE: This will only show the Security Officer's userid in both files as well as INSTALLATION and EXEC8 in the SACRD$ file.

p. Recreate the userids and then the ACRs. Make the following runstream and @START it.

```
@SIMAN,B
@ADD SECURITY*USERS.
@ADD SECURITY*ACRS.
@EOF
```

NOTE: This may run for a long time (a few hours).

q. Make sure the userids and ACRs were created in SIMAN.

```
@SIMAN,B
GEN USE_SUM ;
GEN ACR_SUM ;
@EOF
```

NOTE: All of the userids and ACRs will be installed.

r. Reload the TSS$FILE tape saved in Step (b) above.

s. Sign off and back on with the Security Officer's userid. The password will be back to normal.

t. Check for a SIMAN Environment update.

```
@SIMAN
```

If the normal SIMAN menu appears, go on to the next step. If a warning that states the user needs to perform a SIMAN Environment update, do the following:

1. Type Y in the home position of the screen and transmit.

2. Keep transmitting through the SIMAN Environment screens until it loops back. Once satisfied with the environment, type, COMMIT in the home position of the screen and transmit.

u. The security files have been reinitialized.

v. Save all three security files.

5. DATABASE MANAGEMENT UTILITIES/RETRIEVALS

DataBase Editor (DBE), Query Language Processor (QLP) with Update, Interactive Query Utility (IQU), and Louis II/Louis Link are products used in the recovery, maintenance, and retrieval of Data Management System (DMS) databases. Due to the power of these utilities to view and modify raw data and change physical database structures, these products require special protection. Access to any of these database management utilities will be obtained according to the procedures described in *Section 5.5.2* IQU, DBE, EZLOAD, and TERMRUN$ – ALN *or Section 5.5.3* IQU, DBE, SYMCTL, RNCNT1, and EZLOAD – DFAS-IN. These access requirements apply to all personnel.

a. Scope. Interactive data base update and retrieval processors exist on almost every Unisys platform in the DOD inventory.

b. Protection Period. DBE, QLP w/Update, IQU, and Louis II will be protected throughout the life cycles of these products or they will be removed/deinstalled from the system.

5.1 DBE

DataBase Editor (DBE) is used to perform manual updates to online databases. The processor is so flexible and dangerous that extreme care needs to be taken in securing this product. DBE will be secured and managed by the IAO. All sites using DBE will implement DBE security. When DBE security is implemented, it creates a file called <DBE qualifier>*DBE$SEC. The DBE qualifier for DFAS-IN (Indianapolis) sites is DMS. The DBE qualifier for ALN sites is DMS$0000. The only authorized version of DBE is the version released by SSO Montgomery. Source files for DBE (<DBE qualifier>*F1 through F5 or <DBE qualifier>*File1 through File5) are only authorized on the SSO Montgomery development systems.

- *(S103.310.00: CAT II) The SA will ensure sites using DBE implement DBE security.*
- *(S103.290.00: CAT II) For DISA sites, the SA will ensure only the authorized version of DBE version released by SSO Montgomery is used.*
- *(S103.300.00: CAT II) For DISA sites, the SA will ensure the DBE source files are only available on SSO Montgomery development systems.*

5.1.1 DBE with Normal Security

DFAS-IN (Indianapolis) sites that are running normal DBE with userid security will use the following procedures. If a user has update capabilities in DBE with Normal Security, the user can update any functional database in any application group on the system. However, all updates performed by DBE with Normal Security are displayed on the console and written to the system log file. For these reasons, access to DBE will be limited to high-level functional users. The functional AIS manager at each customer site will identify specific individuals as authorized DBE users. This will be done in a letter and will be redone yearly or upon any additions. This letter will be coordinated at the level specified in *Section 5.5.3.1,* IQU, DBE, SYMCTL, and RNCNT1 Coordination – DFAS-IN, since users can not be restricted to a specific schema or

application group when using normal DBE security. After the site IAO has received the list of authorized users, permanent access will be granted. The IAO will retain the access request letters.

The site IAO will use the following procedures to set up the DBE security environment.

a. Restricting demand access by userid is mandatory; further restriction by terminal-ID is optional, but not recommended.

b. Access to DBE Batch security must be defined at the account level. Adding userids to DBE Batch security will not allow the DBE Batch runstream to work properly.

c. The site IAO will maintain master update control in DBE.

Normal DBE :

- *(S103.310.00: CAT II) The SA will ensure access to DBE with normal security is restricted to specific userids and, if using DBE batch, specific accounts.*

- *(N/A: CAT II) The IAO will ensure User access is be documented in accordance with this STIG requirements.*

5.1.1.1 Initial Installation of Normal DBE

When DBE with userid security is genned, an initial default userid of DBEGEN is identified. To initialize DBE security for the first time, the user must sign on with this default userid. This userid will be installed in SIMAN as a Profile 8 userid. The IAO will sign on to demand with this userid and accomplish the following steps.

```
@ASG,CP   DMS*DBE$SEC/SEC/SEC(+1).,F///128
@DMS*DBE.DBE,S
DBE 6R1C.7 2200/X00 L43 (RELEASE) (990316 0927:51) 990325 1950:35
-<120> INTERNAL ERROR: 000000000005 – REPORT PROBLEM
        -<128> FAC WARNING: 000000100000 ON @ASG,A OF SYSTEM MACRO
           LIBRARY
        -<16> FAC WARNING: 000000100000 ON @ASG,A OF HELP LIBRARY
           FILE
NOTE:      You will only see the above error and warnings will only be seen the first time
           DBE is installed.
USAGE  (Puts the user into DBE's command Language)
I,D        (Initializes demand security)
I,S        (Initializes terminal/site security)
I,B        (Initializes batch security)
C,D,< Security Officer's Userid>     (Creates DBE Master userid)
A,D,< Security Officer's Userid>,A,I,M,U,D,N
           (Gives the Security Officer's Userid the A, I, M, U, D, and N options.)
EXIT <XMIT>  (Writes information to the DBE Security File)
```

EXIT <XMIT>

After installing the DBE Master userid, use SIMAN to remove all run modes from the DBEGEN userid and disable this userid.

Normal DBE :

- *(S103.340.00: CAT II) The SA will ensure following the initial installation of normal DBE with userid security, the DBEGEN userid is disabled with no run modes.*

5.1.1.2 Installing Additional DBE Master Userids

Master userids for normal DBE security will be restricted to the Security Officer and other SIMAN Administrator userids. These userids will be set up in DBE with all of the options (M, U, A, I, D, and N).

Normal DBE :

- *(S103.330.00: CAT II) The SA will ensure access to the DBE Master userids is restricted to the Security Officer and SIMAN Administrator userids.*

5.1.1.3 DBE Restriction by Userid

To set up DBE demand access restriction by userid only, perform the following steps. To give each functional user access to DBE with update, the IAO will install his/her userid internally using the following commands while signed on under a Master DBE userid.

@DMS*DBE.DBE,S
USAGE (Puts the user into DBE's command Language)
C,D,<AIS Userid> (Creates DBE demand userid)
A,D,<AIS Userid>,U,A,I,D,N
(Gives this userid the U, A, I, D, and N options. See NOTE below.)
EXIT <XMIT> (Writes information to the DBE Security File)
EXIT <XMIT>

NOTE: The U option allows updates and will only be given to select high-level functional users. For users that do not need update capability, use a normal userid and omit the U option.

5.1.1.4 DBE Restriction by Userid/Terminal-ID

To set up DBE access restriction by userid and terminal-ID, perform the following steps while signed on under a DBE Master userid. This method is not recommended since terminal-IDs can be spoofed.

@DMS*DBE.DBE,S
USAGE (Puts the user into DBE's command Language.)

C,D,<AIS Userid> (Creates DBE demand account.)
A,D, <AIS Userid>,I,D,N (Gives this account the I, D, and N options.)
C,S,<terminal-ID> (Creates DBE terminal-ID account.)
A,S,<terminal-ID>,I,U,D,N (See NOTE below.)
EXIT <XMIT> (Writes information to the DBE Security File.)
EXIT <XMIT>

NOTE: Notice that if access needs to be restricted by both userid and terminal-ID, the user will not set up the userids in DBE with the A option, as that will defeat the use of the terminal-ID security. The U option allows updates and will only be given to select high-level users.

5.1.1.5 DBE Batch Security

To use DBE in batch runs, access I restricted by account, and can do so by performing the following steps under a DBE Master userid. The commands below will give a specific account and the functional users under this account batch access to DBE with update mode.

@DMS$0000*DBE.DBE,S
USAGE (Puts the user in DBE's command Language.)
C,B,<account> (Creates DBE batch account.)
A,B, <account>,U,A,I,D,N (Gives this account the U, A, I, D, and N options.)
EXIT <XMIT> (Writes information to the DBE Security File.)
EXIT <XMIT>

5.1.2 DBE with Enhanced Schema Security

SSO Montgomery has released a modified version of DBE. This version of DBE provides enhanced security mechanisms by limiting user access to specific functional AIS schemas under a particular ALN. Sites with the secured DBE will use the following procedures. Due to the power of this processor, access to it will be limited to high-level functional users. The functional AIS manager at each customer site will identify specific individuals as authorized DBE users. This will be done in a letter and will be done annually or upon any additions. This letter will be coordinated at the level specified in *Section 5.5.2.1, IQU and DBE Coordination – ALN*. After the site IAO has received the list of authorized users, permanent access will be granted. The IAO will retain the access request letters.

The site IAO will use the following procedures to set up the DBE security environment.

a. Restricting access by account is mandatory; further restriction by terminal-ID is optional, but not recommended.

b. Access to DBE without the update capability can be given freely, but access to the update capability within DBE will be restricted to high-level functional users.

c. The site IAO will maintain master update control in DBE.

Enhanced DBE :

- *(S103.320.00: CAT II) For DISA sites, the IAO will ensure access to DBE is restricted to specific functional AIS accounts and user access is documented in accordance with this STIG requirements.*

5.1.2.1 Initial Installation of DBE With Enhanced Schema Security

5.1.2.1.1 Installing the DBE Master Account

DBE with Enhanced Schema Security has one Master Account that will be used only by the Security Officer and other SIMAN Administrators. Sites using DBE with Enhanced Schema Security will use account 0000DA1A as the DBE Master Account. Install this account (if it does not already exist) by doing the following under the Master Account/Security Officer's userid.

```
@SIMAN,B
INSTALL ACCOUNT = 0000DA1A;
UPDATE ACCOUNT = 0000DA1A  PURGE USERS ;
```

Access to this DBE Master Account will be restricted to the Security Officer and SIMAN Administrators only. The 0000DA1A account will be set up in DBE with all of the options (M, U, A, I, D, and N).

Enhanced DBE :

- *(S103.360.00: CAT II) For DISA sites, the IAO will ensure sites using DBE with Enhanced Schema Security use account 0000DA1A as the DBE Master Account.*

- *(S103.370.00: CAT II) For DISA sites, the IAO will ensure access to the DBE Master Account is restricted to the Security Officer and SIMAN Administrators.*

5.1.2.1.2 Initializing the DBE$SEC File

When DBE with Enhanced Schema Security is genned, an initial default account of DBEGEN is identified. To initialize DBE security for the first time, the user has to be signed on under this account or 0000DA1A. The IAO will sign on to demand under 0000DA1A and accomplish the following steps.

```
@ASG,CP   DMS*DBE$SEC/SEC/SEC(+1).,F///128
@DMS*DBE.DBE,S
DBE 6R1C.7 2200/X00 L43 (RELEASE) (990316 0927:51) 990325 1950:35
-<120> INTERNAL ERROR: 000000000005 – REPORT PROBLEM
-<128> FAC WARNING: 000000100000 ON @ASG,A OF SYSTEM MACRO
    LIBRARY
-<16> FAC WARNING: 000000100000 ON @ASG,A OF HELP LIBRARY FILE
```

NOTE: The above error and warnings can only be seen the first time DBE is installed.

```
USAGE   (Puts the user in DBE's command Language.)
```

```
I,D              (Initializes demand security.)
I,S              (Initializes terminal/site security.)
I,B              (Initializes batch security.)
C,D,0000DA1A     (Creates DBE Master Account.)
A,D,0000DA1A,A,I,M,U,D,N  (Gives the DBE Master Account the A, I, M, U, D, and N
                           options.)
EXIT <XMIT>  (Writes information to the DBE Security File)
EXIT <XMIT>
```

After the DBE Master Account is installed , use SIMAN to delete the DBEGEN account from the account summary file if it was used during the initial installation.

Enhanced DBE :

- *(S103.350.00: CAT II) The IAO will ensure the default DBE installation account (DBEGEN) is not be active in the account file.*

5.1.2.2 DBE Restriction by Account

To set up DBE access restriction by account only, perform the following steps. To give each group of functional users access to DBE with update, the IAO will install their account internally using the following commands while signed on under 0000DA1A. ALN sites running DBE with Enhanced Schema Security will use the Z shred account structure to restrict DBE update capabilities. The only <ALN>DA1A account in the DBE$SEC file will be the Master Account 0000DA1A.

```
@DMS$0000*DBE.DBE,S
USAGE   (Puts the user in DBE's command Language.)
C,D,<ALN><AIS>1Z   (Creates DBE demand account.)
A,D, <ALN><AIS>1Z,U,A,I,D,N      (Gives this account the U, A, I, D, and N options.
                                  See note below.)
EXIT <XMIT>   (Writes information to the DBE Security File)
EXIT <XMIT>
```

NOTE: The U option allows updates and will only be given to select high-level functional users. This can be limited by installing an account that has a Z shred for functional users that need the update function (for example, 5401GV1Z). For users that do not need update capability, use a normal account (for example, 5300FS1A) and omit the U option.

Enhanced DBE :

- *(NA: CAT II) The IAO will ensure ALN sites running DBE with Enhanced Schema Security use the Z shred account structure to restrict DBE update capabilities.*

- *(S103.360.00: CAT II) For ALN sites, the SA will ensure the only <ALN>DA1A account in the DBE$SEC file is 0000DA1A.*

5.1.2.3 DBE Restriction by Account/Terminal-ID

To set up DBE access restriction by account and terminal-ID, perform the following steps while signed on under the DBE Master Account. This method is not recommended.

@DMS$0000*DBE.DBE,S
USAGE (Puts the user in DBE's command Language.)
C,D,<ALN><AIS>1Z (Creates DBE demand account.)
A,D, <ALN><AIS>1Z,I,D,N (Gives this account the I, D, and N options.)
C,S,<terminal-ID> (Creates DBE terminal-ID account.)
A,S,<terminal-ID>,I,U,D,N (See note.)
EXIT <XMIT> (Writes information to the DBE Security File.)
EXIT <XMIT>

NOTE: Notice that if the user wants to restrict access by both account and terminal-ID, The will not be set up in the DBE with the A option, as that will defeat the use of the terminal-ID security. The U option allows updates and will only be given to select high-level users. This can be accomplished by installing an account with a Z shred for functional users that need the update function (e.g., an account of 5401GV1Z).

5.1.2.4 DBE Batch Security

To use DBE in batch runs, restrict the access by account, and can do so by performing the following steps under the DBE Master Account. The commands below will give a specific account and the functional users under this account batch access to DBE with update mode.

@DMS$0000*DBE.DBE,S
USAGE (Puts you in DBE's command Language.)
C,B,<ALN><AIS>1Z (Creates DBE batch account.)
A,B,<ALN><AIS>1Z,U,A,I,D,N (Gives this account the U, A, I, D, and N options.)
EXIT <XMIT> (Writes information to the DBE Security File.)
EXIT <XMIT>

5.1.2.5 Schema Validation

Internal security for DBE consists of a table that verifies access to the schema based on the AIS code from the user's account. This verification is done anytime that a user attempts to perform the schema command within DBE. Any user that wishes to use DBE will be under a standard account for their system code. ALN restriction is still performed for any existing standard user account by the system security.

5.1.3 DBE Update Log Entries

DBE Log Entries are created for both Normal DBE and DBE with Enhanced Schema Security. If the user is given the 'U' option for update capability and executes the 'REWRITE PAGE' command, a message is displayed on the operator's console. This message is displayed on the first valid execution of the 'REWRITE PAGE' command that follows the 'SCHEMA' command.

For every successful 'REWRITE PAGE' command, the message is written to the system log file with the log file entry type 50069. The following is an example of the message that is displayed to the console:

```
RUNIDX*(0000)  UPDATES TO DATABASES ARE BEING APPLIED THRU DBE!!
RUNIDX*(0000)  UPDATES ARE AGAINST SCHEMA SBSS-SCHEMA FOR ALN 5401
RUNIDX*(0000)  AND ARE BEING APPLIED BY THIS RUN WITH ACCOUNT
      5401GV1Z
```

5.2 QLP with Update

5.2.1 General Requirements

SSO Montgomery releases QLP with Update to all ALN, and DFAS/IN (Indianapolis) sites on a separate release tape. This version of QLP with Update will execute out of the predefined file name UDS$$SRC*QLP-UPDATE. This version will not execute correctly from any other file and eliminates the possibility of multiple unauthorized versions of QLP with Update on the system. QLP with Update will not be combined with the standard QLP software product. If the QLP with Update capability is combined with the QLP Inquiry capability, then the entire SYSLIB*QLP file will be secured and this could have an adverse effect on end users who only need the QLP Inquiry capability. Contact SSO Montgomery for assistance if this situation applies to the site. QLP with Update will be secured and managed by the IAO. QLP with Update can be used against any functional database (excluding ALN overlay restrictions) and can be used across multiple application groups. However, updated database pages, including the userid that made the update, are written to the TIP audit trail. For these reasons, QLP with Update presents certain risks and will be limited to high-level functional users. The functional AIS manager at each customer site will identify specific individuals as authorized QLP with Update users. This will be done in a letter and will be done annually and upon any additions. This letter will be coordinated at the level specified in *Section 5.5.1, Access to QLP with Update*. After the site IAO has received the list of authorized users, permanent access will be granted. The method of making and validating a request for QLP with Update access is left to the discretion of the site IAO. Special access requests can be made in advance, as when a major AIS release is going to be loaded and access to QLP with Update may have to be extended to FAB, CDA, or MAJCOM representatives. The site IAO is responsible for keeping a log of users requiring temporary QLP with Update access that will include the name, office symbol, ALN, AIS, userid, and phone number of the person having the access. Temporary access log entries will be retained for at least one year.

- *(S103.276.00: CAT II) For DISA sites, The SA will ensure QLP with Update is not be combined with the standard QLP software product.*

- *(S103.280.00: CAT II) For DISA sites, The IAO will ensure access to QLP with Update is restricted and user access is documented in accordance with this STIG requirements.*

5.2.2 Securing QLP with Update

QLP with Update may be permanently installed on site systems as long as the file containing the processor (for example, UDS$$SRC*QLP-UPDATE.) is secured. The security officer will execute the following six-step process to ensure maximum protection for this processor. ALN domains will use the X shred account structure to secure QLP with Update. DNMC and DFAS-IN (Indianapolis) sites can use the X shred account structure or any application specific account, which is limited to a restricted number of authorized users. This procedure will allow QLP with Update to remain on the system and still restrict access to authorized users.

NOTE: If the file is owned, users with the Bypass Ownership Check privilege are unaffected by these security measures. Similarly, if the file is unowned, users with Bypass ACR Evaluation will be unaffected by these same security measures. No functional user will have either of these bypass privileges.

a. Create the QLP account. This is done only once.

```
@SIMAN,B
INSTALL ACCOUNT = <ALN><AIS>1X ;
```

NOTE: This account may already exist. If so, ignore the error and continue.

b. Create an ACR for the UDS$$SRC*QLP-UPDATE. file. If the ACR is already on the system, the ACR may need to be modified and additional functional user accounts added.

```
UPDATE ACCOUNT = <ALN><AIS>1X   PURGE USERS ;
```

and

```
INSTALL ACR = QLPWUP  OBJECT_ACCESS = EXECUTE
ACCESS_RESTRICTIONS = ACCOUNT EQ <ALN><AIS>1X ;
@EOF
```

or

```
UPDATE ACR = QLPWUP  OBJECT_ACCESS = EXECUTE
ACCESS_RESTRICTIONS = ACCOUNT EQ <ALN><AIS>1X ;
```

c. Save the security files to tape.

d. Copy the UDS$$SRC*QLP-UPDATE. tape to the UDS$$SRC*QLP-UPDATE. file on disk. Note that the modified version of QLP-UPDATE will only allow executions of the QLP with Update absolute from the file UDS$$SRC*QLP-UPDATE. It cannot be executed from a side file.

e. Secure the UDS$$SRC*QLP-UPDATE. file with the ACR that was created.

```
@SIMAN,B
UPDATE FILE = UDS$$SRC*QLP-UPDATE.
ATTACH_ACR = QLPWUP ACR_OWNER = <security officer's userid>  ;
@EOF
```

f. Give authorized users access to account <ALN><AIS>1X, as appropriate, when they are approved for QLP with Update. When the user signs on under this account, the UDS$$SRC*QLP-UPDATE. file may be accessed. This is normally done by using an account index. Once the user no longer needs permanent access to QLP with Update, remove the <ALN><AIS>1X account from the user's account index and remove their userid from the <ALN><AIS>1X account. Access to the file UDS$$SRC*QLP-UPDATE. is recorded in the system log file and Log Analyzer can be used to verify who has accessed the file.

- *(S103.280.00: CAT II) For DISA sites, the IAO will ensure ALN domains use the X shred account structure to secure QLP with Update.*

NOTE: DNMC and DFAS-IN (Indianapolis) sites can use the X shred account structure or any application specific account, which is limited to a restricted number of authorized users.

5.3 IQU

5.3.1 Securing IQU – ALN

SSO Montgomery has released a modified version of IQU to sites running the ALN operating system. This version of IQU uses IQU security groups to identify the specific schemas/subschemas that can be accessed by a particular user based on the AIS code in the user's account. This version of IQU also uses additional IQU security groups to restrict the use of certain IQU schema commands to a Y or Z shred account. Due to the power of this processor, access to restricted IQU schema commands will be limited to high-level functional users. The functional AIS manager at each customer site will identify specific individuals as authorized IQU schema command users. This will be done in a letter and will be redone annually and upon any additions. This letter will be coordinated at the level specified in *Section 5.5.2.1* IQU and DBE Coordination - ALN. After the site IAO has received the list of authorized users, permanent access to restricted IQU schema commands will be granted. The IAO will retain the access request letters.

ALN sites using the secured IQU will use the following procedures to set up userids that are authorized access to restricted IQU schema commands. Note that in order for a functional user to perform restricted IQU schema commands, his or her userid will have access to an account called <ALN><AIS>1Y or <ALN><AIS>1Z.

NOTE: Use of the <ALN><AIS>1Z account gives a user access to both the DBE and IQU processors. Modified security for IQU consists of software that verifies access to the schema based on the AIS code from the user's account. This verification is done anytime a user attempts to perform a command within IQU. Any user that wishes to

use IQU will be under a standard account for their system code. The ALN operating system still enforces ALN restriction for any existing standard user account. To prevent unauthorized access to multiple schemas under an ALN, the only <ALN>DA1A account authorized in the account summary file (ACCOUNT$R1) is the account 0000DA1A. Access to the 0000DA1A account will be restricted to the Security Officer and SIMAN Administrators.

For ALN:

- *(S103.260.00: CAT II) The IAO will ensure access to IQU is restricted and user access is documented in accordance with this STIG requirements.*
- *(S103.260.00: CAT II) The IAO will ensure ALN sites use the Y or Z shred account structure to control access to the secured version of IQU.*
- *(S103.270.00: CAT II) The IAO will ensure the 0000DA1A account is the only authorized <ALN>DA1A account in the account summary file.*
- *(S103.370.00: CAT II) The IAO will ensure access to the 0000DA1A account is restricted to the Security Officer and SIMAN Administrators.*

5.3.2 Securing IQU – DNMC

DNMC sites are not using a secured version of IQU so the site IAO will secure the IQU processor with an ACR or remove it from the system. The restrictions on the ACR used to limit access to IQU may be based on accounts or userids at the IAO's discretion. ACR object access must include *read* and *execute*. If the ACR restrictions are based on userids, then written procedures will be in place to update the ACR when a userid is disabled or deactivated (reference *Section 3.1.2.4,* Change in User Access Requirements*3.4.1.3.1* Userid). A user using the schema command in IQU can update any database in any application group on the system. However, all schema commands are logged in the TIP audit trail. Due to the power of this processor, access to it will be limited to high-level functional users. The functional AIS manager at each customer site will identify specific individuals as authorized IQU users. This will be done in a letter and will be redone annually and upon any additions. This letter will be coordinated at the level specified in *Section 5.5.3.1,* IQU, DBE, SYMCTL, RNCNT1, and EZLOAD – DFAS-IN. After the site IAO has received the list of authorized users, permanent access will be granted by giving these users access to the authorized accounts under the ACR or by adding these users to the list of authorized userids under the ACR. The IAO will retain the access request letters.

DNMC :

- *(S103.260.00: CAT II) The IAO will ensure access to IQU is restricted and user access is documented in accordance with this STIG requirements.*

5.4 LOUIS II/LOUIS LINK

LOUIS II/LOUIS LINK is a software tool designed to significantly increase productivity associated with the process of information access and retrieval. LOUIS II/LOUIS LINK is a licensed product and, at the present time, only the Defense Finance Accounting Service (DFAS) has purchased this product and only DFAS users are authorized to use it. Access to LOUIS II is controlled by a user having a userid entry in the LOUIS II Master File.

5.4.1 Securing LOUIS II/LOUIS LINK – ALN

SSO Montgomery has implemented ALN capabilities in this product so each Field Organization now has a separate LOUIS II Master File. This Master File is normally called 0QU0<ALN>*MASTER in the ALN environment. In addition, to support the ALN implementation and to prevent exempt users from executing LOUIS II without being properly validated by a Field Organization ALN LOUIS II/LOUIS LINK Master File, a default SDF Master File named 0QU09042*MASTER will exist on the system. This default SDF Master File contains a few process statements but no userid records unless site personnel are performing exempt inquiries to satisfy DFAS requirements. Access to the Field Organization ALN LOUIS II/LOUIS LINK Master file will be restricted to the respective Field Organization through the use of an ACR. Each ACR will be tailored for the appropriate Field Organization and the Field Organization System Administrators will identify those individuals who can satisfy the requirement of the ACR. The Field Organization System Administrators will notify the site IAO of authorized individuals via email. If requested by the Field Organization System Administrators, the respective Field Organization ACR can be set up with READ access set to PUBLIC. The Field Organization System Administrators will maintain and update their respective Field Organization ALN LOUIS II/LOUIS LINK Master File, to include adding authorized site userids to the file. To ensure the default Master File 0QU09042*MASTER is not inadvertently updated or deleted, this file will be protected by the ACR ACRRO that is owned by EXEC8.

If Field Organization workload coexists on a Unisys domain with other non-Field Organization ALNs, a default SDF non-Field Organization ALN Master File must exist on the system for each non-Field Organization ALN to prevent unauthorized users from accessing the LOUIS II/LOUIS LINK software. This default non-Field Organization ALN Master File(s), like the 0QU09042*MASTER file, will contain a few process statements but no userid records. To ensure the default non-Field Organization Master File(s) is not inadvertently updated or deleted, these files will be protected by the ACR ACRRO that is owned by EXEC8.

The following is an example of how to set up the appropriate ACR on one LOUIS Master file (0QU07704*MASTER) and will be performed using the Security Officer's userid. Each LOUIS Master file will be assigned a separate, unique ACR (e.g., LOUIS1, LOUIS2, etc.).

```
INSTALL ACR = LOUIS1  OBJECT_ACCESS = WRITE, DELETE
ACCESS_RESTRICTIONS = ACCOUNT EQ 7704BQ1L
OBJECT_ACCESS = READ ACCESS_RESTRICTIONS = PUBLIC ;
@EOF
```

or

UPDATE ACR = LOUIS1 OBJECT_ACCESS = WRITE, DELETE
ACCESS_RESTRICTIONS = ACCOUNT EQ 7704BQ1L
OBJECT_ACCESS = READ ACCESS_RESTRICTIONS = PUBLIC ;

@SIMAN,B
UPDATE FILE = 0QU07704*MASTER.
ATTACH_ACR = LOUIS1 ACR_OWNER = <security officer's userid> ;
@EOF

For ALN:

- *(S103.750.00: CAT II) The IAO will ensure access to each Field Organization ALN LOUIS II/LOUIS LINK Master file is restricted to the respective Field Organization through the use of an ACR.*
- *(S103.760.00: CAT II) The IAO will ensure the default Master File 0QU09042*MASTER exist on system.*
- *(S103.780.00: CAT II) The IAO will ensure the default Master File 0QU09042*MASTER is secured with ACR ACRRO to protect it from modification by unauthorized personnel.*
- *(S103.760.00: CAT II) The IAO will ensure default non-Field Organization Master Files exist on those systems where Field Organization workload coexists with non-Field Organization workload.*
- *(S103.770.00: CAT II) The IAO will ensure default non-Field Organization Master Files is secured with ACR ACRRO to protect them from modification by unauthorized personnel.*

5.4.2 Securing LOUIS II/LOUIS LINK – DFAS-IN

The LOUIS II/LOUIS LINK Master File is normally called <Qualifier>*MASTER in the DFAS-IN (Indianapolis) environment. Access to the LOUIS II/LOUIS LINK Master File will be restricted to the respective Application System Administrators through the use of an ACR. The Application System Administrators will maintain and update their respective LOUIS II/LOUIS LINK Master File, to include adding authorized site userids to the file. If requested by the Application System Administrators, the respective application ACR can be set up with *read* access set to PUBLIC. An example of how to install the ACR and attach the ACR to the LOUIS II/LOUIS LINK Master File is provided in *Section 5.4.1, Securing LOUIS II/LOUIS LINK – ALN.*

DFAS-IN (Indianapolis) :

- *(S103.750.00: CAT II) The IAO will ensure access to the LOUIS II/LOUIS LINK Master File is restricted to the respective Application System Administrators through the use of an ACR.*

5.5 Appropriate Coordination Level

5.5.1 Access to QLP with Update

5.5.1.1 QLP with Update Coordination – ALN

QLP with Update cannot be restricted to specific database schemas within an ALN. In order to grant permanent access to QLP with Update, each individual granted access to QLP with Update will place their signature on the QLP with Update request letter. This request letter will also be signed by an individual with the authority to accept the additional risks associated with the permanent access.

In the Air Force, the civilian and military personnel applications have migrated to consolidated platforms. Accounting and finance applications have consolidated to various Field Organizations. This leaves maintenance and supply as the primary online applications on the Air Force Unisys domains and the DFAS applications on the Field Organization Unisys domains. The appropriate level of authority to sign the QLP with Update request letter will be the data owner for the single functional application area (Chief of Supply, Chief of Maintenance, Field Organization Director, or the Commander of that particular organization). However, all functional areas with DMS databases within that particular ALN would have to coordinate on the request letter or the letter would have to acknowledge their coordination. This cross coordination on the letter itself can be accomplished by the primary OPR for a particular application or a senior enlisted representative, first level officer, or civilian equivalent (e.g., Superintendent, Supply RPS Room; Superintendent, Maintenance Database Managers; etc.). If the letter acknowledges the coordination, then the last paragraph of the request letter would reflect the office symbol of the Superintendent, Supply RPS Room; Superintendent, Maintenance Database Managers, etc.

Guard, reserve, or subordinate units could also be granted permanent access through this avenue. The guard, reserve, or subordinate unit would prepare and sign the access letter and then forward it through the host base for coordination with the other functional areas as indicated above or obtain the host base functional areas' coordination and indicate this fact on the letter before the letter is signed. The guard, reserve, or subordinate userids could also be listed on the host base functional area's letter.

The guidance implied here for all sites, including multiple gangs within an ALN, is that all functional areas potentially impacted by capabilities of QLP with Update, need to be made aware of and acknowledge the risks of another functional area using this processor. The site IAO would grant the final approval and letters will be redone annually when changes occur. Access requirements for QLP with Update apply to all users, including site personnel.

5.5.1.2 QLP with Update Coordination – DTIC and DFAS-IN

QLP with Update cannot be restricted to specific database schemas, cannot be restricted to specific application groups. In order to grant permanent access to QLP with Update, each individual granted access to QLP with Update will place their signature on the QLP with Update request letter. This request letter will also be signed by an individual with the authority to accept the additional risks associated with the permanent access.

The appropriate level of authority to sign the QLP with Update request letter will be the data owner for the single functional application area (e.g., DFAS-IN (Indianapolis) Director, DFAS-Cleveland Director, DIFMS Director, NIMMS Director, or the Commander of that particular organization). However, all functional areas with DMS databases on that particular domain would have to coordinate on the request letter or the letter would have to acknowledge their coordination. This cross coordination on the letter itself can be accomplished by the primary OPR for a particular application or a senior enlisted representative, first level officer, or civilian equivalent. If the letter acknowledges the coordination, then the last paragraph of the request letter would reflect the office symbol of the OPR. Subordinate units could also be granted permanent access through this avenue. The subordinate unit would prepare and sign the access letter and then forward it through the host application for coordination with the other functional areas as indicated above or obtain the host base functional areas' coordination and indicate this fact on the letter before the letter is signed. The subordinate userids could also be listed on the host application functional area's letter.

The guidance implied here is that all functional areas potentially impacted by capabilities of QLP with Update need to be made aware of and acknowledge the risks of another functional area using this processor. The site IAO would grant the final approval and letters will be redone annually when changes occur. Access requirements for QLP with Update apply to all users, including site personnel.

5.5.2 IQU, DBE, EZLOAD, and TERMRUN$ – ALN

5.5.2.1 IQU and DBE Coordination - ALN

The ALN versions of IQU and DBE, if set up correctly, will restrict functional users to their own functional database and ALN. To grant permanent access to IQU and DBE, a request letter only needs to be signed by the functional data owner for that particular application. The appropriate level of authority to sign the IQU or DBE request letter will be the data owner for the single functional application area (Chief of Supply, Chief of Maintenance, Field Organization Director, or the Commander of that particular organization). No cross-coordination with other functional areas is required, and the data owner can authorize (with proper justification) as many users as necessary. Guard, reserve, or subordinate units within the same functional AIS/ALN (including multiple gangs) could also be granted permanent access through this avenue. The guard, reserve, or subordinate unit would prepare and sign the access letter and then forward it through the host base for coordination with their counterpart functional area or obtain the host base functional area's coordination and indicate this fact on the letter before the letter is signed. The guard, reserve, or subordinate userids will also be listed on the host base functional area's letter. The

site IAO would grant the final approval and letters will be redone annually and when changes occur. Access requirements for IQU and DBE apply to all users, including site personnel.

5.5.2.2 EZLOAD and TERMRUN$ Coordination – ALN

EZLOAD can only be used to reload files under a particular user's ALN. TERMRUN$ allows a non-exempt user to access print files created by another user within his or her ALN by using the @SMOQ or @SQ processors. To grant permanent access to EZLOAD and TERMRUN$, a request letter only needs to be signed by a senior OPR for that particular application. The senior OPR for a particular application will be at least an E-7, O-2, or GS-11 (e.g., Superintendent, Supply RPS Room, Superintendent, Maintenance Database Managers, etc.). No cross-coordination with other functional areas is required, and the senior OPR can authorize, with proper justification, users as necessary. Guard, reserve, or subordinate units within the same functional AIS/ALN (including multiple gang) could also be granted permanent access through this avenue. The guard, reserve, or subordinate unit would prepare and sign the access letter and then forward it through the host base for coordination with their counterpart functional area or obtain the host base functional area's coordination and indicate this fact on the letter before the letter is signed. The guard, reserve, or subordinate userids will also be listed on the host base functional area's letter. The site IAO would grant the final approval and letters will be redone annually and when changes occur. If the EZLOAD and TERMRUN$ request letter is consolidated with either QLP with Update, DBE or IQU, the request letter will be signed and/or coordinated at a level that meets the requirements of the most powerful processor listed on the letter.

5.5.3 IQU, DBE, SYMCTL, RNCNT1, and EZLOAD – DFAS-IN

5.5.3.1 IQU, DBE, SYMCTL, and RNCNT1 Coordination – DFAS-IN

IQU and DBE with Normal Security cannot restrict authorized users to their own functional database or application group; however, database updates using these processors are logged in the TIP audit trail or the system log file. The SYMCTL keyin group with Full or Display CONS mode allows a user to move, delete, save, and restore all print files on the system. The RNCNT1 keyin group with Full or Display CONS mode allows a user to change the batch run limit, error jobs off, start jobs, remove jobs from backlog, and change the priority of a job, including deadlining a job. To grant permanent access to IQU, DBE, SYMCTL, or RNCNT1, a request letter only needs to be signed by the functional data owner for that particular application. The appropriate level of authority to sign the IQU, DBE, SYMCTL, or RNCNT1 request letter will be the data owner for the single functional application area (e.g., DFAS-IN (Indianapolis) Director, DFAS-Cleveland Director, DIFMS Director, NIMMS Director, or the Commander of that particular organization). No cross-coordination with other functional areas is required, and the data owner can authorize (with proper justification) as many users as necessary. Subordinate units within the same functional AIS could also be granted permanent access through this avenue. The subordinate unit would prepare and sign the access letter and then forward it through the "host" application for coordination with their counterpart functional area or obtain the host application functional area's coordination and indicate this fact on the letter before the letter is signed. The subordinate userids will also be listed on the host application functional area's letter. The site IAO would grant the final approval and letters will be redone annually and

when changes occur. Access requirements for IQU and DBE apply to all users, including site personnel.

5.5.3.2 EZLOAD Coordination – DFAS-IN

EZLOAD can only be used to reload files for a particular user. To grant permanent access to EZLOAD, a request letter only needs to be signed by a senior OPR for that particular application. The senior OPR for a particular application will be at least an E-7, O-2, or GS-11. No cross-coordination with other functional areas is required, and the senior OPR can authorize (with proper justification) as many users as necessary. The site IAO would grant the final approval and letters will be redone annually and when changes occur. If the EZLOAD request letter is consolidated with either QLP with Update, DBE, IQU, SYMCTL, or RNCNT1, the request letter will be signed and/or coordinated at a level that meets the requirements of the most powerful processor or keyin group listed on the letter.

5.6 Universal Repository Security

The implementation of Universal Repository (UREP) security allows Discretionary Access Control (DAC) over users, user-groups, or program groups based on access rules. Access rules can be described by privileges and permissions for different types of access by security groups. A security group is an entity that can be associated with rights to perform specific operations on other objects in UREP (entities, relationships, and attributes). Users can be grouped according to criteria such as roles, responsibilities, skills, and subject areas in an organization. Users can be members of several groups subject to control by one or more security administrators.

An access control list (ACL) is associated with each object. Each entry in an ACL defines all the access permissions of each security group (user, user group, or program group) for the associated object. Logically, every access control in an ACL entry has a GRANTED flag and a DENIED flag. Set/clear, clear/clear, and clear/set are valid values for the GRANTED/DENIED flags. Set/set is not valid and is not allowed. The security officer or SIMAN administrator will be the only userid authorized to grant or deny access permissions to other users, user groups, or program groups. This is accomplished by verifying that the Security Officer or SIMAN administrators are the only userids with execute rights in the STATIC-CONTEXT SECURITY ACL.

- *(S103.380.00: CAT II) The SA will ensure the Security Officer or SIMAN Administrator are the only userid allowed execute rights in the UREP Security Access Control List.*

5.6.1 Application Group Names

The following are application group names for ALN, DNMC, DFAS/IN (Indianapolis), and DTIC domains. This is the information needed when using UREP and other database utilities.

DOMAIN	APPLICATION	APPLICATION GROUP	APPLICATION NAME	UDS QUALIFIER
ALN	AF, DFAS, Default	1	APPL01	UDS$$SRC
DFAS-IN	PBAS	1	DMRP1	UDS$ONE
DFAS-IN	DTRS	2	DMRP2	UDS$$TWO
DFAS-IN	Validation	3	DMRV	UDS$$THR
DFAS-IN	System Test	4	DMRS	UDS$$FOR
DFAS-IN	Programmer Test	5	DMRT	UDS$$FIV
DFAS-IN	Default	6	APPSIX/UDSSRC	UDS$$SRC
DNMC	Default	3	UDSSRC	UDS$$SRC
DNMC	User	4	APPFOR	UDS$$FOR
DTIC	Default	3	UDSSRC	
DTIC		7	APPSVN	
DTIC		8	APPOCT	

Table 5-1. Application Group Names

5.6.2 Verifying UREP Security

To verify userids with execute rights on the ACL STATIC-CONTEXT SECURITY, do the following and replace the <application group name> with the appropriate information from *Table 5-1, Application Group Names*.

```
@DD,DE ,,<application group name>
REPORT SECURITY OFFICERS.        (The period is required)
@EOF
```

The screen should show the following:

```
** SECURITY OFFICER REPORT **
      USER SECOFF
```

If there is a userid other than the Security Officer's userid (for example, SECOFF or Master) or a SIMAN Administrator, then it will be necessary to update the information in the ACL STATIC-CONTEXT SECURITY.

5.6.3 Recovering the UDS$$SRC*UREP$ACL

a. To recover the UDS$$SRC*UREP$ACL file, a determination has to made as to when the unauthorized userid was granted execute rights to the STATIC-CONTEXT SECURITY ACL. If you have a valid UDSDMP for the system in question and this dump contains the correct Security Officer or SIMAN Administrator information, reload the UREP$ACL file from the dump tape.

NOTE: The UDSDMP must come from the system that one is trying to recover from. To reload the single UREP$ACL file, do the following:

```
@IRU,IEUX
DOWN FILE UDS$$SRC*UREP$ACL ; ACT ;
RELOAD FILE UDS$$SRC*UREP$ACL FROM REEL xxxxxx ; ACT ;
UP FILE UDS$$SRC*UREP$ACL ; ACT ;
```

Replace the xxxxxx with the reel number of the valid UDS$$SRC*DUMP$$01UNT1 tape and be sure to specify the correct application group. Once the UDS$$SRC*UREP$ACL file is loaded, accomplish a UDSDMP on that domain.

b. If the error is not a recent change or if UREP was not installed properly, reinitialize UREP security. Although the UREP Administration Guide (7830 8087) contains some appropriate information, contact SSO Montgomery or DISA Unisys Security Technicians for specific guidance.

5.6.4 Securing the UREP Configuration Entity with UREP User Groups

The following procedure will secure the Urep configuration entity. Though this procedure is assumming an ALN system it will be used with site appropriate changes by all sites. This will allow the granting of access to the configuration function for a specific entity to a user without granting other privileges normally granted a UREP Security Officer.

NOTE: The group name TECHSPT is suggested but non ALN sites may chose any name for the group.

1. Sign on with a userid that is a UREP Security Officers. If the user ID's that have this which userids have this capability, do the following:

```
@DD,DE
REPORT SECURITY OFFICERS.
@EOF
```

2. Once the user has signed on with the correct userid, the following procedures can be used to security the UREP Configuration Entity such as ALN or CONFIG-1.

```
@DD,DE ,,<application group name>                    . Such as APPL01, DMRP1
ENTER SECURITY MODE.
```

```
CREATE USER-GROUP TECHSPT.
ENROLL USER GADA04, SECOFF, GAJZTF IN TECHSPT.
GET ACL FOR STATIC-CONTEXT PROCESS-CONFIGURATION.
CLEAR GRANT OF EXECUTE FOR USER-GROUP ALL-USERS.
SET GRANT OF EXECUTE FOR USER-GROUP TECHSPT.
REPORT ACL.
RETURN ACL.
GET ACL FOR CONFIGURATION ALN.          . Replace with correct config
CLEAR ACL.
SET GRANT OF APPEND-LINKS, CONTROL-DISCRETIONARY, <xmit>
CREATE, DELETE, EXECUTE, NAVIGATE, READ-ATTRIBUTES, <xmit>
READ-LINKS, WRITE-ATTRIBUTES, WRITE-LINKS FOR <xmit>
USER-GROUP TECHSPT.
SET GRANT OF NAVIGATE, READ-ATTRIBUTES, READ-LINKS <xmit>
FOR USER-GROUP ALL-USERS.
REPORT ACL.
RETURN ACL.
LEAVE SECURITY MODE.
EXIT.
```

3. If the site has multiple application groups, follow the above commands for each application group and/or configuration entity within an application group. Do not perform these commands for the configuration entity RELEASE unless the user is actually using this as the active configuration (for example, DFAS-IN Application Group 6).

4. The enroll of userids into the group TECHSPT must be performed by a user who is a UREP security officer and enrolled in the TECHSPT group. By default, the userid who creates the user group is automatically enrolled in the group. The enrolled userids will be limited to authorized DECC/SMC Technical Support personnel. To view the list of userids in the group, perform the following:

```
@BK1
@DD,DE
ENTER SECURITY MODE.
REPORT IMPACT USER-GROUP TECHSPT.
LEAVE SECURITY MODE.
@BK2,E
```

5. A user who is enrolled in the user group TECHSPT must adopt the user group one time. To adopt a user group, a user must perform the following command:

```
@DD,DE
ADOPT TECHSPT.
@EOF
```

Once a user group is adopted, it does not have to be performed again unless the userid is revoked from the user group via the following command:

```
@DD,DE
ENTER SECURITY MODE.
REVOKE USER GADA04 IN TECHSPT.
LEAVE SECURITY MODE.
@EOF
```

NOTE: Do not revoke the last UREP security officer from a user-group or no one will be able to update the group. If this occurs, the documentation indicates the user group can be deleted and re-created.

- *(N/A: CAT II) The SA will ensure user groups are used if there is a need for a user other than the Security Officer or IAO to access the configuration functions of UREP.*

6. MASS STORAGE MANAGEMENT UTILITIES

6.1 File Administration System

The File Administration System (FAS) implements all Unisys Operating System MAC and DAC security mechanisms inherent in the Unisys Operating System file system. In cases where local code has been added to the Executive, such as ALN, the responsible vendor or software developer will assume responsibility for ensuring these changes do not circumvent or weaken the mechanisms already in place.

6.2 EZLOAD

EZLOAD is a utility developed by SSO Montgomery.

6.2.1 EZLOAD – ALN

EZLOAD (and FAS, which EZLOAD uses to actually load files) was modified to eliminate a security vulnerability that allowed non-exempt users to access files belonging to a different ALN. Another security change was to replace the link to the Interface TERMRUN$ with a link to SSAGNAME instead. Under the new EZLOAD, a user needs to have the Privilege SSAGNAME in order to bypass EZLOAD security and get directly to the EZLOAD ACCESS screen. SSAGNAME is only given to Profile 1 users and the System Standard Batch userids. Since only SIMAN Administrators and the Master userid will be assigned Profile 1 userids, this ensures that the EZLOAD ACCESS screen will be secure from unauthorized access. Even with these changes, users with EZLOAD access can still load files belonging to another AIS within their ALN, so access to EZLOAD will be restricted to relatively high-level functional users. The site IAO will make the actual updates to the EZLOAD access database. The functional data owner will submit requests for EZLOAD access to the IAO. Each access request will be redone annually and as changes occur. The request for EZLOAD access will be accomplished and coordinated at the level specified in *Section 5.5.2.2, EZLOAD and TERMRUN$ Coordination – ALN*. After the site IAO has received the list of authorized users, permanent access will be granted. The IAO will retain a copy of the access request letters. Access to EZLOAD by site users will be documented on the individual's SAAR.

For ALN:

- *(S104.610.00: CAT II) For sites using EZLOAD the SA will ensure only the Master userid, SIMAN Administrators, and System Standard Batch userids have access to the SSAGNAME privilege.*

- *(S103.390.00: CAT II) The IAO will ensure users do not have access to the EZLOAD processor without proper justification and documentation.*

6.2.2 EZLOAD – DFAS-IN

DNMC and DFAS-IN (Indianapolis) sites can allow authorized users to use EZLOAD (and FAS, which EZLOAD uses to actually load files) to reload files on the system. With this version of EZLOAD, a user needs to have the Privilege SSAGNAME in order to bypass EZLOAD security and get directly to the EZLOAD ACCESS screen. SSAGNAME is only given to Profile 1 users and the System Standard Batch userids. Since only SIMAN Administrators and the Master userid will be assigned Profile 1 userids, this ensures that the EZLOAD ACCESS screen will be secure from unauthorized access. Even with this change, users with EZLOAD access can still load files belonging to another AIS, so access to EZLOAD will be restricted to relatively high-level functional users. The site IAO will make the actual updates to the EZLOAD access database. The functional data owner will submit requests for EZLOAD access to the IAO. Each access request will be redone annually and as changes occur. The request for EZLOAD access will be accomplished and coordinated at the level specified in *Section 5.5.3.2, EZLOAD Coordination – DNMC and DFAS-IN (Indianapolis))*. After the site IAO has received the list of authorized users, permanent access will be granted. The IAO will retain a copy of the access request letters. Access to EZLOAD by site users will be documented on the individual's SAAR.

DNMC and DFAS-IN (Indianapolis):

- *(S104.610.00: CAT II) For sites using EZLOAD, the SA will ensure only the Master userid, SIMAN Administrators, and System Standard Batch userids have access to the SSAGNAME privilege.*

- *(S103.390.00: CAT II) The IAO will ensure users do not have access to the EZLOAD processor without proper justification and documentation.*

6.3 DSKUTL

DSKUTL is a utility, developed by SSO Montgomery, that is designed to help DataBase Managers (DBMs) perform disk management. Executive requests mandate that a user has to be in Privileged mode (@SYSLIB*COMUS.CLOD,A) to get accurate data from DSKUTL. In order to go Privileged, a user needs to have MODPS$, which is a Profile 4 or higher Interface. The MODPS$ Interface will be restricted to site personnel. To perform certain functions in DSKUTL (e.g., options D(elete) and S(quash)), the MSCON$, DREG, and DBACK Privileges are required. The risk inherent with using these options is reduced since these are Profile 2 and 4 Privileges and, in order to use all these options, the user needs to be a Profile 2 or 1. DSKUTL will determine this beforehand to prevent unauthorized users from deleting or squashing files. To obtain more information on DSKUTL, do an @DSKUTL,H in Demand mode. This will pull up a help menu that is very informative.

- *(S104.440.00: CAT I) The SA will ensure users do not have access to the MODPS$ Executive Interface unless it is authorized for their security profile.*

6.4 FSMFD

There is a Full Screen Master File Directory (FSMFD) processor, developed by SSO Montgomery, which allows the user to quickly retrieve information on all disk files. It allows the user to choose what files to display and how to sort the information that is displayed. Information can be reviewed and/or saved to a disk file by using the SELECT option. This allows the user to use the same MFD snapshot to view information on other files using different select criteria. After the user gets out of the processor, if an @FREEALL has not been done, the user can re-execute the processor using the @FSMFD,R option and save a little time by using the same snapshot of the system disk files. The processor call is @FSMFD.

This page is intentionally left blank.

7. TAPE MANAGEMENT/AUTOMATED CARTRIDGE SILO UTILITIES

7.1 File Administration System

The File Administration System (FAS) implements all Unisys Operating System MAC and DAC security mechanisms inherent in the Unisys Operating System file system. In cases where local code has been added to the Executive, such as ALN, the responsible vendor or software developer will assume responsibility for ensuring these changes do not circumvent or weaken the mechanisms already in place.

FAS can be used to retrieve information from the MFD on catalogued tape files. Reference 7830 7972, FAS Operations Guide, for more information on using the FAS processor.

7.2 STAR Level 7R1 or Higher

7.2.1 Overview

The System for Tape Administration and Reporting (STAR) is a commercial product that provides automated tape management capabilities. Features include tape inventory, scratch and clean functions, vault management for off-site purposes, an interface with automated cartridge systems (robotic silos), and a variety of management reports. The STAR environment, when properly configured, will not allow personnel to access or modify tapes outside of their application. STAR uses two databases. The SYS$*TIF is the primary database and the SYS$*TIFF is used as a backup for recovery purposes. These databases are G-option files (guarded) and are not saved during a normal SAVE/SAVALL process. For this reason, the STAR database will be saved daily and a copy of the STAR save tape will be kept off-site. For sites running the Shared Library System (SLS), only the Master STAR database needs to be saved to tape daily and a copy of the Master STAR save tape will be kept off-site.

- *(S103.510.00: CAT II) The SA will ensure the tape management system environment does not allow personnel to access or modify tapes outside of their application group.*

7.2.2 STRUTIL

The STRUTIL processor can be used to determine the STAR privileged owner code by displaying Page Zero of the STAR database. Having this privileged owner code allows a user to bypass the ownership check on tapes and allows him/her to manipulate items, such as the scratch flag, on all tapes in the database. However, a user needs to have access to the MODPS$ Interface (privilege 4 or higher) and has to go into privileged mode to execute this processor and obtain the STAR privileged owner code. For this reason, the MODPS$ Interface will be restricted to site personnel only.

- *(S104.440.00: CAT II) The SA will ensure users do not have access to the MODPS$ Executive Interface unless it is authorized for their security profile.*

7.2.3 Media Manager Privileges

The SSMMGRILES1, SSMMGRILES2, SSMMGRILES3 and SSMMGRBYPASS Privileges will be restricted as outlined in *Section 3.1.8.5, Media Manager Privileges*, as they allow users additional access to the TIF database and/or non-STAR managed tapes.

- *(S104.510.00: CAT II) The SA will ensure users do not have access to the standalone SSMMGRILES2 privilege.*
- *(S104.500.00: CAT II) The SA will ensure users do not have access to the standalone SSMMGRILES3 privilege unless it is authorized for their security profile.*
- *(S104.520.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES2 privileges unless this combination is authorized for their security profile.*
- *(S104.530.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*
- *(S104.540.00: CAT II) The SA will ensure users do not have access to both SSMMGRILES2 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*
- *(S104.550.00: CAT II) The SA will ensure users do not have access to SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges unless this combination is authorized for their security profile.*
- *(S104.560.00: CAT I) The SA will ensure users do not have access to SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRBYPASS privileges unless this combination is authorized for their security profile.*
- *(S104.490.00: CAT II) The SA will ensure users do not have access to the SSMMGRBYPASS privilege unless it is authorized for their security profile.*

7.2.4 STAR BYPASS Messages

In the STAR Page Zero, the BYPASS value determines how a userid is verified when bypassing STAR validation checks. Based on this value, STAR will allow, deny, or prompt the operator for concurrence when any user attempts to bypass STAR validation checks. On ALN, DFAS-IN (Indianapolis) systems, this prompt for concurrence will be done whenever a user tries to write to a scratch tape, bypassing STAR, or whenever a user tries to read any tape (scratch or non-scratch), bypassing STAR. To ensure this occurs, the STAR BYPASS value on ALN systems will be changed from its current value of octal 013 (decimal 11) to octal 014 (decimal 12). On DNMC systems, the ability to bypass STAR is completely controlled by the SSMMGRBYPASS privilege. To ensure this is successfully accomplished on all read attempts and write actions, the STAR BYPASS value will be changed from its current value of decimal 3 to decimal 4 or octal

014 (decimal 12). Refer to the STAR documentation for information on implementing this change to the Page Zero BYPASS field.

7.2.4.1 Output Tape Bypass Messages

On a normal basis, requests to bypass STAR on output tapes will be answered with an N. To ensure this is done, configure the SMART AMS database to automatically answer the Y/N console messages that are generated when a user assigns an output tape and tries to bypass STAR. Contact the site's local administrator for SMART Console to ensure that these messages are being answered automatically with an "N." If these requests are not automatically answered with SMART AMS, then the operations staff will be properly trained to answer these prompts with an N. Exceptions to bypassing output tapes will be documented and justified, and the IAO will have a copy of this documentation on file. It is also acceptable for a site to develop a routine to handle output tape bypass requests. However, this routine will be automated and update STAR with the userid/run-ID bypassing STAR, reel number of tape, date/time stamp of the BYPASS request, and a reasonable tape retention code.

7.2.4.2 Input Tape Bypass Messages

On a normal basis, requests to bypass STAR on input tapes will be answered with an N. To ensure this is done, configure the SMART AMS database to automatically answer the Y/N console messages that are generated when a user assigns an input tape and tries to bypass STAR. Contact the local administrator for SMART Console to ensure that these messages are being answered automatically with an N. If these requests are not automatically answered with SMART AMS, then the Operations staff will be properly trained to answer these prompts with an N.

Exceptions to bypassing input tapes will be documented and justified, and the IAO will keep a copy of this documentation on file.

- *(N/A: CAT II) The SA will ensure the STAR BYPASS value on non ALN systems is set to octal 004 (decimal 4).*
- *(S104.510.00: CAT II) The SA will ensure the STAR BYPASS value on ALN DFAS-IN (Indianapolis) systems is set to octal 014 (decimal 12).*
- *(S104.510.00: CAT II) The SA will ensure the STAR BYPASS value on DNMC systems is set to decimal 4 or octal 014 (decimal 12).*
- *(S103.140.00: CAT II) The IAO will ensure tape Bypass console messages are answered correctly.*

7.3 Shared Library System

Shared Library System (SLS) allows multiple hosts to share a STAR TIF as well as physical tape hardware. In this configuration, each host has update access to the global Master TIF (comprised of the union of all hosts' local TIFs). Thus, if STAR is compromised on one host, it is effectively compromised on ALL hosts. Because of the inherent vulnerabilities in SLS, it is critical that all hosts' copies of STAR are restricted as outlined in *Section 7.2.2, STRUTIL*.
If a site is using SLS, the site can use the vault parameter file of the Master TIF for the Vault Management System (VMS), or use each domain's vault parameter file for VMS activities.

If a site elects to use the vault parameter file of the Master TIF for VMS, then the following parameters will need to be modified. If these changes are not accomplished, critical files will not be correctly identified for off-site storage.

a. On DNMC systems, the MCYCLE parameter in the vault parameter file on the Master TIF host will be set to 0 (FALSE).

b. On ALN systems, the MCYCLE parameter in the VMSRUN element that is located on the Master TIF host will be set to 0 (FALSE).

NOTE: The VMSRUN element is located in SYSLIB*RUN$ and SYSLIB*STAR.

If a site elects to use the vault parameter file from each domain, then the following changes will need to be made. If these changes are not accomplished, critical files will not be correctly identified for off-site storage.

a. On DNMC systems, the MCYCLE parameter in the vault parameter file on all hosts will be set to 1 (TRUE).

b. On ALN systems, the MCYCLE parameter in the VMSRUN element that is located on all hosts will be set to 1 (TRUE).

NOTE: The VMSRUN element is located in SYSLIB*RUN$ and SYSLIB*STAR.

- *(S103.540.00: CAT II) The SA will ensure sites running SLS set the VMS MCYCLE parameter to the proper value to ensure critical files are correctly identified for off-site storage.*

7.4 Automated Cartridge Silo Utilities

The Client System Component (CSC) and Client Direct Interconnect (CDI) software provide an interface between the Unisys ClearPath domains and the Automated Cartridge Silo system. Although the operator's console is the primary interface to CSC and CDI, a demand terminal provides a secondary interface to these software utilities. To limit the CSC and CDI commands that can be executed from a demand terminal, default demand terminal security features are established during the installation of the CSC and CDI software. A userid needs to have a specific level of CONS mode to execute CSC and CDI commands from a demand terminal.

These demand terminal security features can be further restricted or controlled by setting up Security Level (SEC_LEVEL) statements in the CSC and CDI parameter files. Since these parameter files can be used to override existing demand terminal security features, the files containing these elements will be protected. The CSC parameter file is CSC$PARAM and the CDI parameter file is CDI$PARAM. On ALN and DFAS-IN systems, the CSC$PARAM element is located in SYSLIB*CSC and the CDI$PARAM element is located in SYSLIB*STRPARM.

- *(S103.810.00: CAT II) The SA will ensure the file(s) containing the CSC and CDI parameter elements are secured with the ACR ACRRO to protect them from modification by unauthorized personnel.*

7.4.1 CSC and CDI Default Demand Terminal Security

The default demand terminal security features for CSC and CDI commands are listed below. The numbers listed below determine the level of CONS mode. These default security features can only be overridden by SEC_LEVEL statements in the CSC$PARAM or CDI$PARAM elements.

1 = Basic CONS
2 = Limited CONS
3 = Full CONS
4 = Display CONS
5 = Response CONS
6 = System Console

Defaults (unless overridden by CDI$PARAM or CSC$PARAM):

For CSC 4R1

	CSC	CDI
1 or higher	HELP, LEVEL, MEMORY, QUEUES, STATUS	BUFFER, FLAGS, FS, HELP, ID, STATUS
3 or higher	N/A	PING
5 or higher	ABORT, ACTIVATE, BRKPT, CLEAR, CYCLE, DEBUG, DISMOUNT, DOWN, EABT, EJECT, ENTER, MOUNT, QUERY, TERM, UP, VENTER	BRKPT, CLR, DN, DUMP, SET, TCP, TERM, UP

7.4.2 ALN, DFAS-IN CSC Parameter File

The following security parameter is authorized and overrides the default demand terminal security features. If mission requirements dictate a change, this will be coordinated and approved by the responsible site IAO.

For CSC level 4R1, SEC_LEVEL_4 statement will be.

SEC_LEVEL_4 QUERY,EJECT,ENTER,MOUNT,DISMOUNT

7.4.3 CDI Parameter File

All DOD Unisys domains will use the CDI default demand terminal security features. No SEC_LEVEL statements are included in the CDI$PARAM parameter file. If mission requirements dictate a change, this will be coordinated and approved by the responsible site IAO.

- *(S103.530.00: CAT II) The SA will ensure the CDI parameter file is not modified from the settings specified in this STIG that are the system default settings.*

8. SYSTEM PROCESSORS

8.1 QuickStart

8.1.1 Overview

Originally developed for ALN systems by SSO Montgomery, QuickStart is available to all Unisys users in DOD. Contact SSO Montgomery for more information on this product. QuickStart is part of the NJZMON processor. The QuickStart product provides a more secure way for end users to perform CONS keyins without having to have access to the actual CONS keyin group. With QuickStart running (NJZMON), a user can still perform necessary keyins within a group while being locked out of dangerous or detrimental keyins within the same group. For instance, even if a user has no access to the RNCNT1 keyin group, the user may still E off a job using the QuickStart RKY E keyin rather than the @@CONS E keyin. If users abuse this function, the operator may disallow the RKY E keyin, without affecting other aspects of the QuickStart software.

QUICKSTART KEYIN	*DESCRIPTION*
RQ	Redirects print.
RKY RM <run-id>	Removes specified run-ID from backlog.
RKY CS <run-id>*<command>	Changes status of run-ID (start time or priority)
D*	Returns local time
RKY E <run-id>	Errors run-ID
RKY SM xxxxxx T	Terminates terminal id xxxxx
RKY TM	Sends a terminal message to a user
RKY TP T	Displays active TIP transactions
RKY TP RC *<TIP transaction>	Performs a run check on a particular TIP transaction
RKY T,B <ALN or ELC>	Limits display of the T,B keyin to only the specified ALN or ELC.

Table 8-1. QuickStart Console Keyins

The QuickStart editor controls access to the QuickStart database. The QuickStart database is used to store information concerning batch jobs. Once a batch job is entered into the database, it can be executed through a 'QS <run-id>' keyin. If a user has access to this database, he or she could insert a job that runs at a high privilege level with someone else's userid. To prevent this, QuickStart will be secured.

NOTE: The RKY SM xxxxxx T cannot be used to terminate Demand RSI or FTP terminal-IDs that begin with a G and contains all numeric characters. For example, G00001.

8.1.2 QuickStart Security

Perform the following steps to secure the QuickStart database.

a. Inspect the QuickStart database annually for any suspicious/unauthorized jobs that someone may have added. Check the actual ECL started from QuickStart to see if it is malicious. Undo any damage done by this ECL as required.

b. Secure the QuickStart database. There is a system ACR that will be used to secure the database file.

```
@SIMAN,B
UPDATE FILE = SYS$*QRUNS.
ATTACH_ACR = ACRNA          ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYS$*QRUNS. ;
```

This will attach ACRNA (no access) to the SYS$*QRUNS file. It will then display the file. The file will show the ACR attached. The only users that may update or view the database are those with ACR bypass privileges (site personnel).

- *(S103.740.00: CAT II) The SA will ensure the QUICKSTART file SYS$*QRUNS is secured with ACR ACRNA to protect it from access by unauthorized personnel.*

8.2 Automated Security Programs

SSO Montgomery has released several automated security programs that allow authorized IAOs and TASOs to reset passwords and enable userids that are under their control and an automated account program that allows authorized IAOs to enter userids under non-restricted accounts. Access to these programs and/or related files will be restricted to specific TASO accounts and/or ACRs that are restricted to specific IAO accounts.

8.2.1 Automated Reset Process Program

The Automated Reset Process (ARP) program provides the IAO and TASO in the field with the means to update a user's password and enable a userid while still maintaining a secure environment. The way the ARP process works is an authorized TASO under a particular ALN needs to have a user's password reset and the userid needs to be enabled because the user entered an erroneous password three times. The TASO signs on with his ALN Q-shred account and executes the RESET program (which should be located in SYSLIB*ALTLIB). The RESET program accepts or rejects a request to reset a userid based upon whether the TASO's account contains a Q-shred in position 8 of the account. The RESET program also reads the TASO's account to determine what ALN and AIS Code is being used. Based on the AIS code, the RESET program sends certain messages to the operator's console, which are acted upon by AMS. First, AMS will QS the appropriate job in Quick Start. If the TASO is a non-Supply TASO, the job in Quick Start is set up so it is started by the site's IAO userid. If the TASO is a Supply TASO and a Regional Supply Squadron (RSS) supports the site, the job in Quick Start is

set up so it is started with the RSS IAO userid. Next, based on output from the RESET program, AMS will return messages to the TASO's terminal informing the TASO of how many userids were reset, start/finish of reset, and error messages, if appropriate. The RESET program uses only temporary files so ACR file protection is not required.

All TASOs utilizing the ARP program will verify the identity of userids being entered against the individual's SAAR. The IAOs will verify that only authorized TASOs have access to the Q shred AIS accounts. The site IAOs will maintain a list or documentation of authorized TASOs who have access to the ARP program. This list will contain the TASO's name, userid, organization, phone number, and authorized Q shred AIS account.

- *(S103.850.00: CAT II) The SA will ensure only authorized TASOs and SAs have access to the respective Q shred accounts.*

- *(S103.854.00: CAT II) IAOs will maintain a list of authorized TASOs who have access to the ARP program.*

NOTE: This list will contain the TASO's name, userid, organization, phone number, and authorized Q shred AIS account.

8.2.1.1 DFAS ARP Program

SSO Montgomery has released the DFAS ARP program, which is similar to the ARP program and provides the DFAS Field Organization and Air Force TASOs with the means to update a user's password and enable a userid while still maintaining a secure environment. The way the DFAS ARP process works is based on where the TASO is located. If the TASO is an individual at an Air Force organization, which is supported by a DFAS Field Organization, the TASO can only reset userids that have the same site code as the TASO. If the TASO is an individual at a DFAS Field Organization, the TASO can reset any userid for the sites that are supported by that respective Field Organization.

An authorized Air Force TASO must sign on with his ALN Q-shred and Site Code account to execute the DESET program (which should be in SYSLIB*ALTLIB). The DESET program accepts or rejects a request to reset a userid based upon whether the TASO's account contains a Q-shred in position 8 of the account. The DESET program also reads the TASO's account to determine what ALN and Site Code is being used. The DESET program also sends certain messages to the operators console which are acted upon by AMS. AMS will start the appropriate 0JX0<ALN>*PUTLD.DESET runstream with the respective Field Organization's IAO userid and JX Q-Shred Account. Since an Air Force TASO rather than a Field Organization TASO executed the DESET program, the DESET runstream only allows userids that match the Air Force TASO's Site Code to be updated through SIMAN. Finally, based on output from the DESET runstream, AMS will return messages to the TASO's terminal informing the TASO of how many userids were reset, start/finish of reset, and error messages, if appropriate.

An authorized DFAS Field Organization TASO must sign on with his ALN Q-shred and DFAS Site Code account to execute the DESET program. The DESET program accepts or rejects a request to reset a userid based upon whether the TASO's account contains a Q-shred in position

8 of the account. The DESET program also reads the TASO's account to determine what ALN and DFAS Site Code is being used. The DESET program also sends certain messages to the operators console which are acted upon by AMS. AMS will start the appropriate 0JX0<ALN>*PUTLD.DESET runstream with the respective Field Organization's IAO userid and JX Q-Shred Account. Since the Field Organization TASO executed the DESET program, all userids at the sites that are supported by the respective DFAS Field Organization (owned by the Field Organization IAO) will be updated through SIMAN. Finally, based on output from the DESET runstream, AMS will return messages to the TASO's terminal informing the TASO of how many userids were reset, start/finish of reset, and error messages, if appropriate.

To support the DFAS ARP program, SSO Montgomery released a DESET runstream, which is located in file 0JX0<ALN>*PUTLD and updated by the Field Organization IAO. This file containing this DFAS ARP IAO runstream will be protected with an ACR that is restricted to a Q shred account that is only accessible to the respective Field Organization IAO. All TASOs utilizing the DFAS ARP program will verify the identity of userids being entered against the individual's SAAR. The Field Organization IAOs will verify that only authorized TASOs have access to the Q shred AIS and Site Code accounts. The site IAOs or Field Organization IAOs will maintain a list or documentation of authorized TASOs who have access to the DFAS ARP program. This list will contain the TASO's name, userid, organization, phone number, and authorized Q shred AIS and Site Code account.

- *(S103.856.00: CAT II) The SA will ensure the file containing the DFAS ARP IAO runstream is controlled by an ACR is restricted to the appropriate IAO Q shred account.*

- *(S103.850.00: CAT II) The SA will ensure only authorized TASOs and IAOs have access to the respective Q shred accounts.*

- *(S103.854.00: CAT II) Field Organization IAOs will maintain a list of authorized TASOs who have access to the DFAS ARP program.*

NOTE: This list will contain the TASO's name, userid, organization, phone number, and authorized Q shred AIS and Site Code account.

8.2.2 Automated Account Process Program

SSO Montgomery released an Automated Account Process (AAP), which relied on ECL, IPF, and SSG routines and ACR protected IAO files to process. The sites have further refined and automated this process with locally developed programs. SSO Montgomery is in the process of releasing an updated AAP program that will use temporary files, automated checks for restricted accounts, and eliminate some of the cumbersome routines that are in place today.

If a site is using any AAP program or process, IAO input and/or output files will be protected from unauthorized access through the use of ACRs. These ACRs will be restricted to specific accounts that are only accessible by authorized IAOs. If the AAP program or process uses files that contain sensitive information, these files will be protected from unauthorized access through the use of ACRs.

- *(S103.830.00: CAT II) The SA will ensure the AAP IAO files are secured with an ACR to protect them from access by unauthorized personnel.*

- *(S103.840.00: CAT II) The SA will ensure only authorized IAOs have access to their respective AAP IAO files.*

8.3 FTP and Telnet

For the pulpous of Unisys systems telnet will include Unisys legacy terminal emulation over TCP/IP.

Under certain circumstances the use of FTP and telnet may be the only viable solution (primarily due to legacy applications); however, the use of FTP and telnet is not a recommended best practice. The use of clear text transmission will be phased out as quickly as possible and the use of encrypted sessions will be implemented in the architecture. The use of an encrypted session is required if supported by the device.

- *(N/A: CAT: II) The IAO will ensure if encryption protocols such as SSL or SSH transmit traffic directly to a host, a host based intrusion detection (HID) system is employed on the device if supported.*

- *(N/A: CAT: II) The IAO will ensure all network traffic is visible to an Intrusion Detection System (IDS). VPN traffic does not bypass the security architecture and must terminate in order for the traffic to be processed by a network IDS (NID).*

FTP and telnet are permissible inside an enclave, behind the premise router and protected by a firewall and router access control lists (ACLs); however, the requirement must be documented and maintained by the Information Assurance Officer (IAO). If either of these services is not required, the service will be deleted, disabled, or turned off. If the service is disabled or turned off, the site will continue to ensure that all appropriate patches are applied. When used, all associated traffic will be restricted by IP source and destination address if technically feasible, and other mitigating controls as required by the appropriate STIG will be enforced.

- *(N/A: CAT I) The IAO will ensure FTP and telnet from outside the enclave into the enclave is not permitted, unless encrypted and the following conditions apply:*

  FTP and telnet are acceptable from outside the enclave through a remote access Virtual Private Network (VPN). The connection will terminate outside the firewall as to not bypass the security architecture. The connection will be proxied at the firewall or via an FTP/telnet proxy.

  FTP and telnet are acceptable via a site-to-site VPN between trusted enclaves; however, an Acknowledgement of Risk letter (AORL) must already be in place for the tunnel. FTP and telnet are acceptable within distributed enclaves, if required, as long as the traffic is physically or logically segregated from normal traffic using a method supported by the network technology to create a virtual connection (e.g., VLAN, VPN, LANE, MPLS, IPSec tunnels).

In addition to the data transmission being in the clear, the user credentials are also passed in the clear, which violates the DOD 8500.2, IA Control IAIA-1. As mitigation for this vulnerability, special consideration must be given to account maintenance and the types of user privileges associated with these accounts.

- *(N/A: CAT II) The IAO will ensure all user FTP userid (UID) passwords have an expiration date and the password is changed every 90 days.*

- *(N/A: CAT: I) The IAO will ensure under no circumstances the FTP or telnet is used with a userid (UID)/password has administrative or root privileges.*

System-to-system FTP accounts (no user intervention) may be treated as an application-type account and the password will be changed at least once a year or when an administrator with knowledge of the password leaves. A system-to-system FTP account is defined as an account that a human never logs on to. It is only used for authentication of a process or batch job. If a single account is used both by a person and by a system for FTP or any other access, then the password for this account will need to expire every 90 days. Accounting must be configured to alert the system administrator of unauthorized access using system-to-system accounts or accounting logs must be reviewed on a weekly basis to detect unauthorized access. If unauthorized access using a system-to-system account is detected, immediate action will be taken to change the affected account password.

When FTP is used for system-to-system FTP, an acknowledgement of risk letter is required. A system-to-system transfer via a VPN would not require an acknowledgement of risk letter.

The acknowledgement of risk letter (AORL) will be used to document the use of unencrypted FTP or telnet or the risk will be accepted as part of the accreditation package (SSAA). The customer (data owner), the local DAA (when the site is not the data owner) will sign an acknowledgement of risk letter. The IAO will maintain the acknowledgement of risk. This letter will identify the UIDs, passwords, and the data that is being transmitted unencrypted inside the site's enclave. The acknowledgement of risk will be dated and will be reviewed and renewed at least every 18 months.

An "anonymous" FTP connection within the enclave will not be allowed. Individual UIDs will be created for each user. This requirement should not be confused with an anonymous FTP server. An anonymous FTP server is a special purpose server, which is used to distribute information (e.g., files, educational material, etc.). An anonymous FTP server utilizes an unauthenticated default username such anonymous or ftp and a commonplace password such a "guest." An anonymous FTP server is permitted as long as the server is compliant with the applicable Operating System STIG; is segregated into the network Demilitarized Zone (DMZ), is on its own subnet on a dedicated system, and as long as it only houses "public" information (information approved by the Public Affairs Officer or the equivalent).

- *(S103.580.00: CAT III) The IAO will ensure the system does not allow Anonymous FTP connections.*

8.3.1 TASFTP - ALN

TCP/IP Application Services (TAS), one of the commercial FTP server implementation provided by Unisys, does not allow anonymous file transfers by default and relies upon the core user authentication mechanisms to validate transfers. However, the ALN operating system has local code modifications to TCP/IP Application Services (TAS) to allow restricted Anonymous FTP service using ANONYMOUS/GUEST. FSO Montgomery is working with Unisys and CDAs on ways to further secure Anonymous FTP or eliminate its use altogether. Pending completion of this task, the following additional mitigating controls have been put in place for this restricted use of ANONYMOUS/GUEST:

a. ANONYMOUS/GUEST does not have a corresponding SIMAN security record and cannot be used to sign on to the system in an interactive terminal session (TIP or Demand) or start Batch jobs. The current operating system does not support FTP only userids in SIMAN.

b. In most cases, ANONYMOUS/GUEST can only be used to put files on the Unisys system. The exception to this is the Air Force Supply DAAS system uses a DEL parameter to clean up incomplete transfers. ANONYMOUS/GUEST cannot be used to get or pull files from the Unisys system.

c. Inbound ANONYMOUS/GUEST FTP transfers are limited to the size of the file that can be placed on the system. This helps to prevent a malicious user from trying to saturate disk space.

d. Inbound ANONYMOUS/GUEST FTP transfers are restricted to a specific qualifier that cannot be altered by the sending system or user.

e. Inbound ANONYMOUS/GUEST FTP transfers are restricted to a specific prefixed filename that cannot be altered by the sending system or user.

The ALN TAS runstream is found in file SYSLIB*RUN$. This file has appropriate security restrictions placed on it to prevent unauthorized modifications. The parameters $ACCESSLEVL, $QULMASKING, and $FILMASKING in the SYS$LIB$*RUN$.TAS runstream will not be changed or altered without prior approval from DISA FSO

NOTE: If a userid has multiple accounts or an account index, TAS FTP will only use the first entry, even if others accounts are specified.

- *(S103.580.00: CAT III) The IAO will ensure the system does not allow Anonymous FTP connections.*

8.3.2 Virtual FTP Userids

8.3.2.1 General Requirements and Capabilities

SSO Montgomery has released a modified version of TAS to all SSO Montgomery supported sites (primary users of the restricted ANONYMOUS/GUEST referenced in *Section 8.3.1TAS FTP - ALN*), which allows the implementation of 1000 virtual FTP only userids. The userids are called FTP000 – FTP999 and will be the first step in eliminating the usage of ANONYMOUS/GUEST. Management of the Virtual FTP userids and their corresponding passwords will be determined by each site.

a. Virtual FTP userids do not have a corresponding SIMAN security record and can not be used to sign on to the system in an interactive terminal session (TIP or Demand) or to start Batch jobs. The current operating system does not support FTP only userids in SIMAN.

b. In most cases, Virtual FTP userids can only be used to PUT files on the Unisys system. The exception to this is the Air Force Supply DAAS system uses a DEL parameter to clean up incomplete transfers. Virtual FTP s cannot be used to GET or pull files from the Unisys system.

c. Inbound Virtual FTP transfers are limited to the size of the file that can be placed on the system. This helps prevents a malicious user from trying to saturate disk space.

d. Inbound Virtual FTP transfers are restricted to a specific qualifier that cannot be altered by the sending system or user.

e. Inbound Virtual FTP transfers are restricted to a specific prefixed filename that cannot be altered by the sending system or user.

8.3.2.2 Securing FTP Virtual Userids

These Virtual FTP userids and their corresponding passwords are located in the file SYSLIB*TASANON$. The file SYS$LIB$*TASANON$ will be secured with the ACR ACRNA that is owned by EXEC8. As stipulated in *Section 8.3.2.1, General Requirements and Capabilities*, management of the Virtual FTP userids and their corresponding passwords will be determined by each site. Passwords for Virtual FTP userids will be manually changed at least twice a year and when an administrator with knowledge of the password leaves. The IAO can use the following procedures to secure this file.

```
@SIMAN,B
UPDATE FILE = SYS$LIB$*TASANON$.
ATTACH_ACR = ACRNA        ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYSLIB$*TASANON$. ;
```

This will attach ACRNA (no access) to the SYSLIB*TASANON$ file. It will then display the file. The file will show the ACR attached. The only users that may view or update elements in the file are those with ACR bypass privileges (site personnel).

- *(S103.670.00: CAT II) For DISA sites, the SA will ensure the file containing the Virtual FTP userids and passwords is secured with ACR ACRNA to protect it from access by unauthorized personnel.*

8.4 DDP

8.4.1 Anonymous DDP

Anonymous DDP will not be configured on production or development machines. Anonymous DDP is enabled by setting the FJT-USERID and the FJT-PASSWORD fields in the DDP configuration file. Anonymous DDP is disabled by setting the DDP-FJT-PASSWORD and FJT-USERID fields in the DDP configuration file to NULL. An example of how to do this is provided below. A host name of M19A is used in the example. Replace the host name with a platform unique host name.

```
@SYS$LIB$*COMUS.CLOD,A
@SYS$LIB$*DDP-PPC.CSUPDT,LPZ
MODIFY HOST NAME=M19A FJT-USERID=NULL FJT-PASSWORD=NULL ;
@EOF
```

- *(S103.570.00: CAT II) The SA will ensure the system does not have Anonymous DDP configured.*

8.4.2 Securing the DDP Configuration File

The DDP Configuration file will be secured with the System ACR of ACRRO and the restricted use of the processor CSUPDT, or a site unique ACR that restricts *read and write* access to the DDP Subsystem userid (for example, -DDP-PPC-) and, if needed, a network type account. If execution of the processor CSUPDT is restricted, it will be restricted to the Profile 2 privilege SSWRSUBDAC.

8.4.2.1 Securing DDP through CSUPDT and ACRRO

The DDP configuration file can be secured by restricting the execution of the processor CSUPDT to a Profile 2 privilege SSWRSUBDAC. This type of restriction requires a local code change to this processor. Contact the Systems Support Office Montgomery for additional information.

To prevent unauthorized users from deleting the DDP configuration file, the System ACR of ACRRO (read only) will be attached to the file. To attach ACRRO to the DDP configuration file, do the following:

```
@SIMAN,B
```

```
UPDATE FILE = DDP*CS$CONFIG.
ATTACH_ACR = ACRRO       ACR_OWNER = EXEC8 ;
DISPLAY FILE = DDP*CS$CONFIG. ;
```

This will attach ACRRO (read only) to the DDP*CS$CONFIG file. It will then display the file. The file will show the ACR attached. The only users that may delete this configuration database are those with ACR bypass privileges (site personnel).

8.4.2.2 Securing DDP with a Site Unique ACR

A site unique ACR can also be used to protect the DDP configuration file. If used, the ACR must be installed so the DDP Subsystem userid has *read and write* access to the DDP configuration file. The site can also add a network type account to the ACR if needed. If the site uses a unique ACR, replace occurrences of ACRRO in the example above with the unique ACR and the ACR owner of EXEC8 with the owner of the unique ACR.

NOTE: When a site unique ACR is attached to this file, only userids with the BYACR privilege or userids that pass the site unique ACR's restrictions can do DDP-FJT COPY and SUBMIT commands via IPF, the DDPFJT batch command interface, or the DDPFJT menu interface. Users doing TAS TRANS(fer) commands via IPF or the TAS menu interface are not impacted when an ACR is attached to this file.

- *(S103.660.00: CAT II) The SA will ensure the DDP configuration file (DDP*CS$CONFIG) is secured by the restricted use of the processor CSUPDT and ACR ACRRO or a site unique ACR to protect it from access by unauthorized personnel.*

8.4.3 Securing the DDP Log and Trace Files

The DDP Log and Trace files will be secured with an ACR to protect them from unauthorized access. These files are owned by the DDP Subsystem userid (for example –DDP-PPC-) so the ACR that is created must be owned by the DDP Subsystem userid. The ACR that is attached to these files must also be installed so the DDP Subsystem userid has *read and write* access to these files. Once the ACR is installed, the ACR should be manually attached to the following files:

```
DDP$TRC
DDP$LOG
DDP$BNKLIST
```

The qualifier of DDP Log and Trace files is based upon the project-id in the PPC runstream (SYSLIB*RUN$.PPC).

The DDP configuration file also needs to be updated to reflect the ACR Name. An example of how to do this is provided below. A host name of GNMB and an ACR name of DDPACR are used in the example. Replace the host name with the domain unique host name and the ACR name with a site unique ACR.

```
@SYS$LIB$*COMUS.CLOD,A
@SYS$LIB$*DDP-PPC.CSUPDT,LPZ
```

```
MODIFY HOST NAME = GNMB ACR-NAME = DDPACR ;
@EOF
```

- *(S103.662.00: CAT II) The SA will ensure the DDP Log and Trace files are secured with an ACR to protect from unauthorized access.*

NOTE: The DDP configuration parameter ACR-NAME will be used to identify the ACR that is used to protect the DDP Log and Trace files.

8.5 TIP Utilities

The following TIP utilities are considered dangerous programs because of the damage they can do to the transaction processing environment:

ABSOLUTE PROGRAM	***INTERFACE NEEDED***
BOXER	TPFLG$ (Enforcement being tested – Profile 4)
TFCIO	FC$SSN (Not secured to date)
TFUR	FC$SSN (Not secured to date)
TREG	FCREG$ (Enforced – Profile 6)
TPUR	VT$PUR (Enforcement being tested – Profile 6)
VTBUTL	VT$CHG (Enforcement being tested – Profile 2)
SUPUR	VT$PUR (Enforcement being tested – Profile 6)
FREIPS	FCREG$/FC$SSN (Enforced see TREG)
TMINIT	TM$SET (Enforcement being tested – Profile 2)
TPINIT	AC$NIT (Enforcement being tested – Profile 2)

Table 8-2. TIP Utilities Interface Usage

Since the utilities above are not adequately secured from execution by non-site personnel, these utilities will be secured by changing selected Interfaces from an UNENFORCED status to an ENFORCED status. Because this action could impact system or application software, each site will work with SSO Montgomery to enforce appropriate Interfaces. Many of the Interfaces have been enforced and are currently being tested on the Air Force development systems. It is recognized that there may be cases where non-site personnel will need access to these utilities. The site will evaluate the user profile and the mission requirement, and upgrade the user if necessary with the appropriate Interfaces. Until the enforcement testing of these TIP utilities is completed, the file TIP$*TIPRUN$ will be secured with ACR PUBRD, owner -CHAMELEON- or Read/Write Keys.

- *(S103.600.00: CAT II) The SA will ensure dangerous TIP utilities are secured in accordance with this STIG requirements.*

8.6 MAPPER

8.6.1 Securing MAPPER

The MAPPER registration RID and MAPPER system information are not secured by default. The registration RID contains all of the MAPPER userid/password information in plain text. MAPPER system information contains critical data concerning the MAPPER configuration. These files will be secured by exclusively assigning these files to the MAPPER run via an @ASG, AX in the MAPPER batch runstream just prior to the execution of MAPPER. Reference the MAPPER documentation for more information. The most common file names that contain the MAPPER registration RID and MAPPER system information are provided below. The site will be using one of these sets.

ALN	*DNMC/DFAS-IN*
M00001	MAPER1
M00002	MAPER2

Table 8-3. ALN MAPPER

Additionally these files, all other MAPPER database files, the MAPPER configuration file, MAPER0, MUPER1, and MUPER2 will be protected with an ACR that can be read and written by the userid that the batch MAPPER background run executes under and/or additional userids of users who would be doing maintenance of these files outside of MAPPER execution. This will protect the files when MAPPER is not running from inadvertent or malicious corruption.

- *(S103.400.00: CAT II) The SA will ensure the MAPPER registration RID and MAPPER system information file are secured with an ACR to protect them from unauthorized access.*
- *(S103.404.00: CAT II) The SA will ensure all other MAPPER database files are secured with an ACR to protect them from unauthorized access.*
- *(S103.402.00: CAT II) The SA will ensure the MAPPER configuration file, <MAPPER qualifier>*HLDMAPis protected with an ACR to protect them from unauthorized access.*
- *(S103.402.00: CAT II) The SA will ensure MAPER0, MUPER1, and MUPER2 are secured with an ACR to protect them from unauthorized access.*

8.6.2 MAPPER Parameter Settings

There are several MAPPER parameter settings that will be set to ensure they comply with documented DOD security policies and procedures. These parameter settings are located in the element <MAPPER qualifier>*HLDMAP.MAPPER/PARAMETERS.

NOTE: The batchport userid will be exempted from the MAPPER password change requirement. There is one batchport userid per MAPPER, this userid does not have a SIMAN security record, and the batchport userid/password is not readily available to the normal MAPPER user. To exempt the batchport userid from the password change

requirement, the MAPPER Coordinator will place an * in column 129 of the user registration report.

Once the parameter changes have been made, MAPPER will be restarted in accordance with normal site procedures. The following parameter settings and their values are listed below:

PARAMETER SETTING	*VALUE*
PSWSIX – Requires a 6 character password	1
SECCHG – Days/Months to change password. Will be set for PSWSIX to work correctly. Will be 90D or 3 (Months).	90D or 3
SECTIM – The time a user has to correctly sign on to the system. Needs to be set for the other security parameters to work correctly. Will be set to 2 – 180. Value in seconds. This value will not be set to 1 since that deactivates the parameter.	180
SECTRY – Number of times a user has to sign on correctly to the system before being disabled.	3

Table 8-4. MAPPER Parameter Settings

- *(S103.410.00: CAT II) The SA will ensure the MAPPER parameter PSWSIX is set to a value of 1.*
- *(S103.410.00: CAT II) The SA will ensure the MAPPER parameter SECCHG is set to a value of 90D or 3.*
- *(S103.410.00: CAT II) The SA will ensure the MAPPER parameter SECTIM is set to a value of 180 or less.*
- *(S103.410.00: CAT II) The SA will ensure the MAPPER parameter SECTRY is set to a value of 3.*

8.6.3 Starting MAPPER – ALN Sites

Sites running the ALN operating system will start each MAPPER with a non-exempt project-ID and non-exempt account so that it will restrict users from starting jobs out of MAPPER to their own ALN. In addition, MAPPER will not be started with a userid that has access to exempt project-IDs or accounts, for example, the standard batch userid used to start other jobs on the system. ALN sites will create a new userid for each MAPPER run, re-profile it using PROFILE/OPS, and then ensure this userid is Batch only (TIP access is optional), is project-ID restricted, cannot enter a project-ID or account, has only the appropriate MAPPER non-exempt project-ID and account listed in the userid record, and is only inserted under the appropriate non-exempt MAPPER account.

NOTE: The CBAS MAPPER userids will need access to the T0 and DB non-exempt project-IDs and accounts.

ALN :

- *(S103.420.00: CAT II) The IAO will ensure MAPPER is started with a non-exempt project-ID and non-exempt account.*

- *(S103.430.00: CAT II) The IAO will ensure MAPPER is not be started with a userid has access to exempt project-IDs or accounts.*

- *(S103.430.00: CAT I) The SA will ensure each MAPPER userid is set up with the userid attributes specified in this STIG.*

8.6.4 MAPPER File Creation

All runs that create MAPPER files, normally PRESTR and PREMAP will attach the ACRs required in section 8.6.1Securing MAPPER.

- *(S103.434.00: CAT II) The SA will ensure runstreams creating MAPPER files attach appropriate ACRs to the created files.*

8.7 Sightline and Torch Files

The Datametrics software has been changed to the Sightline System's Sightline and Torch software. This software is a commercial product that is used to generate information and reports for computer performance management, capacity management, and fee-for-service billing. As such, the information in various Sightline and Torch files needs to be protected from modification or access by unauthorized users.

8.7.1 Securing Sightline and Torch Files – ALN and DFAS-IN Sites

To properly secure the Sightline and Torch files in the HMP IX 5.1 or HMP IX 6.1 environments, the ACR DEVP99, Owner SECOFF or ACR PUBRD, Owner -CHAMELEON- will be attached to them.

The ACR DEVP99 will have the Object Access fields controlled as follows:

READ
WRITE
DELETE
ACR_DELETE
MODIFY
EXECUTE

The ACR access restriction will be controlled by the account 0999VP1A. If the user is still using the account 0999DV1A for DISA Denver Capacity Management personnel, their account needs to be updated to 0999VP1A.

The ACR DEVP99 will be attached to the following Sightline and Torch files:

DATAMETRICS*DENVER
DATAMETRICS*PMS-xxyy (where xxyy the site code and domain code)
DATAMETRICS*TORCH

To attach the ACR DEVP99 to the DATAMETRICS*DENVER file, do the following:

```
@SIMAN,B
UPDATE FILE = DATAMETRICS*DENVER.
ATTACH_ACR = DEVP99     ACR_OWNER = SECOFF ;
DISPLAY FILE = DATAMETRICS*DENVER. ;
```

The ACR PUBRD, OWNER -CHAMELEON- will have the Object Access fields controlled as follows:

READ

This ACR access restriction will be granted to PUBLIC. This ACR will allow any user to view and execute programs from these files, but only those users with the Bypass ACR privilege can make modifications to these files.

The ACR PUBRD, OWNER -CHAMELEON- will be attached to the following Torch files:

SYSLIB*TORCH
SYSLIB*TORCH-RPTS
SYSLIB*TORCH-AUTO
SYSLIB*SIGHTLINE
SIGHTLINE*RUNS

The runstream LIBRARY/FILES will automatically attach the ACR PUBRD, Owner -CHAMELEON- to the above files. If it is necessary to attach the ACR manually, do the following:

```
@SIMAN,B
UPDATE FILE = SYS$LIB$*TORCH.
ATTACH_ACR = PUBRD    ACR_OWNER = -CHAMELEON- ;
DISPLAY FILE = SYS$LIB$*TORCH. ;
```

For ALN:

- *(S103.730.00: CAT II) For DISA sites, The SA will ensure Sightline and Torch files are properly secured to protect them from access by unauthorized personnel.*

8.8 Site Unique Configuration File

8.8.1 Overview

The SYSLIB*STRPARM file was originally established for use by the STAR software and contained elements such as VAULT and AAFPARM. However, in the past several years, other site unique configuration elements have been added to this file by SSO Montgomery. For example, CSC and CDI parameters, AUTO$START, WHOAMI parameters, etc. Due to the critical nature of these site unique configuration elements, this file will be secured to protect it from modification by unauthorized personnel.

8.8.2 Securing SYSLIB*STRPARM

The SYSLIB*STRPARM file will be secured with the System ACR of ACRRO (*read-only*) or a site unique ACR that restricts write and delete access and is controlled by a system type account. To attach ACR ACRRO, do the following:

```
@SIMAN,B
UPDATE FILE = SYS$LIB$*STRPARM.
ATTACH_ACR = ACRRO        ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYS$LIB$*STRPARM. ;
```

This will attach ACR ACRRO (Read Only) to the SYSLIB*STRPARM file. It will then display the file. The file will show the ACR attached. The only users that may update elements in the file are those with ACR bypass privileges (site personnel). All users can read elements in the file. If the site uses a unique ACR, replace occurrences of ACRRO with the unique ACR and the ACR owner of EXEC8 with the owner of the unique ACR.

- *(S103.720.00: CAT II) The SA will ensure the site unique configuration file SYS$*STRPARM file is secured with the ACR ACRRO to protect it from modification by unauthorized personnel.*

8.9 Display Processor System

8.9.1 Overview

The Display Processor System (DPS) allows an application to utilize screens so an end user only has to input information into certain predefined fields to submit a transaction that will update or modify an application database. These screens are usually released with application programs so the predefined fields match the appropriate program. The DPS system is configured with three files—TERMFILE, PAGEFILE, and PASSFILE. These files are in addition to the various application screen files that may be on the system. Application screen files may be dedicated or shared between two or more applications. The DPS utility program FLMU is used to load new screens into the correct application screen file. The FLMU processor determines if the userid is running privileged (access to the MODPS$ Interface is required) or if the userid is entered into the DPS Password file (PASSFILE) with the appropriate authorization before a screen load is attempted. For this reason, access to the MODPS$ Interface is restricted to site personnel only.

8.9.2 DPS Password Files – ALN Sites

On ALN systems, the DPS utility program FLMU or ALN utility TCB can be used to load new screens into the correct application screen file. If the userid used to load the screens is not running privileged, the FLMU processor determines if the userid is exempt or non-exempt. If running exempt, FLMU will check the DPS password file for appropriate access and, if valid, will load the screens into the TIP$*SCRNFxxx file. If running non-exempt, FLMU will check the ALN unique DPS password file for appropriate access and, if valid, will load the screens into the ALN unique screen file. Since site personnel load most of the application screens, the exempt and non-exempt DPS password files may only contain the DPS userid. However, if this is not the case, only authorized users will be entered into the DPS password file. Only site personnel will have access to Password Functions. Only site personnel will have access to all Form Libraries. Only select, high-level functional users will be authorized access, and these users will be granted the minimum DPS privileges needed to load their application screen files. They will not have access to all screen files on the system and will not be able to create, delete, or modify other DPS userids. The password identified for a userid in the DPS password file will not be the same password that is assigned to the userid in SIMAN.

8.9.3 DPS Password File –DFAS-IN

On DFAS-IN (Indianapolis) systems, the DPS utility program FLMU is used to load new screens into the correct application screen file. If the userid used to load the screens is not running privileged, the FLMU processor will check the DPS password file for appropriate access and, if valid, will load the screens into the TIP$*SCRNFxxx file. Only authorized users will be entered into the DPS password file. Only site personnel will have access to Password Functions. Only site personnel will have access to all Form Libraries. Only select, high-level functional users will be authorized access, and these users will be granted the minimum DPS privileges needed to load their application screen files. They will not have access to all screen files on the system and will not be able to create, delete, or modify other DPS userids. Exceptions to these requirements will be documented. Also, a *SAAR* will be submitted to the site IAO along with appropriate

justification. The password identified for a userid in the DPS password file will not be the same password that is assigned to the userid in SIMAN.

- *(S104.440.00: CAT I) The SA will ensure users, except where documented, do not have access to the MODPS$ Executive Interface unless it is authorized for their security profile.*

- *(S103.440.00: CAT II) The SA will ensure only documented authorized personnel have access to Password Functions in the Display Processing System.*

- *(S103.450.00: CAT II) The SA will ensure only documented authorized personnel has access to all Form Libraries in the Display Processing System.*

- *(S103.460.00: CAT II) The SA will ensure only select, high-level functional users are allowed access to the Display Processing System, these users are granted the minimum DPS privileges needed to load their application screens, and this access is documented.*

- *(S103.470.00: CAT I) The SA will ensure the password identified for a userid in the DPS password file is not the same password is assigned to the userid in SIMAN.*

8.10 Unattended Operations Support Software

8.10.1 Overview

The Unattended Operations Support Software (UOSS) allows sites to set up various runstreams to support unattended and attended operations. These runstreams and the userid used by UOSS are located in a control file (SYSLIB*UOSS$C) and this file will be secured with ACR ACRNA to protect it from access by unauthorized personnel.

8.10.2 Securing the UOSS Control File

To attach ACR ACRNA to the UOSS Control file, do the following:

```
@SIMAN,B
UPDATE FILE = SYS$LIB$*UOSS$C.
ATTACH_ACR = ACRNA        ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYS$LIB$*UOSS$C. ;
```

This will attach ACR ACRNA (no access) to the SYSLIB*UOSS$C file. It will then display the file. The file will show the ACR attached. The only users that may update or view this file are those with ACR bypass privileges (site personnel).

- *(S103.820.00: CAT II) The SA will ensure the UOSS Control file (SYSLIB*UOSS$C) is secured with the ACR ACRNA to protect it from access by unauthorized personnel.*

9. THE SCHEDULER

The Scheduler system provides a site with a complete job scheduling and workload management system. Although the commercial product consists of four modules, only the Schedule Generator and the Scheduling Activity Monitor (SAM) modules are discussed in this STIG. The Schedule Generator produces computer-processing schedules for all batch processing, and provides accurate operations documentation for report assembly and distribution. Once a schedule has been produced, it is turned over to SAM for processing. SAM performs all functions and decisions that were once made by computer operators. It schedules jobs based on relative priorities, requested start times, job dependencies, availability of input files, number of tape drives, etc. The Scheduler also provides an interface to the STAR tape management software.

9.1 SAM Keyins

If a site is using Scheduler (SAM), the site will ensure SAM keyins are restricted to users with DISPLAY CONS. This is accomplished by modifying the SAMS-RUN/ECL element in the Scheduler program file. This will restrict functional AIS users, who are not allowed to enter certain SAM commands through the SAMREQ screen, from bypassing the SAMREQ screen by entering those commands through @@CONS. Failure to do so is a clear violation of the boundary placed on non-site users. Security requirements dictate that access for non-site users will be restricted to prevent them from having access to privileged SAM keyins.

- *(S103.250.00: CAT II) The SA will ensure the CONS level in the Scheduler runstream is configured to DISPLAY.*

9.2 Internal Scheduler Security

The Scheduler system contains internal security features that range from no security to total security, including userid/passwords, functional specifications, and data access codes. There are three modes of Scheduler security implementation: Full, which requires a userid and password; Partial, which requires a userid only; and Off, which has no requirements. At the sites, Scheduler Full security will be implemented. This is accomplished in the System Maintenance screen. The following table provides guidance on setting up userids within Scheduler.

FIELD	***REQUIRED INPUT***
USER ID	Enter the new user's <userid>.
PASSWORD	Enter A (Initial password of A will be used).
USER NAME	Enter the new user's name.
HOW TO CONTACT	Enter the new user's office phone number.
DEPT	Enter the new user's department (4-character ALN + 2-character AIS for ALN sites).
LANGUAGE	Enter 0 (zero = English).

FIELD	*REQUIRED INPUT*
SECURITY LEVEL	MS – Master Level (site) SK – Scheduler Level (site) OP – Operations (site or High level Functional User) US – User (End User) See tables below for more information on security levels, access codes, and data access codes.
RESTRICT TO DEPARTMENT	Enter Y for all non-site users. Enter N for site personnel that need to access records in more than one department.
RESTRICT TO PROCESSOR	Leave this field blank unless directed to make an entry here. (This is not a question field thus an entry of N or Y would restrict the new user to processor N or processor Y, which may not exist.)

Table 9-1. Scheduler Setup Process

- *(S103.150.00: CAT II) The SA will ensure Scheduler Full security is implemented.*

9.3 Access Control Methods

There are four levels of users within SAM: MASTER, SCHEDULER, OPERATOR, and USER. Users cannot delete their own user profile record, nor can they add, modify, delete, or display a higher security level user profile record. For example, a USER record created by a MASTER user requires a MASTER user to delete the USER record; either a SCHEDULER user or a MASTER user may delete a USER record created by a SCHEDULER user. Non-site users will be restricted to the OPERATOR or USER access levels and will be restricted to a specific department.

a. Access codes and functions are assigned by the site to identify data to which a user or group of users may have access. These access levels allow users to control and maintain data within their respective area of responsibility. Access codes are set up within the user's profile record; any job record that the user may access will correspond with those set in the user's profile record.

b. Data access codes are designed and structured by the site and assigned by application. sites will create data access codes that will restrict users to only their data within Scheduler. For ALN sites, these data access codes will be the gang plus the AIS code (e.g., 1BQ, 2BQ, 1FS, 3GV, etc.). For DNMC and DFAS-IN (Indianapolis) sites, data access codes will be determined by the application used. Data access codes will be used for all non-site users when a department has multiple application records within it to protect the integrity of the database. In addition, any one of five reserved access codes (ALL, MAS, SKD, SAM, and SUP) will be used to allow specific data manipulation within the Scheduler system.

c. Each access code has a function that defines the type of data manipulation the user may perform. A user may downgrade his own functional access, but cannot upgrade his access.

CODE	*FUNCTION*	*MEANING*
ALL	U	Complete update of codes MAS, SKD, and SUP
	I	Inquiry only of codes MAS, SKD, and SUP
	N	No access allowed
MAS	U	May use SKDUPD screens to alter master file records
	I	May use SKDUPD screens for inquiry only about master file records
	N	No access allowed
SKD	U	May generate production schedules
	I	May only create paper schedules
	N	No access allowed
SAM	U	May issue SAM commands altering run environment and schedule updates
	I	May issue SAM commands for inquiry only
	N	No access allowed
SUP	U	May use SAMUPD screens to update the Daily Schedule after it has been turned over to SAM for processing
	I	May use SAMUPD screens for inquiry only about daily schedules
	N	No access allowed

Table 9-2. Scheduler Codes and Functions

The following tables define the input for the different levels of users within Scheduler. The Scheduler monitor has the discretion to restrict users further by using the above table as a guideline but any deviations from these Scheduler guidelines that cause a less secure environment will be justified and documented on a request letter to the IAO, who may approve or reject the request.

9.3.1 Site Scheduler Security Profiles

Of the four Scheduler security profile levels, three are used for personnel for DISA site : Master, Scheduler, and Operator.

9.3.1.1 Master Level

These users will have the ability to accomplish any function within Scheduler. There will be no more than one primary and as many alternate userids with Master Level access as deemed needed by the IAM to administer the system. These users can have ALL-U. Master Level access is only authorized for site personnel.

FIELD	*REQUIRED INPUT*
SECURITY LVL	Enter MS.
AUTHORIZED ACCESS	The following Access codes are authorized for this level. ALL-U MAS-U SKD-U SAM-U SUP-U
RESTRICT TO DEPARTMENT? (Y/N)	Enter N or leave blank to default to N, since the department restriction will not be used for this level.

Table 9-3. Scheduler: Master Level User

9.3.1.2 Scheduler Level – Primary And Alternate Scheduler Personnel

Within the site, these users are the primary and alternate Schedulers who are responsible for the overall running of Scheduler and troubleshooting Scheduler problems. They can update the master file (MAS-U), generate the daily schedule (SKD-U), update and control SAM (SAM-U), and add jobs to the daily schedule (SUP-U). These users can have ALL-U. Scheduler Level userids with the access code of SKD-U will be restricted to site users only.

FIELD	*REQUIRED INPUT*
SECURITY LVL	Enter SK.
AUTHORIZED ACCESS	The following Access codes are authorized for this level: ALL-U MAS-U SKD-U SAM-U SUP-U
RESTRICT TO DEPARTMENT? (Y/N)	Enter N or leave blank to default to N, since the department restriction will not be used for this level.

Table 9-4. Scheduler: Scheduler Level User

9.3.1.3 Scheduler Level – System Monitor or Surveillance Personnel

Within the site, these people will be the ones doing most of the daily work. They can update or interrogate the master file (MAS – U or I), update and control SAM (SAM – U), and add jobs to the daily schedule (SUP-U). However, they can only inquire against the daily schedule (SKD – I). These users must have ALL – U for the other access codes with Update to work correctly. Scheduler Level userids will not be assigned to non-site users.

FIELD	*REQUIRED INPUT*
SECURITY LVL	Enter SK.
AUTHORIZED ACCESS	The following Access codes are authorized for this level: ALL-U MAS-U or MAS-I SKD-I SAM-U SUP-U
RESTRICT TO DEPARTMENT? (Y/N)	Enter N or leave blank to default to N, since the department restriction will not be used for this level.

Table 9-5. Scheduler: Scheduler Level - Monitor User

9.3.1.4 Operator Level – Site Personnel

This level is used for Operations personnel within the site. These Operations personnel can do SAM updates (SAM – U) and add jobs to the daily schedule (SUP – U). They can only inquire against a schedule (SKD – I) and the master file (MAS – I). These users must have ALL – U for the other access codes with *update* to work correctly.

FIELD	*REQUIRED INPUT*
SECURITY LVL	Enter OP.
AUTHORIZED ACCESS	The following Access codes are authorized for this level: ALL-U MAS-I SKD-I SAM-U SUP-U
RESTRICT TO DEPARTMENT? (Y/N)	The department restriction can be used to further restrict this user level, if necessary. Enter N (or leave blank to default to N) for no restriction.

Table 9-6. Scheduler: Operator Level User (Site)

- *(S103.160.00: CAT II) The IAO will ensure the Scheduler Master userid is not shared.*
- *(S103.170.00: CAT II) The SA will ensure the site has only one primary and as many alternate userids with Master Level access as deemed needed by the IAM to administer the system.*
- *(S103.180.00: CAT II) The SA will ensure Master Level userids are restricted to authorized personnel.*
- *(S103.184.00: CAT II) The SA will ensure the Scheduler Level userids are restricted to the access codes specified in this STIG and are restricted to authorized personnel.*
- *(S103.190.00: CAT II) The SA will ensure the Scheduler Level userids with the access code of SKD-U are restricted to authorized personnel.*
- *(S103.220.00: CAT II) The SA will ensure the Operator Level userids, assigned to site personnel, are restricted to the access codes specified in this STIG.*

9.3.2 Functional Users Scheduler Security Profiles

Of the four Scheduler security profile levels, two are authorized for functional users—Operator and User.

9.3.2.1 Operator Level – High Level Functional Users

This level is used for non-site personnel who are high-level functional users. These users must have ALL – U for the other access codes with *update* to work correctly. These users can interrogate the master file (MAS – I), update and control SAM (SAM – U), add jobs to the daily schedule (SUP – U), and inquire against a schedule (SKD – I).

FIELD	***REQUIRED INPUT***
SECURITY LVL	Enter OP.
AUTHORIZED ACCESS	The following Access codes are authorized for this level: ALL-U MAS-I SKD-I SAM-U SUP-U
RESTRICT TO DEPARTMENT? (Y/N)	Enter Y to restrict the user to a specific department.

Table 9-7. Scheduler: Operator Level – Functional User

If job records exist for multiple applications in the department, then under subsequent code/functions, enter the data access codes to which the new user is authorized access and the

functions the user can perform. For example, if the new user will be allowed to update records having only the 2BQ data access code, the entry would be 2BQ U.

9.3.2.2 User Level

These end users can interrogate the daily schedule (SUP – I). They can inquire against a schedule (SKD – I), interrogate against the master file (MAS – I), and interrogate SAM (SAM - I). They can also have ALL-I.

FIELD	*REQUIRED INPUT*
SECURITY LVL	Enter US.
AUTHORIZED ACCESS	The following Access codes are authorized for this level: ALL-I MAS-I SKD-I SAM-I SUP-I
RESTRICT TO DEPARTMENT? (Y/N)	Enter Y so the user is restricted to a specific department.

Table 9-8. Scheduler: User Level

If job records exist for multiple applications in the department, then under subsequent code/functions, enter the data access codes to which the new user is authorized access and the functions the user can perform. For example, if the new user will be allowed to view records having only the 2BQ data access code, the entry would be 2BQ I.

- *(S103.210.00: CAT II) The SA will ensure non-site personnel are set up in Scheduler with Operator or User Level access only.*
- *(S103.220.00: CAT II) The SA will ensure Operator Level userids, assigned to High Level Functional Users, are restricted to the access codes specified in this STIG.*
- *(S103.220.00: CAT II) The SA will ensure User Level userids are restricted to the access codes specified in this STIG.*
- *(S103.230.00: CAT II) The SA will ensure non-site Scheduler userids are restricted to a department.*

9.4 Restricting Access to the Master Level Scheduler Userids

The default Master Scheduler Userid will be known by one individual in the Scheduling office. As indicated above, additional master level userids may be installed for use. The default password for the initial master userid that is installed when Scheduler is implemented by NEWSECECL will be changed immediately after implementation.

- *(S103.200.00: CAT II) The SA will ensure the default password for the initial Scheduler Master userid is changed immediately after implementation.*

9.5 Other Scheduler Security Requirements

Even with full Scheduler security implemented, there are two Scheduler elements in the SKDPRG file that will be moved to a side file and secured with a restricted ACR. These elements are NEWSECECL and SAMCMDECL. If the site is running the ALN operating system, these two elements will be moved to file SYSLIB*USAF-SECURE so they are protected. The Scheduler database, <QUAL>*SKDMAS, will also be saved on a regular basis via a SAVE, SAVALL, or by other means.

- *(S103.240.00: CAT II) The SA will ensure the elements NEWSECECL and SAMCMDECL are moved to a side file and secured with a restricted ACR.*

10. WebTS

The WebTS software allows TIP transactions to be accomplished using a standard Web browser. Since WebTS functions as a web server the WEB Server STIG will be used as the guidelines for implementation of this product.

This page is intentionally left blank.

11. TELECOMMUNICATIONS SECURITY

11.1 Communications Management System

Unisys has published June 30, 2006 as the end of life date for general support of CMS 1100. After this date, Unisys will not support this product. Because of the termination of support for this product by the vender, there will be no further updates to this section of this STIG. Additionally any site still using this product should move to the appropriate replacement products prior to June 30, 2006. CMS 1100's functionality is replaced by the Unisys products CPCOMM and SILAS.

The Unisys Communication Management System (CMS 1100) is the software that controls the interface between a Distributed Communications Processor (DCP) and the OS2200 mainframe on the mainframe. It also handles the TCP/IP interface from Host LAN Controllers (HLCs), Ethernet Channel Adapters and FDDI Channel Adapters.

11.1.1 Sensitive Configuration Statements

CMS 1100 has many configurations statements, also called network definition statements (NDS), some of which have security implications. The sensitive statements are listed in the table below.

Configuration Statement	*Description*
ADMIN	Configures administrative features.
APPLICATION	Configures TIP application Group.
PID	Configures the relationship between TIP position identifiers (PID) and CMS 1100 end users.
PROCESS	Configures major functions of CMS 1100. Specifically the process CSACSU is of security interest.
RSI	Overrides default Demand properties.
SNMP-MGMT	Configures SNMP Version 1

Table 11-1. CMS 1100 Configuration Statements

For more detailed information about these configuration statements see the Unisys manual Communications Management System Configuration Reference Manual, 7830 9853.

11.1.1.1 ADMIN Statement

The ADMIN statement has two fields that affect security, the SECURITY field and the KEYIN-Name field.

The field SECURITY is optional and controls CMS 1100's action if an attempt is made by a terminal or an @@CONS session to establish a connection to the administrative interface. For @@CONS to use the administrative interface there must be an ADMIN card with the KEYIN-NAME field on it in the configuration.

If the release level IS HMP IX 5.1 or higher the LOG-TELNET-OPENS and VERIFY-TERM-COMMANDS fields have been added to the ADMIN card.

11.1.1.1.1 SECURITY Field

a) If the ADMIN card has a SECURITY field with a NOT-REQUIRED (default) in the second subfield then no challenge will be made when a connection is established to the administrative interface.
b) If the second SECURITY subfield is NO-ACCESS then no connection will be allowed to the administrative interface for a terminal or in an @@CONS session.
c) If the second SECURITY subfield is PASSWORD then the following subfield is a password one to eight character alphanumeric value not containing a slash (/), a space or a comma (,). This password must comply with password construction rules as specified in section: 3.1.6 Password Controls and there must be a procedure established to change this password at an interval no greater than 90 days.

Because the default value for the second subfield of the SECURITY field is NOT-REQUIRED, there will be an ADMIN statement in the CMS 1100 configuration, the ADMIN statement will have a SECURITY field, and it will not have a value of NOT-REQUIRED for the second subfield.

11.1.1.1.2 KEYIN-NAME Field

The KEYIN-NAME field is optional and has a subfield that allows the input, from a system console, of CMS 1100 operation commands without first performing an II keyin to receive an input prompt from CMS 1100. It also allows DEMAND users to perform CMS commands via the @@CONS interface if the user knows the CMS 1100 password. The value found on the second subfield of the KEYIN-NAME field is the console keyin that may be used with this feature. Regardless of the existence of this field the CMS 1100 background run's generated runid with a preceding asterisk can be used from a system console to input a CMS 1100 command without the use of the II keyin prompt.

Format of keyin using the generated runid.

**cmsrunid* STATUS

11.1.1.1.3 LOG-TELNET-OPENS Field

The second subfield of the LOG-TELNET-OPENS field can have the values of YES or NO. When set to YES TELNET opens to CMS 1100 are logged in the CMS 1100 log file. When set to NO they are not logged. NO is the default value if this field does not exist. The second subfield of the LOG-TELNET-OPENS will be set to YES.

Field Format: LOG-TELNET-OPENS,*value* *Where value is YES or NO.*

11.1.1.1.4 VERIFY-TERM-COMMANDS Field

The second subfield of the VERIFY-TERM-COMMAND field can have the value of YES or NO. When set to YES the originator of a CMS 1100 command that will terminate CMS 1100 is informed that the command must be entered twice in a row to become effective upon the first entry and the command will be processed on the second entry. This prevents the accidental

termination of CMS 1100 except in the case where CMS 1100 is in a severe thresholding state. In this case, no warning is given and the first command is processed immediately. When the subfield is set to NO, the default, .the command executes immediately on first entry. The second subfield of the VERIRY-TERM-COMMANDS will be set to YES.

Field Format: VERIFY-TERM-COMMANDS,*value* *Where value is YES or NO.*

NOTE: If used prior to HMP IX 6.1 PLE 17604686 should be applied to prevent problems caused when CMS 1100 is in a severe buffer thresholding state.

- *(S103.870.00: CAT II) The SA will ensure there is an ADMIN statement in the CMS 1100 Configuration.*
- *(S103.870.00: CAT II) The SA will ensure the second subfield of the SECURITY field does not have a value of NOT-REQUIRED.*
- *(S103.870.00: CAT II) The SA will ensure the second subfield of the LOG-TELNET-OPENS field is set to YES.*
- *(S104.870.00: CAT II) The SA will ensure the second subfield of the VERIFY-TERM-COMMANDS field is set to YES.*

11.1.1.2 APPLICATION Statement

The PID-POOL Field, Section 11.1.1.3 PID Statement, will not be used on the APPLICATION Statement.

- *(S103.870.01: CAT II) The SA will ensure the PID-POOL Field is not used on the APPLICATION Statement.*

11.1.1.3 PID Statement

The PID statement PID POOL field will not be used as it makes it difficult to ascertain the physical source of a session without a prohibitive amount of trace and log information being captured.

- *(S103.870.02: CAT II) The SA will ensure the PID-POOL field of the PID statement is not used.*

11.1.1.4 PROCESS Statement

The PROCESS statement has two areas of concern. The first being the PROCESS statement with the process name CSACSU and the second being the PROCESS statements with the TYPE of TSAM.

11.1.1.4.1 Process Name CSACSU

The PROCESS statement with the process name of CSACSU allows the administrative functions of CMS1100 to be accessed from Distributed Communications Processors (DCPs), DCA or TCP/IP terminals establishing a CSACSU session, and Demand users using an @@CONS interface. If the "PROCESS,CSACSU" statement is not in the configuration the process CSACSU is configured by default and is available to Demand users, DCPs, and, if the DCP is configured to allow it, sessions established from DCA terminals but not TCP/IP. If the "PROCESS,CSACSU" statement exists and there is an INTERNET-ADR field then the administration functionality is available for all interfaces. There is no way to restrict access to this functionality in TCP/IP to specific IP address so if there is a "PROCESS,CSACSU" statement in the configuration it will not have an INTERNET-ADR field.

- *(S103.870.03: CAT II) The SA will ensure, if there is a "PROCESS,CSACSU" statement in the configuration, it does not have an INTERNET-ADR field.*

11.1.1.4.2 TYPE TSAM

The Process statement with the TYPE of TSAM, or TSAM/CPCOMM, is to identify an API with certain properties to be used by software needing CMS 1100's lower level transport services. There are many example configurations to be found in software installation guides. These examples define a PASSWORD field with a specific password subfield. The password subfield is used in conjunction with the process id subfield to uniquely identify this TSAM PROCESS statement when called via the TSAM API. The problem is that in many configurations for CMS 1100 these examples are implemented without changing the password subfield. Since malicious code could hijack this API if the writer knows the process id and the password, no password found in an example configuration will be used.

- *(S103.870.04: CAT II) The SA will ensure no password from an example configuration is used on a CMS 1100 configuration statement.*

11.1.1.5 RSI Statement

The RSI statement is optional and has three fields that are of concern, the GENERIC field and the TIME-OUTS field.

11.1.1.5.1 GENERIC Field

The GENERIC field is optional and creates an end point or application name for a terminal to establish a Demand session that is not identified by a specific terminal ID. The second subfield is the name of the end point or application. This field will not be present on a RSI statement.

11.1.1.5.2 TIME-OUTS field

The TIME-OUTS field is optional and determines CMS 11000's response for a Demand session that has an inactivity timeout contingency issued by the operating system. The second subfield of the TIME-OUTS field is either YES or NO. When the subfield is YES the session is terminated. If the subfield is NO then the timeout contingency is ignored and the session is

allowed to continue. The default value if this field is not present is YES. The second subfield of the TIME-OUTS field if present will be YES.

- *(S103.870.05: CAT II) The SA will ensure, if the RSI statement is used, it does not have a GENERIC field.*

- *(S103.870.05: CAT II) The SA will ensure, if the TIME-OUTS field of the RSI statement is used, the value of the second subfield is YES.*

11.1.1.6 SNMP-MGMT Statement

The SNMP-MGMT statement is used to configure the agent interface for Simple Network Management Protocol on Unisys systems. Since CMS 1100 only supports version 1 of SNMP which is not allowed by the Network STIG, it should not be used.

- *(S103.870.06: CAT II) The SA will ensure there is no SNMP-MGMT statement in the configuration.*

11.1.2 Batch Run Userid Requirements

The userid used in the execution of the background batch run will have the following privileges and interface accesses. This will be a batch only userid and will not have any privileges or interfaces not needed. This userid will be allowed to create only owned files.

11.1.2.1 Privileges Required

The CMS 1100 background run requires the following privileges.

SSADID	Always required.
SSLOGER	Always required.
SSCONSOLE	Always required.
SSSSCALLANY	Required if TSAM is used.
SSRUNXOPT	Required if resilient configuration.
SSTOKEN	Required if available in operating system level.

11.1.2.1.1 Additional Privileges Required for Remote Batch Processing

The following privileges are required to bypass access controls on print and punch files for traditional remote batch processing. This does not apply to DEPCON printing. If there is no remote batch processing in use, these privileges will not be given the userid that is used to run the CMS1100 batch run. To verify that traditional remote batch processing is in use make the following checks.

> IS there one or more DCPs? If no then remote batch processing is not in use. If there is a "PROCESS,RSBCSU" statement in the CMS 1100 configuration it has no effect but to cause the CMS 1100 modules for process remote batch sites to be loaded into memory. In this case the "PROCESS,RSBCSU" statement should be removed.

If there is one or more DCPs, is there a "PROCESS,RSBCSU" statement in the CMS 1100 configuration? If not then remote batch processing is not configured.

SSSMOQUE
SSBPFC
SSBRWK
SSBYCL
SSBAFC
SSBKUP
SSBYPASSOWNR
SSBYCOMP

Additionally, the CMS 1100 batch run will be privileged while executing the CMS 1100 Program. This means that the file SYS$*DLOC$. will be assigned, with the correct read and write keys, to the run or there must be an execution of @SYSLIB*COMUS.CLOD,A prior to the CMS 1100 execution .

11.1.2.2 Interfaces Required

The CMS 1100 background requires the following secured interfaces.

MCODE$	Required for HLC-2s.
PB$CON	Always required.
TF$KEY	Always required.
CONNECT$TIP	Always required.

Normally the following interfaces are unsecured. If any are secured, either locally or by the Unisys security levels installed above level 1, then the batch userid would require access to them. To avoid problems arising from changes in interface security causing an interruption of communications, the userid for the CMS 1100 batch run will always have access to these interfaces.

CMS$REG
MQF$
RSI$
RT$INT
RT$PID
TIP$SM
TIP$TALK
TIP$XMIT

- *(S103.870.07: CAT II) The SA will ensure the batch run userid for CMS 1100 background run is set up as described in this STIG.*

11.1.3 Account Requirements

The only account requirements for the CMS 1100 batch run are.

The account will allow Real Time Level 2.
The account will not be the Privilege Account used for tape labeling.
ALN additional needs.
If remote batch processing as described in *Section 11.1.2.1.1, Additional Privileges Required for Remote Batch Processing*, is configured the account will be an ALN exempt account so that the batch run can assign all files queued to remote printer queues.

- *(S103.870.08: CAT II) The SA will ensure the CMS 1100 batch run account allows Real Time Level 2.*

- *(S103.870.08: CAT II) The SA will ensure the CMS 1100 batch run account is not the Privilege Account.*

For ALN:

- *(S103.870.08: CAT II) The SA will ensure the CMS 1100 batch run account is an ALN exempt account.*

11.1.4 Subsystem Userid Requirements

The CMS 1100 product contains an extended mode fixed gate subsystem therefore the file containing the subsystem will be owned by a subsystem userid. The file owned by this userid normally is "SYSLIB*CMS1100." on a standard mode "A" install of CMS 1100 and "CMS1100*TEST$LIB." for a mode "TEST" install. Unisys recommends the subsystem userid have the following properties. This is one of the System Userids described in section 3.1.5 System Userids.

PROPERTY	***Unisys STIG Value***	***Vender Suggested Value***
Userid Name	-CMS1100-	-CMS-SUBSYS-
ACR Name attached to userid	CMSSS or EXEDEL	CMSSS
ACR Execute Argument	PUBLIC	PUBLIC
ACR Delete Argument	Background run userid or master userid	Background run userid or master userid
Run Mode	None	None
Processor Privilege	Read Executive GRS	Read Executive GRS
Access Privilege	Trusted	Trusted
Sharing Level	Application	Application
Clearance level	Max 0; Min 0	Max 0;Min 0
Compartment set if Security Level 2 or greater	Maximum = NULL Default = NULL	Maximum = NULL Default = NULL (no compartments assigned)
Trusted Privileges	None will be selected	None will be selected
Other Privileges	SSGAP	SSGAP
Interfaces	DUMP$SUBSYS	DUMP$SUBSYS
ACR Name (ACR that owns subsystem file)	PUBRD	PUBRD
ACR Read argument	PUBLIC	PUBLIC

Table 11-2. CMS 1100 Subsystem Userid Requirements

NOTE: This STIG requires this userid to be disabled.

- *(S103.870.09: CAT II) The SA will ensure the CMS 1100 Subsystem Userid is configured as described in this STIG.*

11.1.5 Dynamic CMS 1100 Configuration Changes

The CMS 1100 configuration can be modified at runtime from the operations console. This is referred to as dynamic updating of the configuration. Dynamic updating of the CMS 1100 configuration should not be done.

11.1.5.1 Emergency Dynamic Configuration Changes

If an emergency requires a dynamic configuration change, following steps will be taken.

a) Verify that there is no current dynamic change or, if there is, that it is correctly documented. See *Section 11.1.5.2 Verifying Dynamic Changes and Their Logging*
b) Make the change.
c) Documented the change in the security log along with the time and date of the change, the reason for the change, the authorizing authority, and the time and date found on the CONFIG MODIFIED line of the CMS 1100 STATUS command response prior to this dynamic change so that change documentation can be back tracked. If multiple changes are being made at the same time then the last change's time and date should be used in the documentation.
d) This documentation will be available for the previous 48 hours or until a static configuration has been made, removing all dynamic configuration changes.

If a temporary configuration change is required, when the change is no longer required the configuration will be reverted to the original source configuration with a full CMS 1100 static configuration as soon as possible without unduly impacting communications availability.

If the change is to be permanent, the source configuration will be modified and the new source configuration will be implemented with a full CMS 1100 static configuration as soon as possible without unduly impacting communications availability.

11.1.5.2 Verifying Dynamic Changes and Their Logging

To verify that no unreported dynamic configuration changes are in effect there will be a procedure in place to enter the CMS 1100 STATUS command once a day at the system console and the results will be verified to ensure the following values are equal or in some levels the second value, CONFIG MODIFIED, will not be present if no dynamic modification changes have been made.

CONFIG GENERATED: *hh:mm:ss dd:mmm:yy*
CONFIG MODIFIED: *hh:mm:ss dd:mmm:yy*

If the time date stamps are not equal then a check will be made to ensure that there is a security log entry for the time date found for the CONFIG MODIFIED field's time date. If the change was not documented, the IAO will be immediately informed and if the discrepancy cannot be explained, actions will be taken to revert to the current source configuration.

The STATUS command can be entered without a prompt by typing the following at the system console.

**cmsrunid* STATUS

Where *cmsrunid* is the current generated runid of the CMS 1100 background run. The asterisk is required.

If this requirement is implemented via the SMART Console AMS database then the AMS database will be configured to cause the CONFIG GENERATED and CONFIG MODIFIED messages to be placed in the HOLD window so that they can be verified.

- *(A102.340.00: CAT II) The SA will ensure, if in an emergency a dynamic update must be made, it is logged in the security log.*

- *(S102.870.10: CAT II) The SA will ensure, if an emergency update is made, actions are taken as described in this STIG to either change the source configuration if necessary and implement the new source configuration, or revert to the original source configuration after the emergency is resolved, in a timely manner.*

- *(A102.350.00: CAT II) The IAO will ensure there is a procedure to verify an undocumented dynamic change to the CMS 1100 configuration has not been made.*

- *(A102.360.00: CAT II) The IAO will ensure documentation is available for the previous 48 hours or until a static configuration has been made, removing all dynamic configuration changes.*

11.1.6 Securing CMS 1100 Created Files

During the course of normal operation CMS 1100 creates several files, logs, traces, dumps, etc. Some of these files will contain sensitive information so all of these files will be treated as FOUO. If the CMS 1100 word addressable configuration file (WAD file) is created as a private file, all files created by CMS 1100 will be created private. Since the batch run userid is required to create owned files, *Section 11.1.2 Batch Run Userid* Requirements ~~*Batch Run Userid* Requirements~~ ~~*Batch Run Userid* Requirements~~, these files will be created as private to the CMS 1100 batch run userid. Therefore, the CMS 1100 WAD file will be cataloged private and owned by the CMS 1100 batch run userid.

NOTE: If the user is going to change the CMS 1100 WAD file to private start by changing to private or delete the existing cycles of the files created by CMS 1100 beforethe start of the CMS 1100 batch run or it will error. Testing has shown that this works best when the file attributes are changed first and then CMS 1100 is taken down and restarted.

These files are:

LOG as defined on the LOG statement in the CMS 1100 configuration.
TRACE as defined on the TRACE statement in the CMS 1100 configuration.
CMS1100-PMD
CMS1100-SNAP
CMS1100-ERR

TELCON dump files, if generated, will also be private.

On SSO Montgomery supported systems, the WAD file is usually SYS$*NCO. An intermediate configuration file, SYS$*CONF, is also used. The log and trace files on these systems will usually be SYSLIB*TRACE$FILE and SYS$LIB$*LOG$FILE

- *(S103.690.00: CAT II) The SA will ensure the CMS 1100 word addressable configuration file is cataloged private and owned by the CMS 1100 batch run userid.*

11.2 Distributed Communications Processor

Unisys has published December 31st 2004 as the termination date for general support of DCPs and their related software. This includes TELCON, DCP OS, LAN Platform and all other products that run solely on a Distributed Communications Processor. Any site that is still dependent upon this hardware and software at this time should establish a separate agreement with Unisys for continued support until the site can migrate to other supported means of communicating with their Unisys equipment. Since the vender no longer supports this product, no further updates will be made to this section of this STIG. Additionally this section and all other information that pertains to DCPs will be removed from this STIG on the first major update following 31 December 2005.

The Unisys Distributed Communications Processor (DCP) is one of the communications links between the user and the Unisys host. This unit concentrates all incoming communications traffic into a single path for introduction to the host. There are significant threats inherent to the

DCP. The site will also implement additional security measures to further secure dial-up connections.

- *(A101.120.00: CAT II) The IAO will ensure the site implement additional security measures to secure dial-up connections to DCPs.*

11.2.1 Pre-TELCON 10R2

If the site is running a level of TELCON prior to 10R2, there is a significant threat in the form of the Network Management System (NMS) password. Prior to TELCON 10R2, any DCP in the network is trusted by all the other DCPs in the network. So while each DCP may have a unique NMS password known only by the local site communications personnel, if any NMS password is compromised, it can be used as a means to compromise every other DCP in the network. Because of this weakness, it is critical that only personnel responsible for maintaining a particular DCP know the NMS password for that DCP. At the site, there is no strict limit on the number of personnel assigned to this function. However, at the remote sites, no more than two people will know the NMS password for the local DCP. The NMS password will be periodically changed by the site and remote sites, especially if a change in personnel (for example, retirement, relocation, job reassignment, etc.) occurs. As a minimum, the NMS password will be changed every 365 days. The NMS password will be constructed in accordance with password rules described in *Section 3.1.6.1, Requirements*, (e.g., a combination of alphanumeric, non-repeating, non-consecutive characters). There is a software change available in TELCON 9R1 and above that further secures the NMS password. This software change prevents a user from using the privileged INSPECT command to view the NMS password.

- *(A101.110.00 and A103.030.00: CAT II) The IAO will ensure knowledge of the NMS password is limited to authorized individuals, and will ensure the password is changed on a periodic basis or, as a minimum, every 365 days.*

- *(A103.040.00: CAT II) The SA will ensure the NMS password consist of a combination of alphanumeric, non-repeating, non-consecutive characters.*

- *(A103.050.00: CAT II) The SA will ensure the TELCON software change prevents a user from using the privileged INSPECT command to view the NMS password has been applied.*

11.2.2 Post-TELCON 10R2

After TELCON 10R2, the DCPs are no longer trusted by each other, and Identification and Authentication (I&A) mechanisms in the form of individual userids/passwords are implemented. In this environment, each individual requiring access to the DCP will have a unique userid and password for Identification and Authentication. Also, because individual accountability will be implemented, there will be no restriction on the number of remote personnel who have access to the DCP.

11.3 Securing TELCON and CMS Files

As a minimum, the Telecommunications Configuration (TELCON) and Communications Management System (CMS) files listed below will be secured from unauthorized access. These files contain Front End Processor (FEP) load elements, Remote Concentrator DCP load elements, configuration files, source code, etc. The ACRs listed below are recommendations but the intent of the access (read, write, or delete) will be followed. The site may create unique ACRs to protect these files as long as access is appropriately restricted to authorized site personnel only.

FILENAME	*RECOMMENDED ACRs*
SYSLIB*FEPLOAD	ACRNA, or restricted read, write, and delete ACR tied to a network type account.
SYSLIB*LOAD	ACRNA, or restricted read, write, and delete ACR tied to a network type account.
TELCON Source File – Filename will vary by site. Some use DCFS*TELCON.	ACRRO, or restricted write and delete ACR tied to a network type account. The site may also make this ACR read, write, and delete restricted if desired.

Table 11-3. TELCON and CMS 1100 System Files

To attach ACR ACRNA, do the following:

```
@SIMAN,B
UPDATE FILE = SYS$LIB$*FEPLOAD.
ATTACH_ACR = ACRNA        ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYS$LIB$*FEPLOAD. ;
```

This will attach ACRNA (no access) to the SYSLIB*FEPLOAD file. It will then display the file. The file will show the ACR attached. The only users that may view or update elements in the file are those with ACR bypass privileges (site personnel). If the site uses a unique ACR, replace occurrences of ACRNA with the unique ACR, and the ACR owner of EXEC8 with the owner of the unique ACR. To attach ACR ACRRO to the TELCON source file, replace ACRNA with ACRRO, and replace the filename SYSLIB*FEPLOAD with the TELCON source filename.

- *(S103.680.00: CAT II) The SA will ensure the Telecommunications Configuration (TELCON)/Communications Management System (CMS) file (SYSLIB*FEPLOAD) is secured with the ACR ACRNA to protect it from access by unauthorized personnel.*

- *(S103.710.00: CAT II) The SA will ensure the Telecommunications Configuration (TELCON) file (SYSLIB*LOAD is secured with the ACR ACRNA to protect it from access by unauthorized personnel.*

- *(S103.700.00: CAT II) The SA will ensure the Telecommunications Configuration (TELCON) source file is secured with the ACR ACRRO to protect it from modification by unauthorized personnel.*

11.4 NAPZ00 Terminal Configuration File – ALN

11.4.1 Overview

The NAPZ00 Terminal Configuration file (now called SYS$*PMSCBP104FNP) was established prior to the implementation of Phase IV to provide terminal security for the various applications processed on the system. This file contains pertinent application information and links certain Position Identifiers (PIDs) and terminal IDs to specific applications. This file is critical to the security contained in TIP Interface with ADS (TIWADS) and will be secured to protect it from access by unauthorized personnel.

11.4.2 Securing the NAPZ00 Terminal Configuration File

The NAPZ00 Terminal Configuration file (SYS$*PMSCBP104FNP) will be secured with the System ACR of ACRRO (*read-only*) or a site unique ACR that restricts write and delete access to select site personnel. The site can delegate update capability to selected BNCC personnel, but this will be strictly controlled and these users will be restricted to their specific ALN. To attach ACR ACRRO, do the following:

```
@SIMAN,B
UPDATE FILE = SYS$*PMSCBP104FNP.
ATTACH_ACR = ACRRO        ACR_OWNER = EXEC8 ;
DISPLAY FILE = SYS$*PMSCBP104FNP. ;
```

This will attach ACR ACRRO to the SYS$*PMSCBP104FNP file. It will then display the file. The file will show the ACR attached. The only users that may update elements in the file are those with ACR bypass privileges (site personnel). If the site uses a unique ACR, replace occurrences of ACR ACRRO with the unique ACR and the ACR owner of EXEC8 with the owner of the unique ACR.

- *(S103.800.00: CAT II) The SA will ensure the NAPZ00 Terminal Configuration file (SYS$*PMSCBP104FNP) is secured with the ACR ACRRO or a similar site unique ACR to protect it from modification by unauthorized personnel.*

12. SYSTEM PRINT UTILITIES

12.1 PSERVER

12.1.1 Overview

PSERVER is a Unisys product that enables users on an OS 2200 host in a network to transfer print output between OS 2200 hosts, transfer print output between OS 2200 hosts and Unisys U Series hosts that support PSERVER, and transfer print output between OS 2200 hosts and desktops that have PC On-line Print software installed. PSERVER allows for the automatic movement of user designated print listings from one print queue on the host to another print queue on the same host. PSERVER, in conjunction with the Tape File Transfer facility, can also be used to transfer tape files between OS 2200 hosts in the network.

In the current DISA environment, the Print Distribution by Queue Processor (PDQ) software is now used to accomplish the MOVE functions previously performed by PSERVER. Since the On-line Print software has been decommissioned, the SEND function of PSERVER is being migrated to the Distributed Enterprise Print Control (DEPCON) product. PSERVER is now being used primarily to transfer tape files between OS 2200 hosts in the network.

12.1.2 Configuration Statements

PSERVER has three configuration statements, KEYTYPE, RECEIVE, and SEND, that are of particular security concern.

12.1.2.1 KEYTYPE Configuration Statement

The configuration statement KEYTYPE is used to define the keyin used to communicate with the PSERVER background run while it is executing. By default the value for this keyin is PS. The format of this statement is:

KEYTYPE *keyin-type*

Where *keyin-type* is the value used to start the keyin command for this PS. It must be unique to all other keyin values, system defined or user defined, be up to 8 alphanumeric characters, it may contain an asterisk (*), and must not start with a numeric. Since systems do not contain an asterisk, it is recommended that one be used in this keyin.

Since any user granted CONS privileges at any level are allowed to execute KEYIN$ keyins and there are destructive PSERVER commands that would impact the availability of PSERVER or its functionality, there will be a KEYTYPE statement in the PSERVER configuration and it will not have the value PS.

- *(S103.610.01: CAT II) The SA will ensure there is a KEYTYPE statement in PSERVER configurations.*

- *(S103.610.02: CAT II) The SA will ensure the value of the second field of the KEYTYPE field is not be PS.*

12.1.2.2 RECEIVE Statement

The RECEIVE statement allows the PSERVER host to receive files from other PSERVER hosts. Since the ClearPath IX no longer supports any directly attached printers, the RECEIVE statement is not required for print files; however, it is need to for the tape transfer process (TXFR). Since PSERVER will not be allowed to receive print files, the following statements will not be present in the PSERVER configuration.

ASG-DEVICE
ASG-PACKID
ASG-SIZE
FILE-ACCESS
QUAL-FILE

To ensure PSERVER can only receive files associated with the tape transfer process, the RECEIVE statement will contain a Print Server receiver application name. The Print Server receiver application name, which can be 1 to 12 alphanumeric characters, must match the destination application name in the SEND parameter statement in the PSERVER runstream on the sending host. On SSO Montgomery supported systems, the receiver application name will be provided by the PSERVER AIS Manager.

- *(S103.610.03: CAT II) The SA will ensure none of the statements related to the RECEIVE statement, which are prohibited by this STIG, are present in the PSERVER configuration.*

- *(S103.610.04: CAT II) The SA will ensure the RECEIVE statement contains a receiver application name.*

12.1.2.3 SEND Statement

As stated in section 12.6.1.1.2, RECEIVE Statement, PSERVER will only be used for the tape transfer process. To ensure print files cannot be sent by PSERVER, the PSERVER configuration will only contain SEND statements that reflect a sending Tape File Transfer queue. These SEND statements will also contain a destination application name. On SSO Montgomery supported systems, the destination application name will be provided by the PSERVER AIS Manager. An example of a SEND statement using a destination application name is provided below:

SEND TXFR32 TO GNMB,TXFR32 USING xxxxxxx

- *(S103.610.05: CAT II) The SA will ensure the PSERVER configuration file only contains SEND statements identify a sending Tape File Transfer queue.*

- *(S103.610.06: CAT II) The SA will ensure each SEND statement contains a destination application name.*

12.1.3 Userid Requirements

The PSERVER background run's userid will be a batch only userid and disabled. This userid will have the following privileges.

BYACR
BYCOMPMT
BYOWNER
BYCL
BYPRVFLC
BYRWKEY
BYRWMODE
COM$PRV
CREEXCLG
MODRECCL
SMOQUE
SSSSCALLANY

These privileges are required so that PSERVER can assign and transfer any file found on the system by overriding any MAC or DAC restrictions placed on the file. Additionally the batch runstream must be privileged prior to the execution of the PSERVER absolute, either by assigning DLOC$ correctly or executing CLOD,A. The system standard batch userid can be used to start the PSERVER background run.

- *(S103.610.07: CAT II) The SA will ensure the PSERVER batch run userid is batch only.*
- *(N/A: CAT II) The SA will ensure the PSERVER batch run userid is disabled.*
- *(N/A: CAT II) The SA will ensure the PSERVER batch run userid have the privileges required by this STIG.*

12.1.4 Account Requirements

There is only one general account requirement for the PSERVER background run. The account must allow realtime execution if the user configures the PSERVER to run realtime. In an ALN system the account must be an exempt account since PSERVER must be able to access any file it finds on a system regardless of who sent it.

- *(S103.610.08: CAT II) The SA will ensure the PSERVER background run account is allowed realtime privilege.*

For ALN:

- *(S103.610.08: CAT II) The SA will ensure the PSERVER background run account is an ALN exempt account.*

12.1.5 EXECUTION requirements

The execution of the PSERVER absolute in the background runstream will contain the "B" option, which allows PSERVER to transfer files created by the Tape Transfer process. The background batch run will have the "O" execute option set to cause all PSERVER message traffic to be sent to a system console. The background batch run will have the "U" execute option set, which allows PSERVER to transfer files that have the SV bit set.

- *(S103.610.09: CAT II) The SA will ensure the background batch run execution of PSERVER has the "BOU" execute options set.*

12.1.6 Securing PSERVER

The file containing the PSERVER routing tables (for example, PS$$0000*00) will be secured by using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. This will prevent users that do not have the BYACR Privilege from modifying the PSERVER routing tables but will allow read only access. To attach ACR ACRRO, do the following:

```
@SIMAN,B
UPDATE FILE = PS$$0000*00.
ATTACH_ACR = ACRRO          ACR_OWNER = EXEC8 ;
DISPLAY FILE = PS$$0000*00. ;
```

This will attach ACR ACRRO (*read-only*) to the PS$$0000*00 file. It will then display the file. The file will show the ACR attached. The only users that may update elements in the file are those with ACR bypass privileges (site personnel). All users can read elements in the file. If the site uses a unique ACR, replace occurrences of ACR ACRRO with the unique ACR and the ACR owner of EXEC8 with the owner of the unique ACR.

The following automated procedure may also be used to secure the PSERVER file. Start the JX$$0000*00.NJX0PS job with the Security Officer's userid and the Master Account. Notice that this job will report the number of errors encountered during both the ACR install and ACR attach segments. Review the printed output to identify and resolve any errors.

- *(S103.610.00: CAT II) The SA will ensure the PSERVER routing tables are secured with ACR ACRRO, or an ACR like ACRRO to protect them from modification by unauthorized personnel.*

12.2 DDP-FJT Tape Transfer Facility (TXFR)

12.2.1 Overview

The Tape Transfer Facility (TXFR) is a Unisys product that allows local host users to transfer tape files from a tape device on one OS 2200 host to a tape device on another OS 2200 host that also has Tape File Transfer configured. TXFR can be used to transfer single-reel or multi-reel, labeled or unlabeled, catalogued or uncatalogued tape files in any of the following formats: FURPUR-formatted, System data format (SDF), Quarter-word frame format, 6-bit packed frame format, or 8-bit packed frame format. Each tape file transfer involves the following hosts: Sending host where the tape originally resides, Receiving host to which the tape is being transferred, and Initiating host, which is the local host for the user who initiates the transfer. The initiating host may be the sending host, receiving host, or another host.

For the TXFR process to work properly, the correct Executive configuration statements, PSERVER configuration statements, and TXFR configuration statements must be identified on the sending, receiving, and initiating hosts. The TXFR process requires the following files:

SYSLIB*TXFR-STATUS	Tape File Transfer Status File
SYSLIB*TXFR-POOLREG	Tape Pool Registration File
SYSLIB*TXFR-CONFIG	Tape File Transfer Configuration File

12.2.2 Securing the TXFR Configuration File

Information in the TXFR Configuration File ensures that tape file transfers are only received from authorized sources. To protect this file from modification by unauthorized personnel, the file containing the Tape File Transfer Configuration will be secured using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. Reference the procedures in *Section 12.1.6,* Securing PSERVER, for an example of how to attach ACR ACRRO.

- *(N/A: CAT II) The SA will ensure the Tape File Transfer Configuration file is secured with ACR ACRRO, or an ACR like ACRRO to protect it from modification by unauthorized personnel.*

12.2.3 DDP-FJT Tape Transfer Userids

The Air Force HQ Standard Systems Group (HQ SSG) and SSO Montgomery personnel utilize the DDP-FJT Tape Transfer Processor, TXFR, to initiate tape-to-tape transfers of approved software releases to certain OS2200 hosts. Two specific userids have been assigned to these organizations for this process. Detailed security requirements for these userids are contained in Section 3.1.9.6.

12.3 QTPIE - ALN

12.3.1 Overview

QTPIE, developed by SSO Montgomery, functions much like PSERVER and is used to redirect print files. The routing table for this software is normally located in the 0DP00000*PMSCRQ055-DP file or a site-specific file. The QTPIE routing table will be secured to prevent modification by unauthorized personnel. The QTPIE absolute, for those sites that are running an ALN operating system, is located in SYSLIB*USAF-SECURE, which is automatically secured with the ACR GUJXFG.

12.3.2 Securing QTPIE

The routing table file will be secured using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. Reference the procedures in *Section 12.1.6,* Securing PSERVER, for an example of how to attach ACRRO. If there are other programs or elements in that file that users need access to, move the QTPIE routing tables to a file that can be secured. If the site is not running the ALN operating system, you need to also secure the QTPIE absolute.

- *(S103.620.00: CAT II) The SA will ensure the QTPIE routing table is secured with ACR ACCRO, or an ACR like ACRRO to protect it from modification by unauthorized personnel.*

12.4 PDQ

12.4.1 Overview

PDQ, developed by SSO Montgomery, is another print directing utility and presents the same risks as PSERVER and QTPIE. The routing table for this software resides in a print utility file, in most cases PS$$0000*00, and will be secured to prevent modification by unauthorized personnel.

12.4.2 Securing PDQ

The file containing the PDQ routing tables will be secured using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. Reference the procedures in *Section 12.1.6,* Securing PSERVER, for an example of how to attach ACR ACRRO. If there are other programs or elements in that file that users need access to, move the PDQ routing tables to a file that can be secured.

- *(S103.630.00: CAT II) The SA will ensure the PDQ routing tables are secured with ACR ACRRO, or an ACR like ACRRO to protect them from modification by unauthorized personnel.*

12.5 AB Utilities and Routing Tables - ALN

12.5.1 Overview

The AB utilities and tables, developed by SSO Montgomery, are another means of directing print and presents the same risks as PDQ, PSERVER, and QTPIE. The AB utilities can reside in files AB*00, AB$$0000*00, or AB$$<ALN>*00, and the routing tables for these utilities can reside in files AB*AABP0D and AB*AABP0M, 0AB000000000*AABP0D and 0AB000000000*AABP0M, or 0AB0<ALN><PLN>00*AABP0D or 0AB0<ALN><PLN>00*AABP0M. Any AB files of this nature will be secured to prevent modification by unauthorized personnel.

12.5.2 Securing AB Utilities and Routing Tables

The files containing the AB utilities and routing tables will be secured using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. Reference the procedures in *Section 12.1.6,* Securing PSERVER, for an example of how to attach ACR ACRRO. If there are other programs or elements in these file that users need access to, move the AB utilities and routing tables to other files that can be secured.

- *(S103.650.00: CAT II) The IAO will ensure that the AB utilities and routing tables are secured with ACR ACRRO, or an ACR like ACRRO to protect them from modification by unauthorized personnel.*

12.6 Output Manager

Output Manager (formerly DEPCON) is a Unisys product used to distribute print files to network printers. It has two components, the Unisys IX mainframe print server/client and the Windows based DEPCON print server/client. Unisys has recently renamed this product Output Manager but for clarity, it will continue to be referred to as DEPCON.

12.6.1 DEPCON on Unisys IX Mainframe

On the OS 2200 system DEPCON can be configured as a client and as a server. As a client it will send print files queued to system print queues to the DEPCON Windows print server. This allows mainframe print files to be printed along with additional functionality that will be discussed in *Section* 12.6.2 DEPCON on Windows System.

12.6.1.1 Configuration Statements

DEPCON has six configuration statements of particular security concern and they are; KEYTYPE, TCP-PROCESS, TSAM-PROCESS, LPR-PROCESS, RECEIVE, and TSAM-PEER.

12.6.1.1.1 KEYTYPE Configuration Statement

The configuration statement KEYTYPE is used to define the keyin used to communicate with the DEPCON background run while it is executing. By default the value for this keyin is DEPCON. The format of this statement is:

KEYTYPE *keyin-type*

Where *keyin-type* is the value used to start the keyin command for this DEPCON. It must be unique to all other keyin values, system defined or user defined, be up to 8 alphanumeric characters, it may contain an asterisk (*), and must not start with a numeric. Since systems do not contain an asterisk, it is recommended that one be used in this keyin.

Since any user granted CONS privileges at any level are allowed to execute KEYIN$ keyins and there are destructive DEPCON commands that would impact the availability of DEPCON or its functionality, there will be a KEYTYPE statement in the DEPCON configuration and it will not have the value DEPCON.

- *(S103.640.01: CAT II) The SA will ensure there is a KEYTYPE statement in DEPCON configurations.*

- *(S103.640.02: CAT II) The SA will ensure the value of the second field of the KEYTYPE field is not DEPCON.*

12.6.1.1.2 RECEIVE Statement

The RECEIVE statement allows the DEPCON mainframe component act as a server receiving print files from other DEPCON clients, either mainframe or PC based and queuing the to local print queues. Since the ClearPath IX no longer supports any directly attached printers, the RECEIVE statement should not be present in any DEPCON configuration. Since the DEPCON component on the mainframe should not be allowed to receive files, the following statements should not be present in the DEPCON configuration.

ASG-DEVICE
ASG-PACKID
ASG-SIZE
FILE-ACCESS
QUAL-FILE

If a site must use the RECEIVE statement to satisfy operational requirements, a QUAL-FILE statement will also be used. The QUAL-FILE statement will be in the format QUAL-FILE QUAL-H1,QUAL-H2,FILE-H1,FILE-H2. Use of additional subfields on the QUAL-FILE statement is optional.

- *(S103.640.03: CAT II) The SA will ensure, if the RECEIVE statement is used, a QUAL-FILE statement is also used.*

- *(S103.640.04: CAT II) The SA will ensure the QUAL-FILE statement has the following format:*
  QUAL-FILE QUAL-H1,QUAL-H2, FILE-H1,FILE-H2.

12.6.1.1.3 TCP-PROCESS, TSAM-PROCESS, and LPR-PROCESS Statements

These three statements are all references to CMS 1100 or CPCOM TSAM process statements. Since these processes could be hijacked by malicious code the values found for the password field will never be one used in an example configuration. The TSAM-PROCESS statement also contains an optional TSEL-NAME field. If the TSEL-NAME field is used the second subfield of this field will not contain any values from any example configurations.

- *(S103.640.05: CAT II) The SA will ensure the PASSWORD field of these statements does not contain any value found in any example configurations.*

- *(S103.640.06: CAT II) The SA will ensure the TSEL-NAME field of the TSAM-PROCESS statement does not contain any value found in any example configurations.*

12.6.1.1.4 TSAM-PEER Statement

The TSAM-PEER statement has four subtypes. The TSAM-PEER statements with the TRANSPORT=OSI or TRANSPORT=DCA should not be used. The remaining TSAM-PEER statements are distinguished by the TRANSPORT= field and are described below.

12.6.1.1.4.1 TRANSPORT=TCP

The TSAM-PEER statement with the TRANSPORT=TCP field is used to describes a TCP/IP connection that will be used by the TIP LPR process to send LPR/LPD style print from a TIP PID session to a printer or print server that understands the LPR/LPD protocol. Since the LPR/LPD protocol transmits data in ASCII text format, the destination net address of the destination should be within the local network.

12.6.1.1.4.2 TRANSPORT=TP0

The TSAM-PEER statement with the TRANSPORT=TP0 format describes a TCP/IP connection that uses the TP0 protocol to transmit print files from one DEPCON peer to another. In this case from the mainframe to the DEPCON PC print server. Since the TP0 protocol does not use encryption the net address of the destination should be within the local network. This statement also contains an optional TSEL-NAME field and the TSEL-NAME field will not contain any value found in a sample configuration.

- *(S103.640.07: CAT II) The SA will ensure the TSEL-NAME field does not contain any value found in a sample configuration.*

12.6.1.2 Userid Requirements

The DEPCON background run's userid will be a batch only userid, it will be disabled and it will not have any privileges except the following:

BYACR
BYCOMPMT
BYOWNER
BYCL
BYPRVFLC
BYRWKEY
BYRWMODE
COM$PRV
CREEXCLG
MODRECCL
SMOQUE

These privileges are required so that DEPCON can assign and transfer any file found on a configured print queue by overriding any MAC or DAC restrictions placed on the file. Additionally the batch runstream must be privileged prior to the execution of the DEPCON absolute, either by assigning DLOC$ correctly or use of a utility such as SYSLIB*COMUS.CLOD.

NOTE: Testing has shown that the following privileges are not needed nor is does the run need to be privileged. Therefore the userid that is used for the DEPCON background run should not have the following privileges and should not be privileged.

BYACR
BYCOMPMT
BYCL
BYPRVFLC
BYRWKEY
BYRWMODE

- *(S103.640.08: CAT II) The SA will ensure the DEPCON batch run userid is batch only.*
- *(S103.640.08: CAT II) The SA will ensure the DEPCON batch run userid is disabled.*
- *(S103.640.08: CAT II) The SA will ensure the DEPCON batch run userid only has the privileges allowed by this STIG.*

12.6.1.3 Account Requirements

There is only one general account requirement for the DEPCON background run. The account must allow realtime execution if DEPCON is configured to run realtime. In an ALN system the account must be an exempt account since DEPCON must be able to read any print file it finds on a system print queue regardless of who sent it.

- *(S103.640.09: CAT II) The SA will ensure the DEPCON background run account is allowed realtime privilege.*

For ALN:

- *(S203.640.09: CAT II) The SA will ensure the DEPCON background run account is an ALN exempt account.*

12.6.1.4 EXECUTION requirements

The execution of the DEPCON absolute in the background runstream will not contain the "Y" option which allows users with "FULL" console mode or better to answer the read and reply messages generated by DEPCON for commands entered to DEPCON entered from a remote console (@@CONS) terminal.

The background batch run will have the "O" execute option to cause all DEPCON message traffic to be sent to a system console.

The background batch run will have the "S" execute option to restrict the reception of files to hosts configured on the TSAM-PEER statements.

- *(S103.640.10: CAT II) The SA will ensure the background batch run execution of DEPCON does not have the "Y" execute option set.*

- *(S103.640.10: CAT II) The SA will ensure the background batch run execution of DEPCON does have the "O" execute option set.*

- *(S103.640.10: CAT II) The SA will ensure the background batch run execution of DEPCON does have the "S" execute option set.*

12.6.1.5 Securing DEPCON Configuration File

The file containing the DEPCON routing tables will be secured using an ACR such as ACRRO or a site unique ACR that restricts write and delete actions to select site personnel. Reference the procedures in *Section 12.1.6, Securing PSERVER*, for an example of how to attach ACR ACRRO. If there are other programs or elements in that file that users need access to, move the DEPCON routing tables to a file that can be secured.

- *(S103.640.00: CAT II) The SA will ensure the DEPCON routing tables are secured with ACR ACRRO, or an ACR like ACRRO to protect them from modification by unauthorized personnel.*

12.6.2 DEPCON on Windows System

The DEPCON client server that runs on a Windows based system is a multi function program that receives print files from multiple sources, then, using selection criteria can reformat the print file following user defined rules and then send the reformatted files to other systems or network and locally attached printers. We are specifically interested in the functionality where DEPCON receives files from the ClearPath mainframe component and converts the file format from a native OS 2200 print file to an ASCII text file. Then, by applying rules, prints the resulting files or mails them to a user.

The directions here apply to DEPCON level 5R1 and above. This is not designed to be an in-depth configuration manual for DEPCON but to cover those features and configuration requirements that effect security.

12.6.2.1 System Requirements

DEPCON will be installed on a Windows system. DEPCON stores plain text copies of all files to be printed in its working directories, which by default are subdirectories to the installation DEPCON directory. DEPCON allows the configuration of other directories for interim print files and should be configured to use directories other than the default subdirectories to segregate data from the software. All DEPCON system directories and Group Print Hold directories will be restricted to the user(s) allowed to run the DEPCON server software. This requirement does not apply to customer's directories, which are used by DEPCON to store the customer's copy of the print file.

- *(S103.640.12: CAT II) The SA will ensure all DEPCON system directories and Group Print Hold directories are restricted to user(s) allowed to run the DEPCON server software.*

12.6.2.1.1 DEPCON Userid Requirements

Because DEPCON in the Windows environment will not run as a service, and it would be necessary to shutdown the DEPCON process for a new userid to sign on to operate DEPCON, the userid used to run DEPCON may be a group userid. The DEPCON userid will have the minimum domain privileges need to accomplish its task but it may be a local administrator on the DEPCON server. Since the userid used to run DEPCON should be a group userid no other processes will be run on this server. Additionally, since a group userid is used to run DEPCON, the DEPCON Windows Server will be maintained in a secure environment as required by the highest security level of objects transferred.

- *(S103.640.13: CAT II) The IAO will ensure the DEPCON Windows is physically secured to the level required of the highest security objects transferred.*

12.6.2.1.2 Printing Requirements

The userid running DEPCON should have access to the network printers that DEPCON uses. Because DEPCON does not encrypt files, all printers that will be accessed should be on the local

intranet network. The use of encrypted tunnels should be encouraged when spanning other networks.

12.6.2.1.3 DEPCON Configuration

DEPCON has a large number of configuration parameters, many of which can be misused to change the destination of a print file. Therefore, it is necessary to secure both the physical machine that DEPCON runs on and the DEPCON configuration password. Additionally the directory that contains the DEPCON configuration, the directory where DEPCON is installed, will be restricted to users that run DEPCON or need to configure DEPCON.

12.6.2.1.3.1 DEPCON Configuration Password

The DEPCON configuration will be protected by a password. This password will be known only to personnel who configure DEPCON. The Depcon Server Administrator will establish a procedure to ensure that the password is changed on a 90 day interval.

- *(S103.640.15: CAT II) The SA will ensure DEPCON has a configuration password.*
- *(S103.640.16: CAT II) The SA will ensure the DEPCON configuration password is known only to personnel who configure DEPCON.*
- *(S103.640.17: CAT II) The DEPCON SA will establish a procedure to ensure the password is changed every 90 days.*

12.7 Print Viewing Utilities

These utilities use the SMOQUE$ Interface to view or move print files that reside in one of the system print queues. Processors include @SMOQ, @SQ, @SM-USE, @Q, and @SMQ. Regardless of which of these is used at the site, certain restrictions will be implemented to preserve system integrity.

First, most functional users need to be prevented from accessing and moving print files not directly created by them or their processes. Some high level functional users (for instance, application group managers) may be given greater span of control in order to manage print products for their entire application or site. When possible, users of one application will be restricted from accessing print files generated or controlled by another application.

In an ALN environment, non-exempt users will be restricted from accessing or moving print files created under another ALN. Since the @SMQ processor has not been *ALNized* or otherwise restricted, non-exempt users can not have access to the file @SMQ resides in. Under the ALN operating system, the Executive Interface TERMRUN$ allows a non-exempt user to access print files created by another user within his or her ALN by using the @SMOQ or @SQ processors. Access to this interface will be justified and documented on a request letter to the IAO. The functional data owner will sign the letter. This letter can be consolidated with the EZLOAD, IQU, or DBE request letter. Specific capabilities of TERMRUN$ in conjunction with @SMOQ and @SQ are detailed below.

USERID/ACCESS TO PRIVILEGE	*@SMOQ*	*@SQ*
ALN Exempt/No TERMRUN$	Security Error	Access to All Files
ALN Exempt/TERMRUN$	Access to All Files	Access to All Files
Non-Exempt/No TERMRUN$	User Files Only; Security Error with Others	User Files Only; No Info with Others
Non-Exempt/TERMRUN$	All Files within ALN	All Files within ALN

Table 11-4. TERMRUN$ and ALN Print Utilities Functionality

- *(S104.600.00: CAT II) The SA will ensure access to print viewing utilities are restricted in accordance with this STIG requirements.*

13. SOFTWARE DEVELOPMENT

In general, software development will not be done on production domains unless the production workload is separated from the development workload or the DAA accepts the level of risk associated with this function. In an ALN environment, this may involve the creation of a special ALN for the development function. Other services may be required to pursue other means of workload separation (e.g., unique qualifiers), or acquisition of a separate domain for software development. Software configuration management policies will be implemented and strictly enforced to ensure untested software is not inadvertently loaded to production software files.

- *(S101.040.00: CAT II) The IAO will ensure software development on a production system is separated through the use of a separate ALN or unique qualifiers.*

- *(N/A: CAT II) The IAO will ensure software configuration management policies are implemented and strictly enforced to ensure untested software is not inadvertently loaded to production software files.*

13.1 Language Compilers

There are many Unisys and third party compilers available for the Unisys OS2200 system. Among these are the Universal Compiling System (UCS) products, the ASCII compiler products (ACOB, etc.), and the Meta-Assembler (MASM) product. These products support basic and extended mode programming and have many low-level interfaces into Exec code. Because of the risk involved in the development and testing of software on a production system, SSO Montgomery has removed as many of these products as possible from the software delivered to the sites for production systems that Montgomery supports. Unless authorized by SSO Montgomery these product will not be installed on any system they support.

NOTE: Not all of the compiles can be removed because of the way the runtime libraries are packaged by Unisys.

Dedicated Development Only Domains

If a system is only used for software development and processes no production workload, the following deviations from this STIG policy are allowed:

a. Application software developers may require multiple userids, such as one for software development and one for unit test purposes. The standard security profile for dedicated Central Design Activity (CDA) programmers is a Profile 4; however, local conditions may require that some or all of these userids have additional Interfaces and Privileges. All exceptions will be documented on the SAAR for the particular users.

b. System software developers may require multiple userids, such as one for software development and one for unit test purposes. The general rule of thumb to use when assigning a security profile to system software developers is to use a profile similar to, but not identical to, a site technical support or system analyst counterpart. For example, the STAR AIS manager at the CDA SSO Montgomery will have a profile similar to a site

STAR tape librarian. This rule is not perfect, as additional Privileges may be needed in order for the AIS manager to successfully accomplish his/her duties as a system software developer. In all cases, decisions will be based on the concept of least privilege. In cases dealing with the development and unit testing of security-related software, the AIS developers may require IAO level Privileges. The requirement for IAO capabilities will require an agreement between the developer and the site to help identify and reduce the additional risk involved. All exceptions will be documented on the SAAR for the particular users involved.

c. Independent test organizations may require multiple userids to simulate different levels of users in a typical site environment. The general rule of thumb to use when assigning a security profile to independent test activities is to use a similar profile as a site technical support or system analyst counterpart. For example, the STAR AIS manager at the test organization will have a profile similar to a site STAR tape librarian. This rule is not perfect, as additional privileges may be needed in order for the quality assurance evaluator to successfully accomplish his/her duties as a system or application software evaluator. In all cases, decisions will be based on the concept of least privilege. In cases dealing with the unit and integration testing of security-related software, the quality assurance evaluator may require IAO level privileges. The requirement for IAO capabilities will require an agreement between the test organization and the site to help identify and reduce the additional risk involved. All exceptions will be documented on the SAAR for the particular users involved.

d. If the development or test environment is an ALN environment and there is no need to separate users on a given domain by ALN, the site IAO may give the developer or quality assurance evaluator access to an ALN exempt account or allow the developer or quality assurance evaluator to enter a project-ID or account at sign-on time. This requirement will be documented on the individual's SAAR.

13.2 Shared Production/Development Domains

If software development is accomplished on a shared production/development system, the only deviations from this STIG deal with the assignment of profiles to application programmers and the profile distribution associated with these users. On shared production/development systems, application programmers are authorized to have a PROFILE/DNMC, Profile 5, Profile 6, or Profile 7. On these domains, profile distribution should reflect the guidelines shown in the Profile Distribution matrix in *Section 3.1.12.11, Unisys User Profile Distribution Guidelines.*

- *(S101.040.00: CAT II) The SA will ensure authorized profiles for application developers on shared production/development systems are Profiles 5, 6, or 7.*

- *(S101.040.00: CAT II) The IAO will ensure the profile distribution of Profiles 5, 6, and 7 on shared production/development domains are as designated in Section 3.1.12.11, Unisys User Profile Distribution Guidelines.*

APPENDIX A. RELATED PUBLICATIONS

A.1 Government Publications

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

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

Chairman Of The Joint Chiefs Of Staff Manual (CJCSM) 6510.01, "Defense-In-Depth: Information Assurance (IA) And Computer Network Defense (CND)" 25 March 2003

DOD Instruction 5200.40, DOD "Information Technology Security Certification and Accreditation Process (DITSCAP)", 30 Dec 97

DISA Enclave Security Technical Implementation Guide.

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

Defense Logistics Agency Regulation (DLAR) 5200.17, "Security Requirements for Automated Information and Telecommunications Systems," June 9,1993.

Army Regulation (AR) 380-19, "Information Systems Security," February 27,1998.

Secretary of the Navy Instruction (SECNAVINST) 5239.2, "Department of the Navy Automated Information Systems Security (INFOSEC) Program," July 14, 1995.

Navy Staff Office Publication (NAVSO Pub) 5239-15, "Controlled Access Protection Guidebook," December 1994.

A.2 Commercial Publications

Most Unisys documentation can be accessed online from Unisys using the following procedure:

a) Go the URL http://www.support.Unisys.com/.
b) Click on the documentation link.
c) Read and agree to the Terms of Use.

This will take the user to a list of current online documentation. The documentation primarily of interest is in the ClearPath IX/2200 section. However, the MAPPER documentation is found in a separate section. There is also a section for Single Point of Operations.

Unisys/Team Quest 7831 0661, Site Management Complex (SIMAN) Administration and End Use Guide.

Unisys 7831 0307, OS 2200 Security Planning and Administration Reference Manual.

Unisys 7862 1760, Security Administration for ClearPath OS 2200 Help, replaces Unisys 7831 0307 in HMP IX 7.0.

Unisys 7831 0885, Security End Use Guide.

Unisys 7831 0315, System Log Operations and Support Reference Manual.

Unisys/Team Quest 7830 7436, Log Analyzer (LA) Administration and End Use Reference Manual.

NOTE: SSO Montgomery will supply any current Unisys and Teamquest documentation to sites supported by SSO Montgomery upon request.

APPENDIX B. GLOSSARY OF ACRONYMS AND TERMS

B.1 Acronyms

ACR	Access Control Record
ADP	Automated Data Processing
ADPE	Automated Data Processing Equipment
ADPF	Automated Data Processing Facility
ADPS	Automated Data Processing System
ADS	Automated Data System
AIS	Automated Information System
ALN	Access and Location Number
ATO	Authority to Operate
BDI	Bank Descriptor Indicator
BLISS	Base Level Integrated Support System
CAMS	Core Automated Maintenance System
CDB	Centralized Database
COTS	Commercial-Off-The-Shelf (Software)
CP OS 2200 n.n	Software release that level that runs on a Unisys ClearPath IX machine. (n.n = 7.1, 8.0, 8.1 etc) New vender designation.
CPU	Central Processing Unit
DAA	Designated Approval Authority
DBE	Database Editor
DCP	Distributed Communications Processor
DECC	Defense Enterprise Computing Center (previously DMC)
DECC-D	Defense Enterprise Computing Center -Detachment
DEPCON	Distributed Enterprise Print Control
DFAS	Defense Finance & Accounting Service
DISA	Defense Information Systems Agency
DNMC	Defense-Navy-Marine Corps
DOD	Department of Defense
DSAWG	DISN Security Accreditation Working Group
DTIC	Defense Technical Information Center
EAL	Evaluation Assurance Level
ECL	Executive Control Language
ELC	Enterprise Location Code
ER	Executive Report
HMP	Heterogeneous multiprocessing
HMP IX n.n	Software release that level that runs on a Unisys ClearPath IX machine. (n.n = 5.1, 6.0, 8.1 etc)
HQ SSG	Headquarters Standard Systems Group
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IATO	Interim Authority to Operate
IMDS	Integrated Maintenance Data System
IPF	Interactive Processing Facility
IPL	Initial Program Load
IQU	Interactive Query Utility

LA	Log Analyzer
LAN	Local Area Network
MAC	Mission Assurance Category
MAJCOM	Major Command
MSP	Main Storage Partition
MUX	Multiplexer
NMS	Network Management System
OPR	Office of Primary Responsibility
PC	Personal Computer
PID	Position Identifier
PKI	Public Key Infrastructure (PKI)
PMP	PID Management Processor
QLP	Query Language Processor
REMIS	Reliability & Management Information System
SA`	System Administrator
SBLC	Standard Base Level Computer
SBn	System Base n (such as SB4, SB5, etc.)
SECMGR	Security Administration Processor
SIMAN	Site Management Complex
SMC	Systems Management Center
SOA	Separate Operating Agency
SSG	Symbolic Stream Generator
SSO	Systems Support Office
SSP	System Support Processor
ST&E	System or Security Test and Evaluation
TASO	Terminal Area Security Officer
TIP	Transaction Processing
TIWADS	TIP Interface With ADS
USIT	Unisys Security Integrated Toolkit
WAN	Wide Area Network

B.2 Terms

Account. All AIS users on the site platforms will be arranged by standard accounts. Accounts can be ALN-exempt (sometimes called Privileged), non-exempt, or Service defined.

Access. The ability of a user to communicate with, pass data through, or have entry to a site component or system. It is also used to describe entry to a specified Restricted area. This definition does not include those persons (customers) who simply receive products created by the system and who do not have communications or other interface with the ADPS or its personnel.

Access Control Record (ACR). An object in SIMAN that specifies a group of users by some attribute (userids, accounts, project-IDs, etc.) and the type of access allowed to that group. This ACR is then attached to either files or userids. Access to these objects is then restricted to those users who meet the requirements of the ACR. Files with an ACR attached are considered semi-private.

Accreditation. Official DAA authorization to place a system in operation. See also DITSCAP.

Access and Location Number (ALN). At a site, this number can be used to distinguish workloads from different remote sites. This concept is tied to a special version of the Unisys operating system developed for the DECC Air Force supported environment and is usually referred to as the "ALN Exec." Initially, the ALN assigned to a base will be the same as that site's old DPC number.

Applications Programs. Those routines designed by or for ADPS users and customers to complete specific, mission-oriented tasks, jobs or functions, using available ADP equipment and software.

Approval or Authority to Operate (ATO). Represents agreement by the DAA that a satisfactory level of security exists. That is, minimum requirements are met and there is an acceptable low level of risk. The DAA authorizes the operation of an AIS at an ADPF.

Automated Data Processing Facility (ADPF). The physical resources, including structures or parts of structures, which house and support data processing capabilities. For each computer facility designated as a site, the ADPF is the site. For small computers, the ADPF is the physical area in which the computer is located.

Automated Data Processing Resources. The totality of ADP equipment, software, data, time, contractual services, personnel, and supplies.

Automated Data Processing Security Plan. The overall plan for providing security throughout the life-cycle of an automated project or program, AIS, or ADPF.

Automated Data System (ADS). A system on the mainframe that controls the automated functions for a specific group of users (CAMS, Accounting and Finance, Supply, etc.). This term is being phased out in favor of Automated Information System.

Automated Information System (AIS). An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control information. A system on the mainframe that controls the automated functions for a specific group of users (CAMS, Accounting and Finance, Supply, etc.).

Batch [Mode]. A mode of Unisys processing where all input and processes are defined and no interactions with a user are required, other than possibly scheduling.

Batch (SIMAN). An interactive means of performing commands in SIMAN without the use of screens. SIMAN batch runstreams are written in this command language.

Certification. A statement by the appropriate official (AIS or ADPF) of the extent to which the security measures in the system or facility meet technical specifications and security requirements. It is based upon the results of a risk analysis and does not necessarily imply a guarantee that the system described is impenetrable. It is submitted to the DAA as part of the Accreditation Package. See also DITSCAP.

Class. Hierarchical ranks denoting a certain level of trust based on DOD 5200.28-STD (the Orange Book).

Clearance Level. One of 64 (0 – 63) designated levels in SIMAN that determines file access sensitivity. Virtually all user or application files and the vast majority of system-level files on the Unisys mainframes are cataloged at clearance level 0 (zero).

Controlled Access. The process of limiting access to the resources of an AIS only to authorized personnel, users, programs, processes, or other ADP systems (computer networks).

Controlled Area. An environment, considered in part or as a whole, where all types and aspects of access are checked and controlled.

Conversational Timesharing System (CTS). An interactive program development capability used for producing software. This language is no longer supported by Unisys and all programs written in CTS should be converted to IPF.

Customer. A person or organization that receives products produced by an AIS, but who does not necessarily have any means of access to the system (see Access).

Data Owner. The authority, individual, or organization who has original responsibility for the data by statute, Executive order, or Directive.

Data Processing Center. Refers to a stand-alone mainframe computer site rather than a site.

Demand [Mode]. An interactive mode of processing where input is required from the user, usually by commands rather than transactions.

Designated Approval Authority (DAA). An official designated to approve the operation of ADP systems at the ADPF(s) under his or her jurisdiction for processing classified or sensitive unclassified information, or for critical processing.

DITSCAP. DOD Information Technology Security Certification and Accreditation Process.

Enclave. A network under the operational control and authority of a single organization with the responsibility to define and implement security controls. A group of one or more security domains that typically share close physical proximity and that can have a clearly defined perimeter. Within DOD, this could be a tenant activity located on a base controlled by another organization. The tenant activity is expected to have a firewall at the perimeter of its network "enclave" and additional internal firewalls to separate different security domains.

Executive (EXEC-8). Unisys 2200 Executive System, as used in this publication. Synonymous with operating system, monitor, Master Control Program, and supervisor.

Executive Interface. An instruction that causes a special interrupt requesting Executive Service such as input, output, time of day, or elapsed time. Also, the service resulting from the request.

This is the standard interface between application programs and the Executive. This term replaces the term Executive Request.

Executive Request. An instruction that causes a special interrupt requesting Executive Service such as input, output, time of day, or elapsed time. Also, the service resulting from the request. This is the standard interface between application programs and the Executive. This term has been changed to Executive Interface.

Exempt. This term refers to an account or project-ID or job that is exempt from ALN replacement. For the most part, this will be limited to system jobs and DPC/site userids.

Extended Security. The portion of SIMAN that controls clearance levels, subsystem access, ERs (Interfaces), Privileges, and cataloged file security.

Firewall. A system designed to defend against unauthorized access to or from a private network. Firewalls can be implemented in hardware and software, or a combination of both.

Field Assistance Branch (FAB). The FAB is the primary point of contact for all functional or operational problems that require assistance that may be unavailable at the site, stand-alone data processing center, or customer site.

Gang. An independent database under an ALN.

Interactive Processing Facility (IPF). The approved text editor that is fully supported by Unisys. This editor replaces CTS and ED. It comes with HELP menus, DDP commands, and full-screen text options.

Internal Security Controls. Hardware, firmware, and software features within an AIS that restrict access to passive “objects” (hardware, firmware, software, and data) by only authorized active subjects (persons, programs, or devices).

Keys. Any password associated with a file. There are read keys and write keys.

Material. Refers to any data processed, stored, used, or generated by an AIS such as programs, reports, data sets, files, and records.

MODPS$. A secured Executive Interface that activates certain secured Privileges.

Network. Two or more computer systems connected by a communications medium.

Non-Exempt. This term refers to accounts, project-IDs, or jobs that are subject to ALN replacement.

Password. In ADP systems, a protected string of characters that is used to authenticate the identity of an individual user for access to a site or DPC component. It is known only to that user.

Personal Computer (PC). A computer small enough to fit on a user's desk. Also called a microcomputer. A personal computer may be connected to a mainframe via a MUX, DCP, and/or LAN.

Privilege. One of a set of capabilities controlled by the Unisys security system and/or the SIMAN security processor.

Privileged Mode. Privilege Mode allows a user access to all DLOC$ Privileges associated with their userids.

Profile. Any of the user groupings or categories that are defined according to the job the user performs.

Project-ID. Each userid has a project-ID defined in its SIMAN record, and that project-ID is the default file qualifier for that userid. Project-IDs will be standardized and can be Exempt, non-Exempt, or Service determined.

Residual Risk. That portion of risk that remains after security measures have been applied.

Risk. The loss potential that exists as the result of threat vulnerability pairs. Reducing either the threat or vulnerability reduces risk.

Risk Analysis. A part of risk management that is used to minimize risk by effectively applying security countermeasures commensurate with the relative threats, vulnerabilities, and value of resources to be protected. It may be thought of as consisting of four assessment modules: Sensitivity, Risk, Economic, and Security Test and Evaluation.

Risk Assessment. A detailed study of the vulnerabilities, threats, likelihood estimates, loss or impact, and theoretical effectiveness of security measures. The results of risk assessment may be used to develop security requirements, specifications, and countermeasures.

Security Incident. Any act or circumstance that involves sensitive information in which there is a deviation from the requirements of governing security regulations (e.g., compromise, inadvertent disclosures, need-to-know violations, and administrative practice deviations).

Security Mechanisms. Elements of software, firmware, hardware, or procedures included in a system to satisfy the security requirements for that system.

Security Officer. The individual responsible for monitoring, evaluating, and ensuring procedures and controls for AIS security. Additionally, Unisys uses this term to refer to the owner of the master userid or the "Security Officers Userid". This is the most privileged userid on a Unisys system.

Security Record (SIMAN). The portion of the SIMAN userid record that resides in the SYS$*SACRD$ file.

Security Test and Evaluation (ST&E). The process used to determine if the system's administrative, software, technical, and physical security measures are adequate.

Sensitive. Confidentiality level between public and classified.

Sensitive Processing Resources. Those resources that will be protected because their compromise, alteration, destruction, or loss will adversely affect the security of classified, proprietary, personal, or other information, which has been restricted by competent authority from general disclosure. This includes information used to manage sensitive resources such as high dollar value, munitions, and personnel records.

Sensitive Unclassified Information. Information that requires protection due to the risk and magnitude of harm or loss that could result from unauthorized disclosure, alteration, loss, or destruction. Privacy Act and "For Official Use Only" data is included in this definition.

Significant Modification. Any modification to the ADPF or AIS that impacts the operations of the system or affects the security measures of the system.

Site Management Complex (SIMAN). The overall security processor for Unisys mainframes. SIMAN defines security parameters on such things as user Privileges and sign-on parameters, ACR maintenance, file security, Quota maintenance, account maintenance, and steps taken upon unauthorized sign-on.

Skeleton. A control structure used by the Symbolic Stream Generator to construct symbolic data.

Symbolic Stream Generator (SSG). A system-provided capability for generating runstreams from user specified inputs.

System Administrator. System Administrator is a privileged user with IA responsibilities these responsiblities are detailed in the 8500.2. Establishes and managesauthorized user accounts for DOD information systems, including configuring access controls to enable access to authorized information and removing authorizations when access is no longer needed.

SYS$*ACCOUNT$R1. The standard file name of the SIMAN Security System database containing user account information.

SYS$*SACRD$. The standard file name of the SIMAN Security System database containing Access Control Records and user Privileges.

SYS$*TSS$FILE. The standard file name of the SIMAN Security System database containing access authorization information.

Threat. The possible exploitation of a vulnerability.

Threat Agent. Those methods and capabilities such as fire, natural disaster, etc., which may be used to exploit the vulnerability in an ADP system, facility, or operation.

Transaction Processing (TIP). A functional mode of processing that is extremely fast and oriented toward processing full-screen information and single transactions.

TIP Interface with ADS (TIWADS). An Air Force-unique security interface function for TIP mode only.

User. An individual or organization with the ability to access site or DPC components.

User Identifier (Userid). A unique string of characters used to identify a user to a, site or DPC component.

Vulnerability. A weakness in ADPS security procedures, administrative controls, internal controls, or practices that could be exploited by a threat agent to gain unauthorized access to sensitive information (classified or unclassified but sensitive) or to disrupt critical processing.

APPENDIX C. ACCESS AND LOCATION NUMBER INFORMATION

This appendix contains service-specific security information that applies to all sites running the Access and Location Number (ALN) operating system. When the main STIG document refers to the "service-specific appendix," this is the location to reference if the user is the security officer at a site running the ALN Exec. Sites running the ALN Exec include but are not limited to the following:

- sites supporting Air Force sites
- Consolidated accounting and finance Field Organizations
- Development systems supporting Air Force applications

C.1 Account and Project-ID Restriction

All standard ALN userids issued to functional users will be restricted to ALN-compliant accounts and project-IDs in order to maintain an MAC II sensitive level of security on domains running multiple site workloads at sites. When installing this type of userid, the Session Control Screen in the SIMAN record will look like the following:

```
                Session Control for GUJ400              screen name: SESSION

   Maximum Session Time Minutes  [ 999 ]    Maximum Pages Output  [ 999999 ]

PROJECT-ID used at Session Initiation           Alternate Run-ID  [ ______ ]
   [ _ ] PROJECT-ID may be user ENTERED
                       PROJECT-IDS Accessible to user
         [ 1BQ060538500 ]     [ 0J4060538500 ]     [ _____________ ]
         [ _____________ ]     [ _____________ ]
   [ * ] PROJECT-ID usage restricted to the above list

ACCOUNT used at Session Initiation
   [ _ ] ACCOUNT may be user ENTERED
                       ACCOUNTS Accessible to user
         [ 6053BQ1A____ ]     [ 6053J41A____ ]     [ _____________ ]
         [ _____________ ]     [ _____________ ]




Control Image to be processed immediately after the System Generated @RUN Image
             [ @                                    ]
```

NOTE: There is no asterisk in the PROJECT-ID may be user entered field or the ACCOUNT may be user ENTERED field but there is an asterisk in the PROJECT-ID usage restricted to the above list field. These parameters restrict a non-exempt userid to the project-IDs and accounts listed in that userid's SIMAN record. To prevent users from crossing the ALN boundary on a sites, functional users will never be given project-IDs or accounts that would make them ALN exempt. With the exception of the SYS$WSxxxxxx qualifier, these exempt project-ID/qualifiers are as follows:

EXEMPT PROJECT-IDS/QUALIFIERS	***EXEMPT ACCOUNTS***
SYS$, SYS$LIB$, TIP$, DDP, UDS$$SRC, APPL01, TIP$00, MQS$, SYS$CIFS$, SIGHTLINE, and DATAMETRICS ***NOTE:*** *SYS$WSxxxxxx (M Series and ClearPath Systems Only) is treated as an Exempt Qualifier only.*	Any account with 0000 or 0001 in the first four positions.

Project-ID Exceptions

In the majority of cases, application users in an ALN environment will be restricted to a list of project-IDs. In addition, they will not be allowed to enter a project-ID. This prevents a user from starting a batch run with an exempt project-ID (and making the batch run exempt) or entering an exempt project-ID at sign on time. If a user has a valid requirement to enter a project-ID or not be restricted to a list of project-IDs, then all functional OPRs on the system will concur with the request since the user does have the potential to acquire exempt status. The coordination and signature level for this letter will be handled like a request for QLP with Update. Reference *Section 5.5,* Appropriate Coordination Level for additional information.

Account Exceptions

In the majority of cases, application users will not be able to enter an account at sign-on time, and will be restricted to a list of accounts. This reduces the risk that they could gain access to an account that they are not registered under. If a user has a valid requirement for access to more than five accounts, they will need to submit their request to the site IAO for approval. Adequate justification will be provided. Once the IAO has approved the request, the user will be allowed to enter an account. Access to exempt accounts, even in this situation, will normally not be approved by the IAO.

C.2 Installing ALN Userids in SIMAN

If a site platform processes multiple non-exempt ALNs, do not give userids access to exempt project-IDs (reference *Section C.1, Account and Project-ID Restriction*) because any userid that signs on to a system under an exempt project-ID has as much power as a userid that signs on under an ALN-exempt account. Enter the user's standard (non-exempt) account. Also

remember that the site will never give any user outside the site access to an exempt account in an ALN environment unless strong justification is provided. Unless a user needs access to more than five Automated Information Systems (AISs) (which should almost never happen), type blanks in the field PROJECT-ID may be user ENTERED and ACCOUNT may be user ENTERED. Exceptions will be handled in accordance with the procedures in *Section 0, Project-ID Exceptions*, and *Section 0, Account Exceptions*.

changeUserid Parameters

These fields make up a standard userid.

a. Site Code. These are listed in *Section C.3, Site Codes*.

NOTE: This site code list is current as of the date this manual was released and there may have been updates since that time. If the user cannot find a site code or need to get a site code assigned, contact the Security Manager at SSO Montgomery through the FAB (DSN 596-5771). These site codes are as meaningful as possible, given the amount of combinations available with two characters. They specify the site or area where the user is stationed, not the site where the user's processing is being performed. Even after a site's workload is regionalized, the site code will still apply to the users at that site. For Field Organizations, Field Organization personnel accessing a Field Organization system will use the Field Organization site code. Field Organization personnel accessing an Air Force base-level system will use the Field Organization site code and the base-level AIS code. For example, if a Dayton Field Organization BQ user signs on to Robins AFB's Supply, the userid will be DTGVxx. Air Force base-level personnel accessing a Field Organization system will use as their site code the Air Force site where they are physically located. For example, if a Robins AFB user signs into BQ at the Dayton Field Organization, this user will have a userid named ROBQxx.

b. AIS Code. This is the 2-character identifier for each AIS. These codes can be found in *Section C.6, System and Application Software – ALN*, in this document. If the user have a MAJCOM-unique system code that conflicts with a standardized system code, enter userids from both system codes separately under the same system code. In other words, start the standardized one at sub-ID 00 and the MAJCOM-unique one at sub-ID 50. Requests for new or modified standard Air Force AIS codes will be directed to the SSO Montgomery. This office can provide the latest procedures or guidance.

c. Sub-ID. This is the final variable in the userid that specifies individual users on the system. Each userid on the system will correspond to one and only one user.

NOTE: Exceptions are discussed in Section *3.1.5, System Userids*,

C.2.1.1 Format

If there is more than one AIS that could apply to a user, assign that user the AIS code used most often by that user, or the one used most often in their work center, as applicable. Common sense should suggest one or the other. If a user simply will not fit into one category, assign that user a userid for each AIS code. The standard userids will be set up in the following format:

a. Other AIS Userids. There is little chance of having more than 1000 users per site per AIS. Therefore the sub-ID is only two positions. Also included in the userid will be the AIS code. These userids will be constructed in the following format.

POSITION	***VALUE***
1-2	Site mnemonic designator d.
3-4	System code (AIS code).
5-6	Sub-ID. For most sites, this value will be completely numeric. For large sites, or possibly for the Supply AIS, this value will have to be alphanumeric.

Examples: KIBQ25 KI Sawyer AFB, Accounting and Finance
LKGV5T Lackland AFB, Supply (more than 100 users)

b. System Userids. Refer to *Section 3.1.5,* System Userids.

c. Hard-coded Application Userids. There are no known hard-coded application userids.

d. Site Userids. Site userids, as a minimum, will use the designated site code for that particular site in the first two positions of the userid. The site can determine the remaining information used for positions 3 – 6 of the userid. This applies to sites userids only.

C.2.1.2 Staggered Userids

For ease of tracking, the user may stagger the last position of the sub-IDs by two, three, or four. By stagger, we are referring to the practice of skipping characters or leaving gaps between consecutive userids. Although it means less userids per AIS, it makes it easier to track userids by their run-IDs. For example, one Supply user signs on in Demand mode on both pages of her terminal. The userid is TRGV00. The run-IDs for both pages are TRGV00 and TRGV01 (duplicated run-ID). Another Supply user then signs on in Demand mode also. This person's userid is TRGV01, and this run-ID will be TRGV02 (duplicated run-ID) and this person will wonder if a terminal was left signed on somewhere else. Sooner or later, this person will begin to ignore these messages, making the system less secure.

a. If the user were to stagger the last position of the sub-IDs by two characters, however, one userid would be TRGV02 and there would be no run-ID duplication in this case. It would only occur if the other person were to sign on to three terminals at once. If the userids are staggered by three or four, this problem would be virtually eliminated.

b. Keep in mind that TIP-only users do not have run-IDs so this does not present a problem for them. They may have a stagger value of one.

c. When staggering userids, fewer combinations per AIS are needed. The following is a chart of how many userids will be available if the are staggered.

STAGGER VALUE	CAMS-NUMERIC	CAMS-ALPHA	OTHER-NUMERIC	OTHER-ALPHA
1	10000	129600	100	1296
2	5000	64800	50	648
3	3334	43200	33	432
4	2500	32400	25	324

Userid Life-Cycle

To prevent the possibility of running out of userids for each AIS, do not delete them once the user is no longer authorized access to the system. Instead, recycle the userids to new users whenever possible. Once a user is no longer authorized, disable or deactivate the userid.

C.3 Site Codes

The list of site codes currently defined for use in an ALN environment can be located at the following Web site. Reference *Section 0, Userid Parameters, Item a*, if one needs to request or delete a site code.

The current copy of this table is located on the SSO Montgomery Website at https://sso.mont.disa.mil. When reaching the site click on Product Support. On the Product Support page click on UNISYS. From the Unisys page click on Unisys Site Codes/AIS Codes. On the Unisys Site Codes/AIS Codes page select the appropriate table the user wishes to view.

C.4 ALN System Accounts

The following system accounts are used by the ALN operating system:

STNDRD-ACCNT	0000TLABEL	0000USAFSITE

C.5 Standard Accounts

Overview

The ALN standard account consists of an ALN number assigned to a site, location, or workload, and an AIS code. In the early days of the Air Force Phase IV program, this number represented the old Data Processing Center (DPC) number and was used for computer inventory purposes. During the Air Force regionalization effort, the DMRD 924 Program Management Office assigned this number. Today, this number is assigned and controlled by the SSO Montgomery. Requests for new ALN numbers will be submitted to the SSO Montgomery to ensure the STIG and other DOD developed documents are kept current and standardized. The AIS code is the two-position code the software was released under. These AIS codes will generally match the ones found in the userids themselves. Reference *Section 0, Userid Parameters, Item b*, on procedures to request new AIS codes or to modify existing AIS codes.

Format

The standard ALN accounts are in the following format.

Characters 1 – 4: ALN (Access and Location Number). This number originally reflected the old DPC number. SSO Montgomery maintains the Master ALN list and is responsible for assigning new ALN numbers. Do not use the site codes found in the userid.

Characters 5 – 6: AIS code.

Character 7: Gang number. This is optional and is set to "1" as a default. Additional accounts can be installed for the different gangs.

Character 8: Alphabetic Shredout. SIMAN only allows roughly 1000 userids per account. To avoid the limit, swap the shredout at 800. With the shredout about 20000 userids can be installed under similar accounts. Since the regionalization software only looks at the first four characters of the account (expandable to six in the future), this shredout keeps different accounts under the same ALN and AIS code.

6053FS1A	-	Gunter CAMS
6053BQ3A	-	Gunter Finance account, Gang 3
6053FS1E	-	Gunter CAMS account, after 3200 userids

Character 9: — (a dash)

Characters 10 and 11: (2-digit base code)

C.6 System and Application Software – ALN

Most ALN sites use a combination of standard system and application software, and MAJCOM unique application software to support base level functions.

Standard AIS Codes

The current list of standard Automated Information System (AIS) codes used by ALN sites can be found on the following Web site.

> The current copy of this table is located on the SSO Montgomery Website at https://sso.mont.disa.mil. When reaching the site click on Product Support. On the Product Support page click on UNISYS. From the Unisys page click on Unisys Site Codes/AIS Codes. On the Unisys Site Codes/AIS Codes page select the appropriate table you wish to view.

MAJCOM Unique AISs

> The current copy of this table is located on the SSO Montgomery Website at https://sso.mont.disa.mil. When reaching the site click on Product Support. On the Product Support page click on UNISYS. From the Unisys page click on Unisys Site Codes/AIS Codes. On the Unisys Site Codes/AIS Codes page select the appropriate table to view.

C.7 Privileged/Exempt Accounts

In an ALN environment, there is an operating system feature known as ALN replacement. The purpose for ALN replacement is to enable multiple workloads to run on a single Unisys mainframe while maintaining the distinct separation between these workloads. ALN replacement will take place for most users of the system, and works as outlined in the following paragraphs. A much more complete explanation of the ALN replacement concept is available in the ALN Programmer's Manual. A user of the system is subject to ALN replacement or exempt from it depending on the account(s) specified in their SIMAN record. ALN exemption also occurs in the case of certain project-IDs.

More on ALN Replacement

When a functional end user at Gunter (ALN # = 6053) creates a file named JX*00., the system will actually create a file named JX$$6053*00. This process is transparent to the end user so when that user types @ASG,A JX*00., the system will assign the file JX$$6053*00. to his run. Thus files created by functional end users (in ALN terms, these are known as non-exempt users) will have the ALN for their site embedded in the file names. Users that are known as Privileged or Exempt users will not be subject to ALN replacement. When an Exempt user creates a file named JX*00., the file that is actually created is JX*00. In other words, for an Exempt user, the system will work exactly as it does today for users not running under the ALN operating system. As indicated in the next paragraph, the operating system determines whether a user is Exempt or not based on the ALN specified in their account number.

Making a User Exempt

A user is made exempt from ALN replacement when the Security Officer gives that user access to an Exempt or Privileged account. An Exempt account is one that has an Exempt ALN in the

first four characters of the account. ALNs are made exempt through the use of the QMAP processor (see AFM 171-110, Volume II for information about QMAP). The only ALNs that are Exempt by default with the SB5 level of the ALN operating system release are 0000 and 0001. This means that any user that signs on with an account that begins with four zeros (such as 0000JX1A, 0000DA1A, etc.) will be an Exempt user and will not be subject to ALN replacement. The 0001 exempt ALN has been created for Dual Version AIS Capability (DVAC) processing.

NOTE: Remember that a user can also become ALN exempt if the user signs on to the system under certain Project-IDs (such as SYS$) but this is not the standard and approved way of making a user ALN exempt, and will not be discussed here.

Who Should be Exempt

In general, people who work within the site (such as operators, Security Officers, System Monitors, Technical Support personnel, etc.) need to be exempt since their work affects multiple AISs, the entire system, or a single AIS at multiple sites. At a site, granting access to Exempt accounts to individuals outside the site will be very limited and thoroughly justified since an Exempt user can access any file on the system regardless of ALN.

C.8 Project-ID Format

In general, a user's project-ID will follow the standard format of a file qualifier for that user's ALN (site) and AIS. The current qualifier standard naming convention requires the 2-character AIS code in positions 2 and 3, and the ALN number in positions 5 through 8. Applicable Central Design Activity (CDA) programming standards may further define qualifier and filename standard naming conventions.

Exempt Project-IDs/Qualifiers

In an ALN environment, certain file qualifiers are defined as ALN exempt in order to prevent files with one of these qualifiers from being duplicated for different ALNs. Most of these qualifiers belong to system files that may be referred to as single-copy files. These exempt qualifiers are important because if a person signs on to the system with an exempt qualifier as their project-ID, the effect is as if they had signed on with an Exempt Account. The following project-IDs are defined as exempt:

TIP$00	MQS$
SYS$CIFS$	SIGHTLINE
SYS$	SYSLIB
TIP$	DDP
APPL01	DATAMETRICS
UDS$$SRC	

NOTE: The qualifier SYS$WSxxxxxx (M series and ClearPath domains only) is considered an exempt qualifier, but a user cannot gain exempt status if this qualifier is used as a project-ID. No userid on the system (except for operator userids) will have access to

any of these Exempt project-IDs. The operator userids will have access to SYS$ as the default project-ID. The only proper way to make a userid ALN exempt is to give it access to an Exempt account.

C.9 ACR Ownership

It will be noted that there are certain system ACRs that exist on all ALN systems (such as the ACR GUJXFG) that are owned by userids other than the security officer. This particular ACR is owned by the standard userid GUJXFG so that the ACR attachment can be automated in the LIBRARY/FILES runstream, which is started out of the LIBLOAD run.

APPENDIX D. DNMC SITE SPECIFIC INFORMATION

This appendix contains service-specific security information for DNMC sites. When the main STIG document refers you to your "service-specific appendix," this is the location to reference if you are the security officer at a DNMC site.

D.1 DNMC Naming Standards

Currently, userids are assigned by Customer Identification Codes (CICs). The first three positions of the userid identify the site. The remainder of the userid may range from four to six alphanumeric characters and reflect the standard that was in-use when the sites migrated to the site. DECC Ogden internal userids will start with 'OG' in the first two positions of their userids. Current site codes are listed in *on the following Web site*.

> The current copy of this table is located on the SSO Montgomery Website at https://sso.mont.disa.mil, when you reach the site click on Product Support. On the Product Support page click on UNISYS. From the Unisys page click on Unisys Site Codes/AIS Codes. On the Unisys Site Codes/AIS Codes page, select the appropriate table you wish to view.

D.2 System and Application Software – DNMC

The following is the current list of standard application Automated Information System (AIS) codes used by DNMC sites. DNMC sites are also authorized to use any of the standard AIS codes listed on the following Web site.

> The current copy of this table is located on the SSO Montgomery Website at https://sso.mont.disa.mil, when you reach the site click on Product Support. On the Product Support page click on UNISYS. From the Unisys page click on Unisys Site Codes/AIS Codes. On the Unisys Site Codes/AIS Codes page select the appropriate table you wish to view.

D.3 Alternate Run-IDs

Many DNMC users are assigned userids consisting of eight characters. The first three characters designate the site and the last five characters make the userid unique. These userids use the alternate run-ID feature within SIMAN to make these userids unique. The use of alternate run-IDs is authorized for all DNMC systems but they will follow the format stipulated above. The alternate run-ID used on the DNMC systems will match the last five or six characters of the userid. There will be no duplicate alternate run-IDs.

This page is intentionally left blank.

APPENDIX E. DFAS-IN SITE SPECIFIC INFORMATION

This appendix contains service-specific security information for DFAS-IN (Indianapolis site). When the main STIG document refers you to your "service-specific appendix," this is the location to reference if you are the Security Officer at a DFAS/IN (Indianapolis) site.

E.1 DFAS-IN Naming Standards

All DECC Ogden internal userids are set to a standard naming convention. They are six positions and begin with an OG code in the first two positions.

DFAS Indianapolis

App Group	Application	UDS Qualifier	App Name
1	PBAS	UDS$$ONE	DMRP1
2	DTRS	UDS$$TWO	DMRP2
3	Validation	UDS$$THR	DMRV
4	System Test	UDS$$FOR	DMRS
5	Programmer Test	UDS$$FIV	DMRT

Table 11-5. Application Groups used by DFAS-IN

E.1.1.1 PBAS

PBAS userids are TIP/Demand users and are set up with a five-position userid. The first three positions of the userid represent the site prefix and the last two positions consist of the user's initials.

E.1.1.2 Non-PBAS

These userids are set-up with a five-position userid. The first two or three positions of the userid represent the department prefix and the last two or three positions consist of the user's initials.

E.1.1.3 FTP

FTP userids are six or seven positions with the first position starting with a D or E.

E.2 System and Application Software – DFAS-IN

Although there are no current documented application AIS codes for DFAS-IN (Indianapolis), this site is authorized to use any of the Standard AIS codes listed in *Table 18, ALN AIS Codes*.

E.3 Other DFAS-IN

There are no other documented standards at this time.

This page is intentionally left blank.

APPENDIX F. INADVERTENT CLASSIFIED PROCESSING PROCEDURES - ALN

The following procedures are a guideline to follow in the event that suspected classified material has been introduced into the Unisys mainframes supported by SSO Montgomery.

Notification

When the site is informed that possible classified material has been introduced into the Unisys mainframe, the following notifications will take place.

a. Local site Director

b. Site Unisys IAO

c. Site Unisys Technical Support (DBAs)

d. Site IAM

e. Site Application Personnel

f. The Unisys CE

Disconnect

F.1.1 All Sites

Access to the affected system will be turned off and then controlled until the suspected classified data can be tracked and cleared. The following steps will be used to disconnect users and control access.

a. Down the user processes through CMS: **DOWN,ALL PROCESS**

b. Put a hold on demand terminals from the system console.

c. Up the demand process only through CMS: **UP PROCESS,RSDCSU**

d. Swap out the system audit trails and secure the tapes.

e. Temporarily remove the hold on demand terminals to allow required personnel access to the system. Once they are signed-on, put the hold back on. Should any other users sign-on, terminate them with the **SM xxxxxx T** command.

F.1.2 Sites Using Data Replication

a. Stop data replication activities between the site and sister site.

b. Notify the sister site so data replication is not activated.

Assessment

The IAO, technical support DBAs, affected application personnel, and the person who reported the suspected action will research and determine the following:

a. The time of the incident.

b. Location of the information.

c. Possible interface contamination.

d. Possible access or duplication of information.

e. Who is responsible.

Research

With the required personnel signed on to the controlled system, research may begin to locate the file with the classified data.

NOTE: These procedures assume the **QUALIFIER*FILENAME** can be determined by researching ADRSS or other system history information. If the filename is not known and cannot be determined, the only option may be a complete JK 4-13 system boot; however, access will be controlled into the system until the boot can be accomplished by using the procedures in Section F.2, Disconnect. Each of the procedures below will indicate the Cylinder, Head, and Device Relative Address (DRA). The **@LOCATE** DRA is in decimal and the **@DSKUTL** DRA is in octal.

a. A **@LOCATE** will be done on the file to determine the location of the file on disk.

b. Or you may MAP the drive or file to determine where it is written on the drives.

1. If the file exists on one drive:

@DSKUTL,BIL device name,,SORT/FILE

2. If the file exists on multiple drives:

(a) MAP by Qualifier:

@DSKUTL,BI qualifier,,SORT/FILE

(b) MAP by Filename:

@DSKUTL,BIF filename,SORT/FILE

c. A Log Analyzer run will be accomplished on the file to determine how many, if any, users have accessed the file, if it was copied, SYM'd to a printer, etc.

NOTE: *If the file was copied, the above steps will be repeated for the copied filename.*

Resolution

Once the location of the file has been determined, and documentation of the location is created and saved, the severity of the problem will be analyzed and a decision made as to whether the disk drive(s) need to be prepped or if the steps below can be taken to overwrite the file's disk locations and zero the granules.

a. If the packs are to be prepped, the Unisys Customer Engineer will accomplish an off-line prep.

b. If the file's disk locations are to be overwritten, follow the steps below:

1. Erase the contents of the file, but do not release the granules. Do this with the command **@ERS,N QUAL*FILE**. Next, copy an unclassified file into the classified file to overwrite any potentially classified information.

NOTE 1: *The file,* ***SYSLIB*UCS$BLDCOMPS.****exists on all Unisys platforms and is usually 3100+ tracks. This is a good candidate for copying into the classified file.*

NOTE 2: *Do an* ***@PRT,F*** *on the classified file to ensure it's maximum track size is large enough to copy a 3100 track file into it. If maximum track size is too small, an* ***@ASG,A*** *will be done to increase the size so the copy will not error.*

2. After the files are copied, follow the MAP procedures in *Section F.4, Research, Item* ***b***, above to ensure that the cylinder and head locations of the classified file have been overwritten (compare the disk maps showing the classified file to ensure every cylinder and head location was written over). After this has been accomplished, delete the file. You can do this with the command **@DELETE QUAL*FILE**.

c. To zero all granules assigned, type the command **@ERS,Z QUAL*FILE**. After this has been accomplished, delete the file using **@DELETE QUAL*FILE**.

Recovery Action (Sites Not Using Data Replication)

After the disk has been cleansed, the system can be brought back online and required individual database recoveries can be accomplished with users online.

Recovery Action (Sites Using Data Replication)

After the disk has been cleansed, restart data replication.

Inadvertent Classified Processing Checklist

Inadvertent Classified Processing

1 Introduction. This attachment provides procedures to follow when classified information is inadvertently entered into a Unisys system during unclassified processing sessions. This attachment is designed to be locally reproduced and placed in the System Console Operator's handbook for ready reference and use. Refer to Appendix F of Unisys Security Technical Implementation Guide for specific procedures.

MASTER CHECKLIST

	Notification	Time	Initials
	Site Commander/Director		
	Site Unisys IAO		
	Site On-call DBA		
	Site IAM		
	Site Application Support personnel (Applicable applications)		
	Unisys Customer Engineer		
	Isolation Process		
	Down all Communication processes thru CMS via a "DOWN,ALL PROCESS"		
	Close the audit trail(s)		
	Up the demand process to allow the Security Officer to sign on via a "UP PROCESS,RSDCSU" through CMS		
	Put a hold on terminals after the Security Officer has signed on and remove any other users who may have signed on.		
	Determine the following:		
	Time of Incident		
	Location of information (disk/tape, etc)		
	Possible interface contamination		
	Possible access or duplication of information (including audit trails, SAVE/SAVALLs, etc.)		
	Research Process:		
	Determine name of files and packs/tapes they reside on.		
	Run Log Analyzer to determine who/how many users access the data.		
	Resolution:		
	Determine if disk/tape will be erased, degaussed, or overwritten.		
	Recovery Action:		
	Bring system back online.		

As each action is taken, record its completion and indicate the time and person completing the action on this master checklist. Attach this checklist to the incident report sent to the Site Security Manager and MAJCOM Security Officer (for sites and stand-alone USAF sites), and provide an information copy to SSO Montgomery, P.O. Box 1300, Gunter Annex AL 36114.

2 Immediately Stop all Processing and Cancel All Terminal Support. When inadvertent classified processing is detected:

a. Stop the System. Use the "$!" keyin to stop all processing. Deny all terminal access. There shall be no exceptions. Power off all components. Leave power off for at least one minute. Under no circumstances will you allow normal processing to continue. Even if you are in the middle of a CAMS database conversion or an Accounting and Finance End-of-Year program. If you continue, these outputs will become classified and will have to be re-accomplished anyway.

b. Contact the Sites Security Officer. The site IAO or alternate must be present to assist and/or direct the decontamination efforts. Call the IAO no matter where he or she might be or what time it is. Continue these steps up to and including determining the scope of the problem. Do not proceed past that point until the IAO arrives.

c. Read the rest of this attachment in its entirety. Do not rush. Have someone else continue with these steps as you read ahead.

d. When it comes to posting guards, remember, most users will have to wait idle while you declassify the system. That is where you would start looking for guards. Call someone in your chain of command with sufficient authority to post guards. This is an emergency.

e. Secure the System. Collect, label, and secure all products created during the time the classified information was in the system. This includes all tapes created (including audit trail and FAS tapes), listings, disk packs, and all other input or output media. Backup copies of each tape shall also be secured.

f. Contact the office or person that was the source of the classified data or who owns the data that was introduced onto the system, and have them determine whether or not it is possible to declassify or downgrade the data to a sensitive unclassified level. If this is possible, it will save potentially many hours of work and down-time for the system. You must make sure, however, that the correct office, person, or organization is contacted to make that decision. Your IAO and site management will be very useful in making this contact.

3 Determine the Highest Classification of the Data. Once you know the highest classification of any of the data on the system, all of it will have that classification until it is cleaned. From this point on, all personnel working this issue must meet the minimum security clearance requirements for the highest level of classification. Remove all unnecessary and uncleared personnel.

4 Physically Secure the Computer Area. Do not allow "visitors" or "demonstrations" of any kind. If the area cannot be secured by door locks and a badge system, post guards of proper security clearance.

5 Determine the Scope of the Problem. This next step is critical. Follow the procedures as precisely as possible. Proceed slowly and carefully. Have another person take notes at each point.

a. Review the Console Log. Try to determine, if possible, the time when classified information was inadvertently entered into the system. Logged job start or stop times, processing command sequences, and operator annotations are examples that might indicate when classified information entered the system. Some other factors to consider are:

(1) Storage. Most likely, classified information was temporarily stored in operating system buffers in main memory, as well as on disk(s) or tape(s). Determine which disk(s) or tape(s) have been in use from the console log. Record their identifying name(s), if any.

(2) Copies. There is a high probability that classified information has also been inadvertently or intentionally copied and distributed to several devices on the system. This potential increases with the time lapse between the actual entry of the classified information into the system and its discovery. From the console log, determine what disk drives or tape drives may have been used, but are not now being used by the system. Record their identifying names, if found.

(3) Record Classification Start and Stop Time. If discovered by reviewing the console log, record the date and time classified information inadvertently entered the system. Otherwise, record the fact the console log does not indicate the time of classified data entry. The stop time will be the time that all processing was halted and terminal access was stopped.

b. Estimate the Extent of Classified Contamination. When possible, make a preliminary estimate of the extent classified information is present in the system. Record this estimate. Depending on the degree of contamination and security risk, recovery procedures can be as severe as complete clearing of all disks and main memory, to as little as declassification for only those disk(s) and file(s) where classified information may have been stored. This preliminary estimate (e.g., at most one hour, at least 10 minutes, cannot be determined) will be useful at later points in these procedures.

STOP! Do not continue until the IAO is present.

6 Enter the Secure Session.

a. Power on all components. Powering off/on components clears memory once the system is booted.

b. Perform a long tape boot and LIBLOAD. This will decontaminate any affected system files. Use the tape drives configured when classified data was introduced to the system.

c. Initialize security. Notify a security team member for procedures on this step and whether it is necessary.

d. Print all queued print listings in all print queues. This print must be reviewed for classified content. If any is found, the classified listing and the printer ribbon become classified products and must be handled and eventually disposed of properly. If you cannot review the listings due to time constraints, have the operator enter "SX A/F" to delete all queued print (management decision).

e. Start CMS from the console. Perform a “DOWN,ALL PROCESS” through CMS. Put a hold on all demand terminals with a “CS HT”. Up the demand process through CMS with a “UP PROCESS, RSDCSU”. Have the operator release the terminal hold with a “CS AT” and sign on to a Demand terminal in the area. If there is none, locate an office with a terminal and sign on. Physically rotate the terminal screen away from doors, windows, and mirrors. Secure the office with guards of proper security clearance. Do not use the telephone to discuss the contents of any classified data found. Do not leave this office unattended. If you must leave, sign off all terminals completely.

f. If the security environment had to be initialized, the proper sign-on procedures are:

U: $$OPEN D$xx
S: Enter your user-ID/password and clearance level:
U: <master user-ID>/SECURI/<new password for master user-id>
U: @RUN SECOFF,<master account>,SYS$

(where U: means user S: means system responses)

NOTE: The syntax for the users response to the Enter your user-ID/Password and clearance level prompt changes the default password for the master user-id to the new password, securing the master user-id by removing the default password as soon as possible.

g. Unacceptable jobs. The following jobs open the system to the network and must <u>not</u> be started by the operator during the secure session:

PPC, DDPLTR, DDPFJT, TAS, WEBTS, WEBPR, CPFTP, ICI, NAxDDN or any other TELCON-type jobs.

h. Once you have signed on, have the operator enter a "CS HT" keyin. This will prevent other users from signing on. If any other user signs on before this keyin can be entered, the operator will down their terminal with an "SM <terminal-ID> T" command.

i. If you have signed off and need to sign back on, the operator must enter "CS AT" to allow terminal access. Once you are signed on, the operator enters "CS HT" to hold terminal access again.

j. Log Analyzer. Use the Log Analyzer Processor (LA) to retrieve information from the system log file to further identify the point at which classified contamination occurred. Capture any information related to the processing activity that happened after classified information entered the system such as users who were on the system, processing being accomplished, and products produced. System log Type 403 records contain catalogued mass storage file usage information, which will be invaluable for determining which disk(s) and file(s) may contain classified information. Other File and Device Log Entries include 405 (Tape Files), 407 (Removable Mass Storage), and 408 (File Name Change).

k. If the suspected files can be identified, use the following procedures to identify the location of the file(s) on the system. These procedures will identify the cylinder, head, and Device Relative Address (DRA) of the file. The @LOCATE DRA is in decimal and the @DSKUTL DRA is in octal.

a. An "@LOCATE" will be done on the file to determine the location of the file on disk.

b. Or you may MAP the drive or file to determine where it is written on the drives.

(1) If the file exists on one drive:
@DSKUTL,BIL device name,,SORT/FILE

(2) If the file exists on multiple drives:

(a) MAP by Qualifier:
@DSKUTL,BI qualifier,,SORT/FILE

(b) MAP by Filename:
@DSKUTL,BIF filename,SORT/FILE

l. Using Log Analyzer, check for the suspected file(s). See if anyone else accessed these files. If so, did they copy the information to other files or tapes? Did anyone access these files or tapes? Were these files SYM'd to a printer? These are the types of things to look for using Log Analyzer. The SYSLIB*USAF.LA-SKEL runstream is very useful in generating LA runstreams. "@ADD" this runstream. It is menu-driven and mostly self explanatory.

7 Review, Mark, and Secure All Products. Until you can positively show that any products produced during the inadvertent classified session or hardware devices are unclassified, they must be declassified or protected as classified. Of special importance are those products used for recovery processing. Follow these rules and procedures carefully:

a. Tape Content Review. Dump all tapes created during the inadvertent classified processing session to the printer and manually review their contents for possible classified data. This review must be done before these tapes can be used during the recovery process or for any further unclassified processing.

(1) TIP Audit Trail Tapes. Audit trail tapes can be dumped for manual inspection using the Audit Trail Analyzer (ATTANL) processor (consult SSO Montgomery for details).

(2) FAS Tapes. If a SAVE or SAVALL command sequence was performed after the inadvertent entry of classified data, then those FAS tape(s) must all be retained and protected until a SAVALL is performed after declassification has been completed.

b. CAUTION. When each file is restored following declassification, the file(s) identified as having classified information on them shall be excluded from the restoral process (consult the FAS Manual, Unisys publication 7830 7972). Otherwise, the restoral process will reintroduce classified data to the system.

8 Select Recovery Method. After all incident investigation work is complete (done in the secure processing environment), the next step is to determine the recovery method to be used. Selection of a proper method must be done in consultation with the IAO or alternate. Always document the rationale used for selection. Be sure to consider the preliminary classified estimate made in paragraph 5.b above.

Some possible steps to be taken next are irreversible!

8.1 Extensive or Unknown Classified Data. If the best judgment of the situation indicates that classified data is extensive or its extent can not be determined (again, consider the notes being taken at each step), then the entire system shall be declassified - all main memory, all disk controllers, all tape controllers, and disk packs that may contain classified information). This will involve a JK 4,13 boot. This is a serious situation since declassification is irreversible.

a. Disk Drives. Declassify every disk drive using DPREP.

b. DPREP Type 4. Perform a Type 4 DPREP specifying that "A" (all) data areas on the disk pack(s) are to be initialized.

c. Tape Files. Mark and secure every inadvertently classified tape for declassification by degaussing. Degaussing will erase all data on the tape, including classified information.

d. Console Logs. Mark and secure all inadvertently classified console logs for retention as prescribed by local procedures.

e. Output Products. Review all output products produced during the period when classified information was in the system. Verify that no classified data is included in these products.

f. System Recovery. After declassification, the system should be rebooted and recovery procedures performed to the LAST recovery point immediately prior to classified contamination. Care must be exercised to avoid loading classified data back into the system. The only tapes you may use for AIS recovery are audit trail and data dump tapes that have been manually reviewed and found not to contain classified data. Do not load any SAVALL or SAVE tapes created during the time period that the system was contaminated with classified data. Ensure any user tapes created during the period of classified contamination do not contain any classified data.

(1) Recovery Point. Start processing from the LAST recovery point immediately prior to classified contamination.

(2) AIS Recovery Procedures. If uncertainty exists for the LAST recovery point immediately prior to classified contamination, then AIS specific recovery procedures should be followed.

g. Pack Disposal. Have the site security officer label packs in accordance with DOD guidelines. If these disk packs are discarded, follow DOD guidelines on disposal procedures.

8.2 Limited Classified Contamination. If there is a reasonably accurate assessment that only certain files are classified, then a much less severe declassification procedure can be done.

a. Tape Files. Mark and secure every inadvertently classified tape for declassification via degaussing. Degaussing will erase all data on the tape, including classified information.

b. Disk Files. The steps below can be used to overwrite Determine the location (Cylinder, Head, and Device Relative Address (DRA)) of the file using the procedures below.

Use the @LOCATE <filename.> command to determine which disk drives the contaminated file was on. Perform an @ERS,IZ on each contaminated file. This procedure will "zero-fill" and release all disk granules assigned to that file. Other files that are on the disk and not classified can then be recovered by normal recovery procedures. Remember that the @ERS,IZ command can only erase those sectors already assigned to the file. It is possible that the classified data was in a program file, the element was deleted, and then the file was packed. If this is the case, the @ERS,IZ will only zero-fill the assigned tracks. Check for this. For data files, check for multiple file cycles.

c. Console Logs. Secure and mark all inadvertently classified console logs for retention as prescribed by local procedures.

d. Output Products. Review all output products produced during the period when classified information was in the system. Verify that no classified data is included in these products.

The @LOCATE DRA is in decimal and the @DSKUTL DRA is in octal.

a. An “@LOCATE” will be done on the file to determine the location of the file on disk.

b. Or you may MAP the drive or file to determine where it is written on the drives.

(1) If the file exists on one drive:
@DSKUTL,BIL device name,,SORT/FILE

(2) If the file exists on multiple drives:

(a) MAP by Qualifier:
@DSKUTL,BI qualifier,,SORT/FILE

(b) MAP by Filename:
@DSKUTL,BIF filename,SORT/FILE

The @LOCATE DRA is in decimal and the @DSKUTL DRA is in octal.

a. An "@LOCATE" will be done on the file to determine the location of the file on disk.

b. Or you may MAP the drive or file to determine where it is written on the drives.

(1) If the file exists on one drive:
@DSKUTL,BIL device name,,SORT/FILE

(2) If the file exists on multiple drives:

(a) MAP by Qualifier:
@DSKUTL,BI qualifier,,SORT/FILE

(b) MAP by Filename:
@DSKUTL,BIF filename,SORT/FILE

11 Reports. Collect notes, checklists, and console logs related to the incident. Prepare, apply security markings, and dispatch an incident report as prescribed by local procedures and DOD policy. Forward the report to the site Security Manager and either the MAJCOM Security Officer (For Air Force sites) or the DISA Computer Security Office. Also provide an information copy to SSO Montgomery, P.O. Box 1300, Gunter Annex AL 36114.

12 Summary. This attachment provides a set of guidelines and procedures which should be applicable to most inadvertent classified processing incidents. Solicit assistance from other people on duty. Keep and refer to notes taken at each decision point. Pause frequently to consider and plan out the next action or step to be done. Discretion, common sense, composure, tact, and on-the-spot judgment are key elements necessary to recover from an inadvertent classified processing incident. If there are any steps or procedures that you have done in addition to these, write them down in the order they were performed in relation to the steps listed here, and send these steps to the Systems Support Office in Montgomery for review and possible publishing.

APPENDIX G. SIMAN

SIMAN (Site Management Complex) is the security processor for the Unisys operating system environment. SIMAN is mainly for use by the Security Officer but may be used in a limited capacity by AIS users. SIMAN operates in two distinct modes that perform much of the same functions but in totally different ways. SIMAN is documented extensively in 7831 0661(SIMAN Administration and End Use Guide). SIMAN provides an overall set of computer enforced internal control protection features, catalogued file security information (including QUOTA information for mass storage resource management, account maintenance features, and a means of updating the Message Of The Day). SIMAN also establishes and defines userids for Demand, Batch, and TIP users. A user's password, run clearance level, default account and project-ID, terminal time-out, CONS mode level and keyins, and secured Interfaces and Privileges are all handled by SIMAN. Further, SIMAN has its own internal security based on an administrative hierarchy.

G.1 Screen Mode

In screen mode, the user is led through a series of menu-driven screens to perform various tasks. By entering @SIMAN, the user is taken to the main menu. By entering responses as indicated on the screen, the user will be led to the desired screen(s). This is especially effective for precise entries or for use by inexperienced users/security officers. Since the screens do extensive checks for valid entries, there is less chance of entering data in error.

a. Commands. On any given screen in SIMAN, all commands are entered in the upper left-hand corner, or home position. When transmitting, the cursor may be in any position on the screen, as it will automatically position itself in the lower right-hand corner for you.

b. Command Strings. More experienced users will find that commands may be strung together by commas. For instance, a user may wish to enter an @SIMAN and then enter a 4 on the main menu screen and then enter a 1 on the cataloged file security submenu in order to display the security information on a file. The experienced user may enter an @SIMAN 4,1 and bypass the menus for faster response time. This also works from the screens. Commands such as COMMIT,X or COMMIT,M,1,3 can save an appreciable amount of time, especially when the system is slow.

c. Exiting. An OMIT can be entered from any non-menu screen in order to avoid finalizing something entered by mistake. For instance, if you accidentally overtype someone's password, type OMIT in the corner and transmit. All changes made since the last COMMIT will be ignored. Entering X from any screen in SIMAN will first have the effect of an OMIT and then take you completely out of SIMAN.

G.2 Batch Mode

SIMAN batch mode is not the same as the Batch run mode for the system as a whole. SIMAN batch mode is an interactive Interface with SIMAN without the use of screens. SIMAN batch is

documented in *Appendix A* of the *SIMAN manual (7831 0661)*. This interface is ideal for runstreams released from SSO Montgomery since it provides almost all of the functions available in screen mode and can be called from a batch job. It is suggested that only experienced SIMAN users use batch mode because there are almost no edits in batch mode and no OMIT option to prevent accidental updates. Also, the syntax can be complicated at times, unlike the screens, which requires little knowledge of SIMAN syntax.

G.2.1 Using Batch Mode

SIMAN batch is invoked by typing @SIMAN,B from a demand session, and is ended by typing @EOF. You can use the batch syntax from *Appendix A* of the *SIMAN manual* to install, modify, delete, or display information about userids, accounts, etc. Any function that can be carried out using the full screen interface can be accomplished in batch mode. When in SIMAN batch mode, a semicolon (;) is used to delimit complete syntax strings. You can either add a semicolon (;) at the end of the line of syntax, or enter a semicolon on its own line after the last syntax. Multiple commands may be strung together by leaving off the semicolon at the end of each line and adding it to the end of the last line or after the last line. The semicolon has the same function as the COMMIT in screen mode. It tells SIMAN that you want to actually execute or carry out the syntax you have been building.

G.2.2 SIMAN Syntax Dumps

One of the most useful features of SIMAN batch is the capability to generate listings of userids, accounts, ACRs, etc. into a data file in SIMAN batch syntax. That way, the information can be pulled into an editor (such as CTS or IPF) and modified, then the file can be run back through the SIMAN batch processor to actually modify the userids, accounts, or whatever as desired. For example, let's say that you wish to generate a listing of all the userids on your system in SIMAN syntax format in a file called SYS$*USERS. Note that there are a number of SIMAN batch commands that can be used to generate only a portion of the userid information from your system rather than all the data as in this example. A detailed explanation of all SIMAN syntax commands is beyond the scope of this manual. Following are the commands to use in this example, starting from a demand prompt:

```
>@SIMAN,B     <xmit>
>DIS  USE = !ALL  SYN  BRE = SYS$*USERS.  ;     <xmit>
>@EOF     <xmit>
```

Next let's say you want to look at the SIMAN syntax dump you just created using IPF. If your site has a large number of userids, the SIMAN syntax dump will be quite large, and the default size of your IPF workspace may not be large enough to read it. If this is the case, perform the following steps (this example assumes your userid is GUJX00) to enlarge the size of your IPF workspace file:

```
>@IPF    <xmit>
>EXEC  "@PRT,I"    <xmit>
```

This command will generate output that looks something like this:

```
>FURPUR  30R5-A      (940406 0944:19) 1995 Mar 09 Thu 2126:45
>SYS$*TPF$(0),MDISK,T
>SYS$*GUJX00(1),MDISK,ZA  IP$IPF$$DDS$,IP$USEAAAAAA,
>SYS$*IPF$GUJX00(1),MDISK,ZXA  IP$USEAAAAAB,
>SYS$*IP$ADDFILE(0),MDISK,T  @@@@AESYM$$$,
```

Your workspace file is SYS$*IPF$GUJX00, and this file can be resized as follows:

```
>LOGOFF
>@FREE SYS$*IPF$GUJX00.                    <xmit>
>@ASG SYS$*IPF$GUJX00.,///9999 <xmit>
```

Now the syntax dump created above can be pulled into IPF with the following commands:

```
>@IPF                          <xmit>
>OLD  SYS$*USERS.          <xmit>
```

The userid listings in the syntax dump will be in a format similar to that in *Table 23* below.

```
-"*************************************************************************
*
-"    USERID J1JZ08          SIMAN 4R3B-03      95-03-13    1913:02
-"*************************************************************************
*
-INSTALL USERID = J1JZ08     " OWNER = J1JX00
-USERID_MAINTENANCE = USER
-FORCE_PASSWORDCHANGE
-MINIMUM_CLEARANCE = 0            MAXIMUM_CLEARANCE = 11
-RECORD_ACCESS = PRIVATE
-FILE = UNOWNED
-QUANTUM_TIMER = DISALLOW
-DEFER_INTERRUPT = DISALLOW
-PROCESSOR_PRIVILEGE = READ_GRS
-ACCESS_PRIVILEGE = ORDINARY
-SHARING_LEVEL
-RUN_MODE = DEMAND , BATCH , TIP
-TIME
-LOGON = 30
-MAXIMUM = 30
-RUN_GENERATION = OVERRIDE_SYSTEM
-MAXIMUM_TIME = 999
-MAXIMUM_PAGES = 999999
-RUN_PROJECTID= PROJECT_ENFORCED, 0JZ011110000
-RUN_ACCOUNT = 1111JZ1A
-CONTROL_IMAGE = '@WHOAMI'
-CONSOLE_MODE = BASIC
-LIST KEYINS =
-  GENSTA,  RUNSTA,  LOGGIN,  DATKEY
-LIST ERS =
-  PB$CON
-LIST PRIVILEGES =
-  SSMMGRILES1,   SMOQUE,   COM$PRV  ;
```

Table 11-6. SIMAN Syntax Sample