Unisys Checklist
for
Unisys Security Technical Implementation Guide

Version 7 Release 2

24 November 2006

Developed by DISA for the DOD

Database Reference Number: ______________________________

Database entered by: _________________ Date: _____________

Technical Q/A by: ____________________Date: _____________

Final Q/A by: _______________________ Date: _____________

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

UNCLASSIFIED UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

Summary of Changes

14 April 2006 – Added VMS 6.0 review procedures.
14 April 2006 – Added VMS 6.0 Vulnerability Key to each checklist item.

24 November 2006 – Added new vulnerabilities to match Unisys STIG V7R2, 28 August 2006

VMS 6.0 Unisys Review Procedures

The following is an outline of the process for performing a Unisys review and entering the results using VMS 6.0.

1. Ensure that asset is registered in VMS under the correct organization. The asset must have at least an Operating system that is a child of Unisys 2200 in its posture. Unisys 2200 6.1 will be used for all software release level 6 regardless of the sub level. Unisys 2200 8.1 will be used for all released level HMP IX 7.0 and above including the new nomenclature CP OS(or just CP) 2200 n.n. The asset may have additional elements (such as database, application server, …) in its posture depending on the functionality of the asset.
2. If the asset is registered skip to Step 4 otherwise you must register the asset. You will find the appropriate selection criteria by selecting Asset Finding Maint → Assets/Findings → By Location → your location → Computing and then click on the file icon to create the asset.
3. On the General tab fill out the Host Name and appropriate values for the other fields on this tab.
4. Determine the enclave that the asset is within.
5. If the asset is in the correct enclave, skip to step 9.
6. Enter the enclave on the Systems/Enclaves tab of the asset creation / or update screen.
7. For registered enclaves, choose the enclave.
8. If the enclave is not present, contact your team lead or your IAM and report that the enclave is not present.

   NOTE: Every effort should be made when registering or updating an asset to include the asset within an enclave.
9. Since at this time there is no scripted review process that automatically generated an import file, only the fields required by VMS are need unless there are other elements in asset posture that require specific fields for their scripts. Any additional fields may be filed in for documentation purposes. The more documentation the better for identifying the system correctly.
10. Print the Checklist and perform a manual review. If you have access to the SRR Management Toolkit developed by SSO Montgomery you may use it to reduce the data needed to perform the review. Care should be taken in using this tool if you do not use the ALN modifications of the operating system and/or do not

follow the userid profiling system described in the Unisys STIG. Since the toolkit was designed to work in this environment it may give both false positives and false negatives with a standard Unisys system release or on a system that does not use the same userid profiling system.

11. Manually key results into VMS.
    Reviewers: By navigating to the pertinent visit, selecting the asset, and expanding the appropriate element for this review. If the asset is not present in the visit, contact your Team Lead and have them enter the asset into the visit.
    Systems Administrators: by navigating to the your location, selecting the asset and expanding the appropriate element for review.
    The appropriate element will be Unisys 2200 6.1 or Unisys 2200 8.1 depending upon the assets posture.
12. Process any additional reviews required by additional elements within the asset posture.
13. The Checks for IAVA compliance should all be marked N/A.

A101.030.00 V0000739 CAT II IAO not cognizant of processes on system

8500.2 IA Control: PRTN-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2, 630-230-19 Security Requirements for Automated Information Systems Chapter 2 Paragraph 7.a

Vulnerability The IAO is not cognizant of the applications, developers, and customer supported sites running on the system.

Vulnerability Discussion If the IAO is not familiar with the system workload, it is impossible to identify suspicious activity.
The IAO will be cognizant of the applications, developers, and customer supported sites running on the system.

Checks

IAO workload knowledge

The reviewer will Interview the IAO to ascertain whether the IAO possess adequate knowledge of the processing environment to perform the their duties
Examples of questions the IAO should be able to answer are:
Does the IAO know what applications are running on the system?
Is developement being done on the system and if so by who?
What users should be logged into the system?

Fixes

IAO training SLA/workload

The IAO should review all SLA/MOAs and become familiar with the system workload.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A101.040.00 V0000736 CAT IV No accnt name format

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2

Vulnerability For a DISA ALN sites, there is no document standard account naming format.

Vulnerability Discussion An account naming standard provides a means for the IAO to positively identify improperly assigned or unauthorized user-IDs under an account. Unauthorized access to an account can allow a user to cross ALN boundaries, gain access to privileged system processors or ACRs, and create erroneous fee for service billing information.
For DISA sites, the IAO will ensure there is a documented standard account format for the system.

Checks

Accnt Naming ALN

The reviewer will interview the IAO to verify that there exist an account naming standard for the site and that it is being followed.

Fixes

Accnt name stand developed

An account naming standard will be developed.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A101.060.00 V0000562 CAT III @@PASWD command used

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.3.6.1

Vulnerability Users use the @@PASSWD command to change their password.

Vulnerability Discussion The @@PASSWD command is logged into the system log and does not mask the old/new password entered by the user and increases the likelihood of password compromise.
The IAO does not ensure that the users do not use the @@PASSWD command to change their password.

Checks

@@PASSWD Instructions

The reviewer should interview the IAO to ensure that the IAO is aware of the problem with the use of the @@PASSWD command by users and that the users are instructed not to use the command.

Fixes

@@PASSWD Instructions

Instruct users not to use the @@PASSWD command and inform them of the reason why.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A101.090.00 V0000705 CAT II Console logs not properly sanitized

8500.2 IA Control: PECS-1, PECS-2, PEDD-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.4

Vulnerability There are no procedures to ensure console logs or SPO logs containing system passwords are secured and destroyed.

Vulnerability Discussion There is a utility program that allows a user to sign on at the systems console. All messages to and from the system console are printed (optional on newer systems), logged in the console devices hardware, and logged in the SPO controller. Because of this, authentication information can be obtained from console listings, console hardware logs, or SPO logs thus creating a means for unauthorized system access.
The IAO will develop procedures to secure and destroy console logs containing system passwords.

Checks

Console log Procedure

The reviewer will interview the IAO to ensure that there is a procedure for securing the console log and SPO log when authentication information is present or changing any password exposed on the system console.

Fixes

Console log procedure

Develop a procedure to secure the console logs and/or SPO logs produced when user authentication information is present (system initialization, starting CONSOL, etc.) or to change the password for the userid that was used to start CONSOL as soon as the system has completed the boot process. Include this procedure in the operating instructions and/or operator training material.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A101.110.00 V0000547 CAT II The NMS password management

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.2.1

Vulnerability Knowledge of the NMS password is not limited to authorized individuals, or the password is not changed on a periodic basis or, as a minimum, every 365 days.

Vulnerability Discussion If the NMS password is compromised, all DCPs in the network can be disabled from a single point resulting in denial of service to the customer.
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.

Checks

NMS Password Mgnt

The reviewer will interview the IAO to verify that there is a procedure in place to restrict knowledge of the NMS password to individuals that configure the Data Communications Processor (DCP). This policy should also require the changing of the password every 365 days or whenever an individual that has knowledge of the password no longer needs access to the DCP.

Fixes

NMS Password Mgnt.

Ensure only those individuals with a valid need to know have access to the NMS password and ensure the password is changed every 365 days or whenever an individual that has knowledge of the password no longer needs access to the DCP. Develop written documentation of this procedure.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A101.120.00 V0000563 CAT II DCP Dial-up connections

8500.2 IA Control: EBRP-1, EBRU-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.2, Computing Services Security Handbook

Vulnerability DCP dial-up connections are not properly secured.

Vulnerability Discussion Dial-up connections present a remote point-of-entry into the data network and must be secured like other network access points to prevent unauthorized users from gaining access to the systems. These are old interfaces and none are in use within DoD.
The IAO will ensure the site implement additional security measures to secure dial-up connections to DCPs.

Checks

DCP Dial-up

Interview the IAO to ascertain whether DCP hosted dial-up connections are in use. If they are in use verify that there is a procedure to manual secure the dial-up lines.

Fixes

DCP Dial-up

Secure dial-up connections in accordance with the guidelines provided in the Computing Services Security Handbook.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.020.00 V0000541 CAT III SAAR form or equivalent usage

8500.2 IA Control: PRAS-1, PRAS-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.8

Vulnerability A System Authorization Access Request (SAAR), DD Form 2875 dated MAY 2004, (or equivalent form) is not being used to request and document access to DoD information systems.

Vulnerability Discussion Use of a standard form for documenting the users, their authorized privileges and exceptions, their supervisor requesting the access, and their supervisor confirming their need-to-know, makes it easier to validate and contact the user when suspicious activity occurs. 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.

Checks

SAAR form

The reviewer will interview the IAO to verify that all users are granted access to the system only after the IAO has received and verified a the current DoD recommended Systems Access Authorization form or an equivalent form. This includes:
Individual user userids.
System Userids which are owned by the IAO and can be
documented on a single form.
System application userids to run specific system
required applications. These are treated the same
as system userids.
Application userids where the point-of-contact for the
application ownes the userid.
FTP userids which are application userids.

Fixes

SAAR form

Use the current DoD recommended SAAR form, or and equivalent, to document new users access, privileges and authorization.

If there are undocumented users that have access to the system, disable the users until documentation is available.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.050.00 V0000542 CAT II Current user information

8500.2 IA Control: PRAS-2, PRAS-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability The IAO does not maintain current information records on all userids/subadministrators the IAO directly administers.

Vulnerability Discussion Userids owned and administered by the IAO are highly privileged or specially tailored userids, and if not properly documented or managed, can pose a serious threat to the system.
The IAO will maintain current information records on all userids/subadministrators the IAO directly administers.

Checks

SAAR form

The reviewer will interview the IAO to verify that all users are granted access to the system only after the IAO has received and verified a the current DoD recommended Systems Access Authorization form or an equivalent form. This includes:
Individual user userids.
System Userids which are owned by the IAO and can be
documented on a single form.
System application userids to run specific system
required applications. These are treated the same
as system userids.
Application userids where the point-of-contact for the
application ownes the userid.
FTP userids which are application userids.

Fixes

SAAR form

Use the current DoD recommended SAAR form, or and equivalent, to document new users access, privileges and authorization.

If there are undocumented users that have access to the system, disable the users until documentation is available.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.070.00 V0000573 CAT III Batch userids

8500.2 IA Control: PRAS-1, PRAS-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.3

Vulnerability Standard userids used to start batch jobs on the system are not documented on a SAAR in accordance with this STIG.

Vulnerability Discussion The userids used to start batch jobs on the system are highly privileged and must be properly documented so the IAO has all the necessary information concerning the use of these user-IDs and the organization that is responsible for these userids.
The IAO will ensure standard userids used to start batch jobs on the system are documented on a SAAR in accordance with this STIG.

Checks

SAAR form

The reviewer will interview the IAO to verify that all users are granted access to the system only after the IAO has received and verified a the current DoD recommended Systems Access Authorization form or an equivalent form. This includes:
Individual user userids.
System Userids which are owned by the IAO and can be
documented on a single form.
System application userids to run specific system
required applications. These are treated the same
as system userids.
Application userids where the point-of-contact for the
application ownes the userid.
FTP userids which are application userids.

Fixes

SAAR form

Use the current DoD recommended SAAR form, or and equivalent, to document new users access, privileges and authorization.

If there are undocumented users that have access to the system, disable the users until documentation is available.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.090.00 V0000703 CAT II Administrator generated passwords not random

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.2

Vulnerability There are no written procedures to ensure user passwords are changed to a random value at install, deactivation, or reset time.

Vulnerability Discussion Using a non-random password scheme provides a means for unauthorized personnel to obtain a password and access the system.
The IAO will developed a written procedures to ensure user passwords are changed to a random value at install, deactivation, and reset time.

Checks

Password policy

The reviewer will interview the IAO to verify that there is a written procedure for password construction rules. This procedure will include the generation of random passwords by the IAO or SA when creating a new userid, reactivating a deactivated userid, or resetting a password.

Fixes

Password Policy.

Develop and implement a written procedure for implementing password rules including processes to ensure passwords are changed to a random value at install, deactivation, or reset time.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.100.00 V0000702 CAT II User termination notification procedure.

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.4

Vulnerability There are no procedures to ensure prompt notification of a user’s transfer, retirement, administrative action, or extended absence so the userid can be disabled.

Vulnerability Discussion Unauthorized personnel can exploit the userids that are no longer needed to gain access to the system.
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.

Checks

Userid retirement procedure

The reviewer will interview the IAO to verify that there is a procedure in place to notify the IAO when a userid is not longer needed, either by the user leaving, being transfered, or a change in duties removed the need-to-know.

Fixes

Userid retirement procedure

Design, document, and implement an enforceable process that ensures that the sub-administrators, TASOs, or IAO are notified of PCS, retirement, administrative action, or extended absence so that any userid owned by the user can be deactivated.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.110.00 V0000704 CAT II ACR Update Procedure for unused userids

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.4, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.4.1.3.1

Vulnerability ACRs on the system containing hard-coded userid names in the condition field are updated when the userid is deactivated.

Vulnerability Discussion Failure to remove hard-coded user-IDs from ACR condition fields potentially allows greater access than required when the userid is reassigned to a new user.
The SA will ensure ACRs on the system contain hard-coded userid names in the condition field are updated when the userid is deactivated.

Checks

ACR update for old userids

The reviewer will interview the SA to ensure that userids that are deactivated are removed from Access Control Records (ACR).

Fixes

ACR update old userids

The IAO will develop and implement procedures to ensure ACRs are updated when a userid is deactivated. This procedure will be disseminated to all SAs with the responsibility of ACR maintenance.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.240.00 V0000710 CAT II Scrubbing classified from unclassified system

8500.2 IA Control: VIIR-1, VIIR-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.6, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE Appendix F

Vulnerability The IAO does not have written procedures for handling the introduction of classified material into the system.

Vulnerability Discussion Data of a higher classification than authorized for a given system could be compromised if introduced. In addition, the availability of the system to end users could be interrupted for a significant time period during the decontamination process. Having procedures in place will minimize the operational impact on the customer as well as the potential data compromise.
The IAO will ensure there are written procedures for handling the introduction of classified material into the system.

Checks

Scrub Classified

The reviewer will interview the IAO to ensure that a procedure exist for the removal of inadvertent introduction of classified information on an unclassified system.

Fixes

Scrub Classified

Develop and document written procedures for the removal of of classified information inadvertent introduced into the system. This procedure should include points of contact, detailed checklist of steps to perform, and incident reporting contacts.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.250.00 V0000711 CAT II Media handling

8500.2 IA Control: PECS-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3

Vulnerability There are no written procedures to make certain all unclassified tapes, disks, and other storage media is cleared prior to off-site maintenance or salvage.

Vulnerability Discussion FOUO, Privacy Act, and Sensitive Unclassified information can be recovered from salvaged storage media.
The IAO will ensure written procedures exist to make certain all unclassified tapes, disks, and other storage media is cleared prior to off-site maintenance or salvage.

Checks

Media Sanitation unclassified

The reviewer will interview the IAO to ensure that written procedures exist to make certain all unclassified tapes, disks, and other storage media is cleared prior to off-site maintenance or salvage.

Fixes

Media Sanitation unclassified

Develop and document written procedures to ensure that storage media are erased prior to offsite maintenance or salvage. Acquire appropriate equipment for this process.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.260.00 V0000751 CAT II Media Disposition Classified

8500.2 IA Control: PECS-2, PEDD-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3

Vulnerability There are no written procedures and/or equipment to ensure that classified tapes, disks, and other storage media are rendered unreadable by approved methods, in accordance with DOD 5200.1-R, prior to offsite maintenance or salvage.

Vulnerability Discussion Classified information can be recovered and potentially exploited from salvaged storage media.
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.

Checks

Media Disposition Classified

The reviewer will interview the IAO to ensure that there are documented procedures for the sanatizing and disposal of classified tapes, disks and other storage media.

Fixes

Media Disposition Classified

Develop and document written procedures to ensure that storage media containing classified information are sanatized prior to offsite maintenance or salvage. Acquire appropriate equipment for this process.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.340.00 V0004104 CAT II Emergency CMS 1100 Dynamic configuration changes

8500.2 IA Control: DCPR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.5.2

Vulnerability There is no procedure for documenting emergency CMS 1100 Dynamic configuration changes.

Vulnerability Discussion Without procedures to document CMS 1100 Dynamic configuration changes there will be no way to verify that a Dynamic change was authorized and the Dynamic change may be lost and not applied to the Static CMS 1100 configuration. This can lead to a denial of service.
The SA will ensure, if in an emergency a dynamic update must be made, it is logged in the security log.

Checks

CMS dynamic change

The reviewer will interview the IAO to verify that there is a procedure that describes how to document emergency dynamic configuration changes.

The procedure will contain a step that displays the last time the configuration was changed. If the last time the configuration was changed does not match the configuration generation date, the log should be checked to verify that the previous change was correctly documented.

If dynamic changes are not allowed this will not be considered a finding.

Fixes

CMS Dynamic change

Develop, document, and deploy a procedure for documenting CMS 1100 Dynamic configuration changes in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.350.00 V0004105 CAT II CMS Undocumented Dynamic Changes

8500.2 IA Control: DCPR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability There is no procedure to verify that no undocumented Dynamic CMS 1100 changes have been made.

Vulnerability Discussion Without a procedure to verify that no undocumented Dynamic CMS 1100 changes have been made, the CMS 1100 configuration could be modified and the change not be applied to the Static CMS 1100 configuration or an unauthorized change can be made.
The IAO will ensure there is a procedure to verify an undocumented dynamic change to the CMS 1100 configuration has not been made.

Checks

CMS Change Detection

Interview the IAO to verify that there is a procedure to periodically compare the CMS 1100 configuration dynamic update time to the CMS 1100 configuration build time.

If dynamic changes are allowed the procedure should check that all change are documented back to the point where the configuration change time matches the configuration build time.

If dynamic updates are not allowed then the procedure just needs to check that the CMS configuration build time equals the CMS configuration update time.

For this an AMS process that automates the check and generates an alert if they times do not match would be acceptable if there is a documented process for responding to the alert.

Fixes

CMS Change Detection

Develop, document, and deploy a procedure to verify that all CMS 1100 Dynamic configuration changes have been documented in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A102.360.00 V0004106 CAT II Retain CMS 1100 Change Documentation

8500.2 IA Control: DCPR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.5.2

Vulnerability The documentation is not being maintained long enough to guarantee that no undocumented Dynamic CMS 1100 configurations are being made.

Vulnerability Discussion If the documentation of a Dynamic CMS 1100 configuration changes is not maintained for at least 2 intervals, 48 hours, of checking that no new changes have been made there will be no way to verify that no unauthorized changes have been made.
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.

Checks

Retaining CMS change docs

The reviewer will interview the IAO to verify that CMS 1100 dynamic configuration change documentation and validation information is kept for 48 hours or the last two cycles of the validation check.

Fixes

CMS change documentation

Maintain all documentation of Dynamic changes to the CMS 1100 configuration for a period no less than required by the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A103.010.00 V0000746 CAT II CENLOG entries are not being generated

8500.2 IA Control: ECAT-1, ECAT-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.5

Vulnerability CENLOG entries are not being generated.

Vulnerability Discussion Without the CENLOG entries, there is no means of identifying security relevant events on the DCPs.
The SA or NA will ensure CENLOG entries are generated for all DCPs in the site network.

Checks

DCP CENLOG Creation

Interview the SA or NA to verify that if DCPs are used they are configured to create CENLOGs and save them to the host Unisys system.

Fixes

Ensure CENLOG entries are gene

Ensure CENLOG entries are generated for the DCPs located within the DECC/DECCD.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A103.020.00 V0000546 CAT III CENLOG entries are not being maintained

8500.2 IA Control: ECRR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.5

Vulnerability CENLOG entries are not being maintained in accordance with the standard.

Vulnerability Discussion The CENLOG entries must be retained long enough to provide data for investigation of network or system compromise.
The IAO will ensure CENLOG entries are retained for a minimum of 30 days.

Checks

DCP CENLOG Retention

The reviewer will interview the IAO to verify that the DCP CENLOGs will be retained for 30 days. Because of the size of the DCP CENLOGs and the limited usefulness of the information captured, data older than 30 days is of questionable value. This facility was designed more for hardware monitoring and problem detection than security.

Fixes

DCP CENLOG Retention

Retain CENLOG entries for the DCPs located within the DECC/DECCD for 30 days.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A103.030.00 V0000745 CAT II Default NMS Password Change

8500.2 IA Control: IAIA-2, IAIA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.8

Vulnerability The NMS password has not been changed from the default.

Vulnerability Discussion The NMS password allows individuals to affect DCP operations throughout the network. The Network or Systems Administrator will ensure the NMS password is changed from the default.

Checks

Default NMS Password

Try to sign on to the DCP using the default password. This will be either Security or TELCON.

At the DCP consol enter:

```
    $$OPEN NMSC
    IDE P TELCON
          and
    IDE P SECURITY
```

If the system responds in the affirmative to either IDE P commands this is a finding.

Fixes

Default NMS Password

Change the NMS password to a random value.

At the DCP consol enter the following:

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

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A103.040.00 V0000586 CAT II The NMS password construction

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.2.1

Vulnerability The NMS password does not comply with documented password construction rules.

Vulnerability Discussion NMS passwords that are easily guessed could allow unauthorized users to compromise one or more DCPs in the network. The SA will ensure the NMS password consist of a combination of alphanumeric, non-repeating, non consecutive characters.

Checks

NMS Password Construction.

The reviewer will interview the SA to verify that he sets the NMS password to a complex value as described in the Unisys STIG.

Fixes

Update the NMS password on eac

Update the NMS password on each DCP using documented password construction rules and ensure it is not easily guessed from one DCP to another.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A103.050.00 V0000548 CAT II TELCONs INSPECT command reveals the NMS password.

8500.2 IA Control: VIVM-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.2.1

Vulnerability TELCONs INSPECT command reveals the NMS password. Applies only to 10R2 and lower release levels of TELCON.

Vulnerability Discussion Under TELCON, the INSPECT command can be used to find the NMS password.
The SA will ensure the TELCON software change prevents a user from using the privileged INSPECT command to view the NMS password which is applied.

Checks

DCP Inspect Vulnerability.

IF the Telcon level is less than 10R2 interview the SA to verify that the patch that fixes the vulnerability allowing an non privileged user to display the NMS password.

Fixes

DCP Inspect vulnerability

Incorporate the TELCON software change that invalidates the use of the INSPECT command to find the NMS password.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A104.010.00 V0000613 CAT II System security posture montering

8500.2 IA Control: ECAT-1, ECAT-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.1

Vulnerability The system is not being actively monitored. The security logs are not being process on a regular basis to identify potential malicious activity.

Vulnerability Discussion Failure to regularly generate and review security reports outlining significant security events and/or threats prevents the IAO from being aware of potential malicious activity on the system.
The IAO will regularly review the system security posture for potential security weaknesses.

Checks

Security Integrity Review

The reviewer will interview the IAO to verify that there is regular activity to detect potentially malicious activity on the system.
The review techniques can be the running of one of the Unisys Log Analyzer products, the regular running of the SRR Manager Toolkit or a combination of both.

Fixes

Security Integrity Review

Schedule and run the security reports within the SRR Manager Toolkit. Retain the Toolkit reports for at least three cycles.
Regularly schedule and run and analyze the LA security reports.
A combination of both approaches would be optimal.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

A105.030.00 V0000696 CAT II JFT-GNO bulletin implementation

8500.2 IA Control: VIVM-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.5

Vulnerability The IAO is not implementing JTF-GNO bulletins in a timely fashion.

Vulnerability Discussion If the JFT-GNO bulletins are not implemented in a timely fashion a known vulnerability will not be mitigated.
The IAO will ensure JTF-GNO bulletins are being implemented in a timely fashion.

Checks

JTF-GNO IAVM implementation

The reviewer will interview the IAO to verify that there is a process for implementing JTF-GNO bulletins in a timely fashion.

Fixes

JTF-GNO IAVM implementation

The IAO will create and document a procedure to ensure that all applicable JTF-GNO bulletins are implemented in a timely fashion.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN110 V0012700 CAT II Training and certification plan is not in use.

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability The DOD component has not developed or implemented security training and certification plans and procedures.

Vulnerability Discussion Failure to provide security training results in a weak security program and can lead to the loss or compromise of classified or sensitive DOD information.

Checks

EN110

Work with the Traditional reviewer to determine compliance and interview the IAO and ask them to provide the IA training and certification documentation.

Fixes

EN110

The IAM will ensure that the DOD component develops and implements training and certification plans and procedures for all personnel who use DOD computer systems to include Certifiers and Managers of Information Systems. Reference DODD 8570.1.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN120 V0012701 CAT III No established security features training program.

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability There is not a comprehensive user security features training program to include password and Internet usage guidance.

Vulnerability Discussion Failure to provide security features training results in a weak security program and can lead to the loss or compromise of classified or sensitive information.

Checks

EN120

Work with the traditional reviewer to determine compliance and interview the IAM/IAO and ask to see the policy or documentation on security features (Internet usage, email usage, Unisys application usage, etc.) training requirements for all users.

Fixes

EN120

The IAM/IAO will establish and implement a comprehensive user security features training program to include password and Internet usage guidance (e.g. Security Features Users Guide or Standard Operating Procedure). Requirements for formal and awareness training are outlined in the DODD 8500.1, and the CJCSI 6510.01-C Information Assurance and Computer Network Defense,

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN130 V0012702 CAT II No established privileged user training

8500.2 IA Control: PRTN-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability No training of privileged users available. Long Name: Training and certification of privileged users (SAs), IAOs, and other professional or management security personnel, is not provided or available.

Vulnerability Discussion Failure to provide security training and certification results in a weak security program and can lead to the loss or compromise of classified or sensitive information.

Checks

EN130

Work with the traditional reviewer to determine compliance and interview the IAO to determine if there is a documented certification and training plan implemented for all privileged users and IA professionals.

Fixes

EN130

The IAM will provide training and certification for all privileged users (i.e. SAs, database administrators, mass storage administrators, and network administrators), as well as for all IAOs and other security personnel based on DOD and DISA SA standards for certification.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN140 V0012745 CAT II Need-to-Know policy is not followed.

8500.2 IA Control: ECAN-1, ECLP-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Users, privileged users and IAOs have access to data, control information, software, and hardware for which they are not authorized access and do not have a need-to-know.

Vulnerability Discussion In order to ensure the confidentiality of an IS, a determination needs to be made as to whether a user has the appropriate credentials to access a system or network. The need-to-know principle is determined by the necessity for access to, knowledge or possession of, specific official DOD information required to carry out official duties. The need-to-know determination is derived from a decision made by an authorized holder of official information that a prospective recipient requires access to specific official information to carry out official duties. Need-to-know principles are applied to ISs within the DOD, and appropriate measures must be in place in order to verify and authorize individuals at all levels. This can be accomplished using various methods such as denying access after multiple unsuccessful logon attempts; however, stringent controls must be in place to standardize this process. Strong authentication controls such as PKI should be used for all privileged access.

Checks

EN140

Work with all reviewers to determine compliance. Interview the IAO to determine if documentation/policy exists to enforce least privilege and need-to-know principles.

Fixes

EN140

The IAM will ensure that privileged users and IAOs access only that data, control information, software, and hardware for which they are authorized access and have a need-to-know.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN150 V0012746 CAT II No discretionary or role based access controls.

8500.2 IA Control: ECAN-1, ECPA-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Discretionary or role based access controls are not established.

Vulnerability Discussion Under the RBAC framework, users are granted membership into roles based on their competencies and responsibilities in the organization. The operations that a user is permitted to perform are based on the user's role. User membership into roles can be revoked easily and new memberships established as job assignments dictate. Role associations can be established when new operations are instituted, and old operations can be deleted as organizational functions change and evolve. This simplifies the administration and management of privileges; roles can be updated without updating the privileges for every user on an individual basis. (NIST/ITL Bulletin, December, 1995)

Checks

EN150

Interview the IAO to determine if there is a process or procedure to ensure that discretionary or role-based access controls are established and enforced, via operating system and application controls. The IAO/IAM must enforce the establishment and use of RBAC and discretionary access controls.

Group and unique userid establishment, to separate duties and need-to-know requirements, must be enforced via OS and application access controls.

The userid profiling system described in the Unisys STIG fulfills this check.

Fixes

EN150

The IAM/IAO will ensure discretionary or role-based access controls are established and enforced, via operating system controls. Group and unique userid establishment, separating duties and functions, should be enforced within the access controls on all operating systems and applications.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN160 V0012748 CAT II Documentation of need-to-know is not available.

8500.2 IA Control: PRNK-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Documentation of need-to-know (e.g. DD Form 2875 or similar access form) is not available, does not exist, or is incomplete for individuals with access to a DOD network.

Vulnerability Discussion If accurate records of authorized users are not maintained, then unauthorized personnel could potentially gain access to a system or the enclave.

Checks

EN160

Work with the traditional reviewer to determine compliance and interview the IAO to determine if there is a policy in place to require system access forms for all users.

Fixes

EN160

The IAM/IAO will ensure all individuals with access to a DOD system or network require the following in the form of a DD Form 2875 or similar access authentication form:

- Verification of the users security clearance and/or investigative requirement for holding an IT (formerly ADP) position.
- Verification of the need-to-know and permission to access the data by the information owner.
- Verification of training
- Acknowledgment, in writing, of users responsibilities to protect the system, data, and password.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN170 V0012749 CAT II Not compliant with DOD personnel requirements.

8500.2 IA Control: PRAS-1, PRAS-2

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Personnel authorization and investigation requirements are not in accordance with the DODI 8500.2.

Vulnerability Discussion Failure to investigate personnel based upon their position sensitivity could result in personnel conducting sensitive duties who have derogatory information in their past
precluding them from holding a sensitive position.

Checks

EN170

Work with the traditional reviewer to determine compliance. Interview the IAO to ensure compliance with the DOD 8500.2 and DOD 5200.1-R requirements for personnel security.

Fixes

EN170

The IAM/IAO will ensure personnel authorization and investigation requirements are processed in accordance with DODI 8500.2

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN210 V0012750 CAT II COOP or disaster recovery plans not exercised.

8500.2 IA Control: COED-2, COED-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability COOP or disaster recovery plans are not exercised in accordance with the MAC level of the system or network.

Vulnerability Discussion Failure to develop a COOP and test it periodically can result in the partial or total loss of operations and INFOSEC. A contingency plan is necessary to reduce mission impact in the event of system compromise or disaster.

Checks

EN210

Interview the IAO to determine if a process is in place to exercise COOP and disaster recovery plans in accordance with MAC level requirements.

This check does NOT apply to Compliance Validation Visits.

Fixes

EN210

The IAM will ensure that the continuity of operations (COOP) or disaster recovery plans or significant portions are exercised in accordance with the requirements set forth in the DODI 8500.2 for the appropriate MAC level of the systems.

COED-2 - COOP, Semi-Annual testing MAC I

COED-1 - COOP, Annual testing MAC II and MAC III

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN220 V0012751 CAT II A disaster recovery plan does not exist.

8500.2 IA Control: CODP-1, CODP-2, CODP-3

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability A disaster recovery plan does not exist.

Vulnerability Discussion Failure to develop a disaster recovery plan and test it periodically can result in the partial or total loss of operations and INFOSEC. A contingency plan is necessary to reduce mission impact in the event of system compromise or disaster. Recovery procedures are critical to IA and the protection of the infrastructure. If a system is compromised, shut down, or otherwise not available for service, this could hinder the availability of resources to the warfighter.

Checks

EN220

Interview the IAO and ask to see the Disaster Recovery Plan that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level.

Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.

This check does NOT apply to Compliance Validation Visits

Fixes

EN220

The IAM will ensure a disaster plan exists that provides for the resumption of mission or business essential functions within the specified period of time depending on MAC level. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

CODP-1 MAC III
A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans,
and plan acceptance.)

CODP-2 MAC II
A disaster plan exists that provides for the resumption of mission or business essential functions within 24 hours activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

CODP-3 MAC I
A disaster plan exists that provides for the smooth transfer of all mission or business essential functions to an alternate site for the duration of an event with little or no loss of operational continuity. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN230 V0012752 CAT II Critical systems are not backed up.

8500.2 IA Control: COBR-1, COSW-1

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Critical systems are not backed up and/or copies of the OS and other critical software are not stored appropriately.

Vulnerability Discussion The use of backups is an integral part of system security. If an operating system or a file is maliciously or inadvertently deleted or corrupted, the system backup provides a valid
replacement for the damaged item. In addition to being a vital part of system security, system backups are required for disaster recovery programs.

Checks

EN230

Interview the IAO to determine if there is a backup policy in place to ensure backup of critical systems and that backup copies of the Operating Systems other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software.

Work with all reviewers to determine compliance with the backup policy.

This check does NOT apply to Compliance Validation Visits.

Fixes

EN230

The IAO will ensure all critical systems, to include infrastructure devices such as routers and inventory records, are backed up and copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational equipment or software.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

EN240 V0012753 CAT II Data backup is not properly performed.

8500.2 IA Control: CODB-1, CODB-2, CODB-3

References: ENCLAVE SECURITY TECHNICAL IMPLEMENTATION GUIDE , UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE

Vulnerability Data backup is not performed daily and recovery media is not stored offsite.

Vulnerability Discussion The use of backups is an integral part of system security. If an operating system or a file is maliciously or inadvertently deleted or corrupted, the system backup provides a valid replacement for the damaged item. In addition to being a vital part of system security, system backups are required for disaster recovery programs.

Checks

EN240

Interview the IAO to determine if there is a backup policy in place that ensures data backup is performed daily, and recovery media is stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data.
For Unisys systems using MAPER or UDS databases with full audit trail, a carefully implemented dynamic backup with the appropriate audit files also backed up, would fulfill the offline backup requirements for the database portion of the offline backup.

CODB-3 Data Backup Procedures MAC I
Data backup is accomplished by maintaining a redundant secondary system, not collocated, that can be activated without loss of data or disruption to the operation.

CODB-2 Data Back-up Procedures MAC II
Data backup is performed daily, and recovery media are stored off-site at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

CODB-1 Data Backup Procedures MAC III
Data backup is performed at least weekly.

This check does NOT apply to Compliance Validation Visits.

Work with the reviewers to determine compliance.

Fixes

EN240

The IAO will ensure data backup is performed daily, and recovery media is stored offsite at a location that affords protection of the data in accordance with its mission assurance category and confidentiality level.

On-line backups to remote sites meet the requirement for off-site storage; however, off-line backups are also required to ensure integrity of the data.
For Unisys systems using MAPER or UDS databases with full audit trail, a carefully implemented dynamic backup with the appropriate audit files also backed up, would fulfill the offline backup requirements for the database portion of the offline backup.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.010.00 V0000709 CAT II Operator unique userids

8500.2 IA Control: IAGA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.1

Vulnerability Each operator on the system does not have a unique userid for use outside of the console area.

Vulnerability Discussion Anytime an operator starts a session using the terminal, or terminal emulation software, other than on the master console, the actions accomplished during the session cannot be attributed to a unique user if the operator does not have a unique userid.
The IAO will ensure each operator who needs access to the system outside the console area has a unique userid.

Checks

Operator unique userids

The reviewer will interview the IAO to verify that each operator who needs to access the system outside of the master console area is given a unique userid.

Fixes

Operator unique userid

Assign a unique userid to each operator requiring access to the system outside of the system console area.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.020.00 V0000697 CAT I The Master Userid is access

8500.2 IA Control: IAGA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.5

Vulnerability The Master userids is being used by more than one person.

Vulnerability Discussion With more than one person sharing any user-ID on the system, there can be no positive identification of user actions. This is critical with the Master userid which has complete span of control in the OS-2200 environment.
The IAO will ensure the Master Userid is only be used by a single IAO.

Checks

Master Userid Access

The reviewer will interview the IAO to verify that only one IAO uses the Master userid.

Fixes

Master Userid Access

Assign the Master userid to the primary DECC IAO. Alternate IAOs at the DECC should be given SIMAN Administrator userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.030.00 V0000555 CAT II TIP audit trails are not secured

8500.2 IA Control: ECTB-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.2

Vulnerability TIP audit trails are not physically and logically secured.

Vulnerability Discussion If TIP audit trails are not sufficiently protected, incident investigation and application recovery could be severely hampered, resulting in denial of service to the customer.
The IAO will ensure TIP audit trails are physically and logically secured.

Checks

TIP Audit Backup

The reviewer verify that the TIP audits are backed up and secured both physically and logically.
Things to check include:
TIP audit trails can be configured for tape or on disk. If they are on tape, they will be called SYS$*AUDIT$0x where x is the application group number. If they are on disk, they will be called SYS$*AT$xL1 and/or SYS$*AT$xL2 (leg 1/leg 2) where x is the application group number. For tape audit trails, go into STAR and verify that the TIP audit trails are R-option tapes. For disk audit trails, the Clearance Level will be 0 or 63 and the files will have either ACRRO or ACRNA attached to them. TIP audit trails on disk should be saved to tape (SYS$*AUDIT$0xUNT1) using the IRU MOVE command and these tapes should be identified in STAR as R-option tapes. Make sure the TIP audit trails are located in the computer room (or offsite storage if the site is keeping them there).

Fixes

TIP Audit Backup

Physically and logically secure the TIP audit trails as described in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.040.00 V0000561 CAT II Software development on a production system

8500.2 IA Control: ECSD-1, ECSD-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 13

Vulnerability Software development on a production system is not separated in accordance with the standard.

Vulnerability Discussion Performing software development on a production system opens the system to increased risk due to the highly privileged development user-IDs and activities. This situation can also compromise software integrity if untested and unverified software is moved to production files.
The IAO will ensure software development on a production system is separated through the use of a separate ALN or unique qualifiers.

Checks

Software Development on produc

The reviewer will interview the IAO to verify that if software developement is done on the production system the production enviornment is protected.

Some of the questions to ask are:

For ALN CDAs, dedicated development systems are usually used for software development. DNMC and DFAS-IN CDAs usually perform software development on production systems. These shared production/development systems should use, as a minimum, a different qualifier to separate development software from production software. Read/Write keys and ACRs may also be appropriate. Configuration management procedures should be used when development software is moved to production files and DECC application support personnel should be kept in the loop.

Fixes

Software developement on produ

Ensure software development is separated from production workload in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.040.10 V0006504 CAT II Software Developement On Production Requirement CM

8500.2 IA Control: DCPR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 13

Vulnerability Configuration Management Policies for development in a production environment are not implemented or are not enforced.

Vulnerability Discussion Without special policies and their enforcement, a denial of service or the compromise of sensitive data can be caused by the inadvertent loading of untested software into production files.
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.

Checks

Unisys Developement in Product

The reviewer will interview the IAO to verify that there are configuration control policies and procedures in place to protect the production environment from the development activities.

Fixes

Unisys Developement in Product

Establish and document configuration management polocies and procedures to protect the production environment from developement activities.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.050.00 V0006431 CAT I Software Patch Maintenance

8500.2 IA Control: VIVM-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability Security related system software patched are not being located, tested and applied in a timely manner.

Vulnerability Discussion If system software security related patches are not located and applied in a timely manner, the system software will be at risk to a known vulnerability that could be exploited. Depending on the vulnerability in question this could lead to the compromise of sensitive data or a denial of service.
The IAO or SA will ensure all security related patches supplied by Unisys are located, applied and tested.

Checks

Security Patches

The reviewer will interview the IAO to verify that the Unisys support site is checked regularly for security related patches to the level of software installed on the system. When security related patches are found are they applied and tested prior to use in a production environment. If possible testing will be on a dedicated test system or during block time without normal access allowed to the system.
If the support for the software is performed by another entity does the SLA describing the support provide for the application of security patches in a timely manner? Additionally does the IAO check the Unisys support site and notify the supporting entity when a security fix has been release but the support provider has not updated the software.

Fixes

Unisys Security Patches

Establish a procedure to ensure that security patches to system software is located, installed, and tested.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.060.00 V0006436 CAT I Verder Droping Software Support

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability Software no longer supported by the vendor has not been removed from the system or upgraded to a supported level.

Vulnerability Discussion Software no longer supported by the vendor will not have patches created for newly discovered vulnerabilities. This leaves the software exposed to exploits of these vulnerabilities.
The IAO or SA will ensure unsupported system software is removed or upgraded prior to a vendor dropping support.

Checks

Unisys Unsupported Software

The reviewer will interview the IAO to verify that all software on the system is supported by the vendor. Software is considered supported if the level of the software is currently in general support by the vendor, the vendor will support any registered user of the software, or there exist a service agreement between the vendor and the site that guarantees the support of the level of the product currently in use.
The current general supported releases of Unisys System Software are:
CP 2200 8.x thru 7/31/2005
CP 2200 9.x thru 9/30/2006
CP 2200 10.x thru 10/31/07

Fixes

Unisys Unsupported Software

After thorough planning and testing, and with Configuration Control Board approval, migrate to a supported level of systems software.
If there is no vendor supported level of the software:
Find an acceptable replacement for the software, test the replacement, modify applications as needed, obtain Configuration Control Board approval, install the new software and remove the unsupported software.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S101.070.00 V0006437 CAT II Formal Migration Plan

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.4

Vulnerability There is no formal migration plan for removing or upgrading the OS systems prior to the date the vendor drops security patch support.

Vulnerability Discussion Having a formal migration plan for removing or upgrading OS systems prior to the date the vendor drops security patch support will lessen the impact of the migration and reduce the exposure to vulnerabilities found after the vendor drops security patch support.
The IAM 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.

Checks

Unisys Formal Migration Plan

The reviewer will interview the IAM to verify that there is a formal plan for removing or upgrading the OS software prior to the date the vendor drops security patch support.

Fixes

Unisys Migration Plan

Develop a formal plan for removing or upgrading the OS software prior to the date the vendor drops security patch support.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S102.014.00 V0003890 CAT II FTP Password Change

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.3.5

Vulnerability There is no procedure to coordinate the change of system-to-system FTP passwords at least every 365 days.

Vulnerability Discussion The passwords used in system to system FTP transfers need to be changed at least every 365 days or when an administrator who knows the password no longer administers the system. When these passwords are changed, the change has to be coordinated between the sending system and the receiving system to avoid an interruption of production processes. Failure to change the password can lead to a compromise of the system and the data contained on the system. Failure to coordinate the change could lead to an interruption of service.
The SA will ensure the maximum allowable password setting for FTP userids used for system to system transfers up to 365 days.

Checks

Unisys S102.014.00 verify

The reviewer will check the SRRALL file for the last password changed date or run the SSO provided SQL Query FTP-Pass-Chg against the SRR Toolkit database

Unisys S102.014.00

The refviewer will interview the IAO to verify that a procedure is in place to make sure the password for the FTP interface useridis are changed at least once every 365 days. The IAO may check the SRRALL file for the last password changed date or run the SSO provided SQL Query FTP-Pass-Chg against the SRR Toolkit database.

Fixes

Unisys S102.014.00

Develop a procedure to change the system to system FTP passwords in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S102.020.00 V0000587 CAT III Subadministrators Userid Transfer

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.7

Vulnerability IAOs and SAs are not keeping a complete and accurate security log of SIMAN subadministrator userid assignments.

Vulnerability Discussion In a decentralized security environment, the creation of userids has been delegated to site subadministrators. However, only the owner of the userid can apply any subsequent changes and only one subadministrator can own a userid. At sites that are supporting a 24X7 operational environment, the subadministrator userid is transferred during shift turnovers or emergency situations. To ensure there is a clear line of accountability for all actions performed by this userid, a security log is maintained to record all transfers of this userid.
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.

Checks

Subadmin Userid transferred

The reviewer will check the security log for at least one subadministrator userid one per system, especially if the site has more than one primary and alternate subadministrator or if the site runs a 24X7 operations, to verify that the procedures are being followed. The log should have the date/time and names of those involved with the transfer of the subadministrator userid.

Fixes

Subadmin Userid Transferred

Ensure all subadministrators are keeping a security log to record any transfers of the subadministrator userid. The IAO should include a review of this log in the semiannual audit of subadministrators.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.050.00 V0000727 CAT II Security Files Backup

8500.2 IA Control: COBR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 4.1.1.2

Vulnerability The security files are not being backed up properly.

Vulnerability Discussion The security system cannot be easily recovered without a current set of backup security files. If a recovery situation is encountered, additional efforts will be necessary to reapply changes made since the last backup was taken. This will delay restoration of computer support to the end user.
The IAO will ensure two cycles of the four security tapes (TSS$FILE, ACCOUNT$R1, SACRD$, and SIMAN$INFO) are available at all times.

Checks

Unisys Security Files Backup

The reviewer will check the STAR reports to see what tapes are available. The SRRPRT also provides this STAR information. NOTE: If a site is using the SEC,SAVE keyin, the TSS$FILE, ACCOUNT$R1, and SACRD$ files are saved on a single tape with a file name of SACRD$SAVE. The IAO should ensure that the TSS$FILE, ACCOUNT$R1, SACRD$, and SIMAN$INFO files are saved twice a week and kept 14 days. For ALN the SECMERGE tape, if created, will be saved at least monthly.

Fixes

Unisys Security Files Backup

Backup the security files in accordance with the Unisys STIG and ensure proper retention techniques are utilized.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.070.00 V0000712 CAT II Warnning Banner before and after

8500.2 IA Control: ECWN-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran
APPENDIX C TO ENCLOSURE C, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.5

Vulnerability The Standard Warning Message regarding authorized use of computers is not being displayed prior to or after signon completion.

Vulnerability Discussion Failure to properly notify unauthorized individuals attempting to access the system can impede prosecution efforts.
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.

Checks

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Fixes

Warning Banner

Implement local code to display the Standard Warning Message prior to signon solicitation and after signon completion.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.072.00 V0003892 CAT III Warning Banner before Sign in

8500.2 IA Control: ECWM-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran APPENDIX C TO ENCLOSURE C, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.5

Vulnerability The Standard Warning Message regarding authorized use of computers is not being displayed prior to sign on solicitation.

Vulnerability Discussion Failure to properly notify unauthorized individuals attempting to access the system can impede prosecution efforts.
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.

Checks

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Fixes

Warning Banner

Implement local code to display the Standard Warning Message prior to signon solicitation and after signon completion.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.074.00 V0003893 CAT III Warning Banner After

8500.2 IA Control: ECWM-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran
APPENDIX C TO ENCLOSURE C, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.5

Vulnerability The Standard Warning Message regarding authorized use of computers is not being displayed after sign on completion.

Vulnerability Discussion Failure to properly notify unauthorized individuals attempting to access the system can impede prosecution efforts.
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.

Checks

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Warning Banner

The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer will sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer should check the TCP/IP and CpFTP connections as well. The warning should be displayed prior to sign on solicitation and after sign on completion. <br>The reviewer sign on to the system in all session modes, including all TIP Application Groups on the system. The reviewer will check the TCP/IP and CpFTP connections as well. This warning should be displayed prior to sign on solicitation and after sign on completion.

Fixes

Warning Banner

Implement local code to display the Standard Warning Message prior to signon solicitation and after signon completion.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.076.00 V0003894 CAT III Warning Banner Content

8500.2 IA Control: ECWM-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran
APPENDIX C TO ENCLOSURE C, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.5

Vulnerability The Standard Warning Message regarding authorized use of computers does not contain the five points required.

Vulnerability Discussion Failure of the Standard Warning Message to contain the five points required by CJCSM 6510.01 can impede prosecution efforts.
The IAO will ensure the warning banner contains the five points required by CJCSM 6510.01 dated March 25, 2003.

Checks

Warning Banner Content

The reviewer will check the content of the warning banner that is displayed. If SSO Montgomery provides support for a particular site, then the standard warning message will contain the five points required by the referenced policy documents. If SSO Montgomery does not provide support for the site, then the reviewer should check the warning message against the Unisys STIG to make sure it contains the five points required.

Fixes

Warning Banner Content

Modify the local code to display the Standard Warning Message containing the five required points prior to sign on solicitation and after sign on completion.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.080.00 V0000728 CAT II TIP Audit trail Retention data recovery

8500.2 IA Control: ECDC-1

References:

Vulnerability TIP Audit trail cycles are not retained in accordance with the standard.

Vulnerability Discussion The TIP audit trails must be retained long enough so they are available for integrated recovery and tracking down possible system compromise.
The IAO will ensure TIP audit trails tapes or disk files are retained for a minimum of 30 days.

Checks

TIP Audit retention

TIP audit trails can be configured for tape or on disk. If they are on tape, they will be called SYS$*AUDIT$0x where x is the application group number.

If they are on disk, they will be called SYS$*AT$xL1 and/or SYS$*AT$xL2 (leg 1/leg 2) where x is the application group number. If on tape, the reviewer will check STAR verify the tapes (SYS$*AUDIT$0x) are being retained based on the volume creation date (VCRTDT) with a 30-day retention. The Volume Scratch (VOLSCR) flag in the STAR AAFPARM file can be used to ensure the TIP Audit Trail tapes are scratched based on this volume create date. The IAO can also check the SYS$*LIB$.CO$CONFIG for the default retention of the TIP Audit Trail tapes.

If the TIP Audit Trails are on disk (SYS$*AT$xL1), then they should be saved via the IRU MOVE command (SYS$*AUDIT$0xUNT1) and kept for 30 days. The reviewer will check STAR to verify the tapes (SYS$*AUDIT$0xUNT1) are being retained based on the volume creation date (VCRTDT) with a 30-day retention. The Volume Scratch (VOLSCR) flag in the STAR AAFPARM file can be used to ensure the TIP Audit Trail tapes are scratched based on this volume create date.

Fixes

Tip Audit retention

Retain the TIP audit trail cycles for a minimum of 30 days.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.090.00 V0000729 CAT II System Log Cycles

8500.2 IA Control: ECRR-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.1

Vulnerability The cycle threshold for the system log file is not set high enough to prevent overwriting data prior to backup.

Vulnerability Discussion The cycle threshold of the system log file must be set high enough so all system log files are properly backed up and available for use when investigating system compromise or reviewing other security relevant events.
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.

Checks

System Log Cycles

The reviewer will do an @CYCLE on the SYS$*F010L1 file. Verify the number of cycles. The reviewer will use @PRT,F to check the earliest and latest available cycles. See if backup information is listed on these two files. Do other @PRT,Fs to see how frequently the files are being created. If saved daily, verify all cycles are backed up. Some of this information is provided in the SRRPRT.

Fixes

System Log Cycles

The cycle threshold should be set to a value that provides for tape backup of all cycles.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.100.00 V0000730 CAT II System log files/save tapes retention

8500.2 IA Control: ECRR-1

References:

Vulnerability System log files/save tapes are not being retained in accordance with the standard.

Vulnerability Discussion The system log file must be retained long enough to provide data for the investigation of possible system compromise and the review of other security relevant events.
The IAO will ensure the system log file save tapes are retained at least one year (365 days).

Checks

System Log file retention

The reviewer will find out what method is used to backup the system log files, SYS$*F010L1. Then the review should check STAR to verify that the tapes created by the backup method chosen are retained for 365 days. An expiration code of 1900 (scratch tape when the entry is no longer in the MFD) is risky and is not recommended for use.

Examples of ways the log may be backuped to tape.
.
The site should be saving these files in a separate FAS runstream on a daily basis (possibly a merge weekly). If this method is used the the reviewer will check any SAVE/SAVALL exemption lists to make sure the SYS$*F010L1 files are identified for exemption, otherwise cycles may be dropped during the daily LOG saves. The reviewer should make sure all cycles of the F010L1 file are exempted by using the FAS masking character in the cycle field (for example, (%).
.
Some sites may use LA to create LOG-DAILY and LOG-MERGE tapes. If so, the reviewer should make sure the LOG-MERGE tapes are kept for 365 days.

Fixes

System Log File retention

Design and implement a process to copy the system log files to tape and retain log file save tapes for at least 365 days.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.110.00 V0000575 CAT II MAPPER Audit Trail File Retention

8500.2 IA Control: ECDC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.5.3

Vulnerability The MAPPER audit trail files are not being retained in accordance with the standard.

Vulnerability Discussion The MAPPER audit trails must be retained long enough so they are available for recovery and tracking down possible system compromise.
The IAO will ensure MAPPER audit trail tapes or disk files are retained for a minimum of 30 days.

Checks

MAPPER Audit File Retention

The reviewer will verify if the MAPPER audit trail files are kept on disk or tape. If they are on tape, they are listed as qualifier*AUDTRL and the reviewer will check STAR to verify
that they be kept for 30 days. If they are on disk, these files have a unique file name of the following format qualifier*AUDTRLxxxxxx where the xxxxxx varies. The reviewer will verify that the file cycles are being retained for 30 days. If the site has a procedure for backing up the disk audit files to tape the reviewer should verify that the tapes created are retained by STAR for 30 days.

Fixes

MAPPER Audit File Retention

Develope a procedure to retain the MAPPER audit trail files for a minimum of 30 days.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.120.00 V0000556 CAT I Security Tape Mounting

8500.2 IA Control: PRNK-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 4.1.1.2

Vulnerability Operators mount security tapes without confirmed authorization from the IAO or alternate IAO.

Vulnerability Discussion Mounting security tapes without proper authorization allows unauthorized users an opportunity to compromise the entire system security environment.
The IAO will ensure operators do not mount the security tapes except upon a verified request from the IAO.

Checks

Security Tape Mounting

The reviewer, with the consent and assistance of the IAO, will spoof a batch job by using the Security Officer’s userid as a runid and assigning a security tape. If the operators mount the tape without contacting the IAO or alternate IAO, then this is a finding.

Fixes

Security Tape Mounting

The operators should be trained to only mount security tapes with confirmed authorization from the IAO or alternate IAO.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.130.00 V0000565 CAT II Account related console message handling

8500.2 IA Control: PRNK-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.2

Vulnerability AER account-related console messages are not answered correctly.

Vulnerability Discussion The site IAO must maintain control over accounts and userids. If an operator or system answers account-related console messages incorrectly, it could allow users access to unauthorized accounts. Access to unauthorized accounts may allow a user to cross ALN boundaries, gain access to privileged system processors or ACRs, or create erroneous fee for service billing information.
The IAO will ensure AER account-related console messages are answered correctly.

Checks

Account Console Message

The reviewer, with the consent and assistance of the IAO, will enter an erroneous account during sign on and see how the operators or AMS answers the prompt. If an ‘A’ or ‘E’ is entered, then this is a finding.

Fixes

Account Console Message

Ensure operators are trained to answer these messages correctly. Additionally the IAO may set up the AMS SMART database to answer these messages correctly, however the operators need to be trained incase the AMS SMART console is disabled.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.140.00 V0000566 CAT II Tape Bypass Message handling

8500.2 IA Control: PRNK-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.4.2

Vulnerability Tape Bypass console messages are not answered correctly.

Vulnerability Discussion The tape management software on the system (STAR) provides for protection of tapes. If a user tries to bypass the tape management software, console messages are generated. If the operator or system answers these messages incorrectly, tapes can be overwritten, corrupted, or provide unauthorized users access to privileged information.
The IAO will ensure tape Bypass console messages are answered correctly.

Checks

Tape Bypass Handling

The reviewer will assign a tape with a ‘,1800’ and see how the operators or AMS answers the prompt. If a ‘Y’ is entered and the operators or AMS perform no other actions, this is a finding. The reviewer will try an output tape that access should not be automatically granted and an input tape that has the scratch bit set.

Fixes

Tape Bypass Handling

Ensure the operators are trained to answer these messages correctly. Additionally the IAO may set up the AMS SMART database to correctly answer these messages, however the operators must still be trained to handle the messages when AMS SMART console is disabled.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.150.00 V0000592 CAT II Scheduler Full Security is not implemented.

8500.2 IA Control: ECCD-1, ECCD-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.2

Vulnerability Scheduler Full Security is not implemented.

Vulnerability Discussion The Scheduler system is an automated workload scheduling system that controls the type, frequency, and number of batch jobs on the system. Individual userids and passwords must be implemented to ensure accurate accountability of all Scheduler actions.
The SA will ensure Scheduler Full Security is implemented.

Checks

Scheduler Full Security

The reviewer will try to execute schedule, normally and @Scheduler command. If prompted for a user-ID/password, Scheduler Full Security is implemented. If no password is requested, Partial Security is implemented. No prompt for a user-ID/password indicates No Security is implemented. If Partial or No Security is implemented, this is a finding.

Fixes

Scheduler Full Security

Implement Scheduler Full Security and assign individual userids and passwords to all authorized Scheduler users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.160.00 V0000593 CAT II The Scheduler Master Userid is shared among users.

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4

Vulnerability The Scheduler Master Userid is shared among users.

Vulnerability Discussion Scheduler Master Level Userids have significant privileges within Scheduler and must be accountable to a single user.
The IAO will ensure the Scheduler Master userid is not shared.

Checks

Scheduler Shared Master

The reviewer will interview the Scheduler point-of-contact and ask if the Scheduler Master userid is being shared..
Note: if there is only one Master level userid in the Scheduler Administrator’s User Report, it’s probably being shared. The same situation is possible if only a few userids are listed in the Scheduler Administrator’s User Report.

Fixes

Scheduler Master Shared

A primary and as many alternate Scheduler Master Level Userid as needed should be established and assigned to specific individuals in the scheduling office. Also, immediately after the new Scheduler Master Level Userids are created, the password to the original Scheduler Master Level userid will be changed.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.170.00 V0000594 CAT II Number of Master Lever Userids

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4

Vulnerability The number of Scheduler Master Level Userids exceeds the number allowed by the STIG.

Vulnerability Discussion Scheduler Master Level Userids have significant privileges within Scheduler and access to these userids must be strictly controlled.
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.

Checks

Scheduler Master Number of

The reviewer will generate a Scheduler Administrator’s User Report and review the report. Master level user-IDs contain ‘MS’. If there are more than four Master Level userids, the reviewer will verify that IAM has authorized this number of Master Level userids. If the number of Master Level userids exceeds four and the IAM has not authorized the number of Master Level userids that exist, this is a finding.

Fixes

Scheduler Master number of

Validate the users with Master Level Userids and ensure all Master Level Userids belong to site personnel and that there are no more than four Master Level Userids (including the default Master Userid) per domain or obtain authorization from the IAM for however many additional Master Level userids as are required.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.180.00 V0000647 CAT II Schedular Master Level Userid Access

8500.2 IA Control: IAIA-2, IAIA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4

Vulnerability Unauthorized personnel have access to Scheduler Master level Userids.

Vulnerability Discussion Scheduler Master Level users have the ability to accomplish any function within Scheduler. If Master Level Userids are not restricted to site personnel, unauthorized users can access any function within Scheduler, including adding and deleting users, and updating the master schedule.
The SA will ensure Master Level userids are restricted to authorized personnel.

Checks

Scheduler Master Access

The reviewer will interview the SA to verify that only authorized users are given access to Scheduler Master Level userids. If there is doubt about the users authorization, veify it using the SAAR or equivalent documentation.

Fixes

Scheduler Master Access

Restict access to the Scheduler Master Level Userids to personnel with appropiate authorization on their SAAR.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.184.00 V0003911 CAT II Scheduler, Scheduler Level userids

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4

Vulnerability Scheduler, Scheduler Level userids are not assigned to access codes in accordance with the Unisys STIG.

Vulnerability Discussion Establishing Scheduler Level userids with unauthorized Scheduler access codes gives users increased capabilities within the database, and could compromise the integrity of the database or allow unauthorized actions to be performed.
The SA will ensure the Scheduler Level userids are restricted to the access codes specified in this STIG and are restricted to authorized personnel.

Checks

Scheduler Level Access

The reviewer will review the Scheduler Administrator's User Report and verify that all SK level user-IDs are set up with the correct access codes. Authorized access codes are ALL-U, MAS-U, SDK-U, SAM-U, and SUP-U or ALL-U, MAS-U or MAS-I, SKD-I, SAM-U, and SUP-U.

Fixes

Scheduler Level Access

Ensure all authorized Scheduler Level users are set up in the Scheduler database with the access codes specified in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.190.00 V0002669 CAT II Unauthorized Secudler Level users

8500.2 IA Control: IAIA-2, IAIA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4

Vulnerability Unauthorized users can create a Scheduler daily production schedule.

Vulnerability Discussion Creation of a Scheduler production schedule initiates scheduled batch processing for a particular day. If the ability to create a production schedule is not restricted to select site personnel, unauthorized users could start a production batch schedule at an inappropriate time. This could impact the processing of an applications end of day or batch runs and result in a denial of service to the customer or a delay in the creation of critical reports.
The SA will ensure the Scheduler Level userids with the access code of SKD-U are restricted to authorized personnel.

Checks

Scheduler Level Authorization

The reviewer will interview review the Scheduler Administrator's User Report and see which users have the SKD-U access code. Is the SKD-U restricted to authorized personnel only? If there is a doubt as to the users authorization, check their SAAR. If there are unauthorize users then this is a finding.

Fixes

Scheduler Level Authorization

Restrict the ability to create a Scheduler daily production schedule to select authorized personnel.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.200.00 V0000595 CAT II Scheduler Master Userid's default

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.4

Vulnerability The initial Scheduler Master Userid's password is not changed from the default.

Vulnerability Discussion The initial Scheduler Master Userid has significant privileges in Scheduler and its default password is frequently known or easily discovered. If compromised, this userid could be used to execute privileged Scheduler commands or perform unauthorized updates to the Scheduler database.
The SA will ensure the default password for the initial Scheduler Master userid is changed immediately after implementation.

Checks

Master Level Default

The reviewer will sign on to demand, enter @SKDMNU, and try the default Scheduler userid/password. If the default Scheduler userid/password works then this is a finding. To find the default userid/password look in the element NEWSECECL

Fixes

Master Level Default

After Scheduler installation, change the default password for the initial Scheduler Master Userid.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.210.00 V0000630 CAT II Scheduler Non-Site Personnel

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.2.2

Vulnerability Non-Site personnel are not set up in the Scheduler database with OPERATOR or USER level userids.

Vulnerability Discussion Establishing non-site users with other Scheduler userid levels gives users increased capabilities within the database, and could compromise the integrity of the database or allow unauthorized actions to be performed.
The SA will ensure non-site personnel are set up in Scheduler with Operator or User Level access only.

Checks

Scheduler Non-Site Access

The reviewer will review the Scheduler Administrator’s User Report and verify all non-site users are assigned with an access level of OPERATOR or USER (OP or US) unless other access is authorized on the SAAR.

Fixes

Scheduler Non-Site Access

Establish each authorized functional user with OPERATOR or USER level userids only. OPERATOR level userids should only be given to high level functional personnel. If authorized on the SAAR these users can be granted higher level access.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.220.00 V0000631 CAT II Scheduler Functional user priviliges

8500.2 IA Control: ECLC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.1.4, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.2.2

Vulnerability Functional users are not set up in the Scheduler database with the access codes specified in the standard.

Vulnerability Discussion Establishing functional users with unauthorized Scheduler access codes gives users increased capabilities within the database, and could compromise the integrity of the database or allow unauthorized actions to be performed.
The SA will ensure userids assigned to functional users are restricted as described in the Unisys STIG.

Checks

Scheduler Functional User

The reviewer will review the Scheduler Administrator’s User Report and verify all functional users are assigned with the access codes listed in the Unisys STIG for OP and US level users. If an access code is not listed (ALL, SKD, SAM, MAS, or SUP), the default setting is Update for that access code.
OP level users will have ALL-U, MAS-I, SKD-I, SAM-U, and SUP-U.
US level users will have ALL-I, MAS-I, SKD-i, SAM-I, and
SUP-I

Fixes

Scheduler Functional Users

Ensure all authorized functional users are set up in the Scheduler database with the access codes specified in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.230.00 V0000632 CAT II Scheduler Non-Site User Department Restrictions

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.3.2.2

Vulnerability Functional users are not restricted to a specific department within the Scheduler database.

Vulnerability Discussion If functional users are not restricted to specific departments, they can access, alter, or add scheduling information for other sites or organizations. This can result in excessive or erroneous jobs being scheduled on the system and cause denial of service or compromise the integrity of another sites scheduling information.
The SA will ensure non-site Scheduler userids and User Level userids are restricted to a department.

Checks

Scheduler Department Restrict

The reviewer will review the Scheduler Administrator’s User Report and verify that all non-site users and all User Level userids have a department listed in their user-ID record and are restricted to this department (Y).

Fixes

Scheduler Department Restrict

Ensure each authorized functional user is restricted to a specific department.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.240.00 V0000596 CAT II The elements NEWSECECL and SAMCMDECL not secure

8500.2 IA Control: ECCD-1, ECCD-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.5

Vulnerability The elements NEWSECECL and SAMCMDECL are not secured.

Vulnerability Discussion Unauthorized individuals can use these runstreams to initialize Scheduler security or perform dangerous commands against the Scheduler database.
The SA will ensure the elements NEWSECECL and SAMCMDECL are moved to a side file and secured with a restricted ACR.

Checks

Scheduler Sensitive ECL

The reviewer will check the Scheduler installation files to verify that these elements are removed or that the file containing these elements is protected with a restrictive ACR that restricts read and write to authorized users. These two elements should be in an ACR protected side file (for example, SYS$LIB$*USAF-SECURE) or the SKDPRG file should be restricted with an ACR. The ACR should restrict access to site personnel only. The SRRPRT contains information for this checklist item.

Fixes

Scheduler Sensitive ECL

Secure these elements in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.250.00 V0000747 CAT II Scheduler CONS Mode

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 9.1

Vulnerability A CONS level other than DISPLAY is configured in Scheduler to allow SAM commands.

Vulnerability Discussion SAM keyins can be used to perform certain commands, such as initiating or terminating batch jobs, and must be tightly controlled.
The SA will ensure the CONS level in the Scheduler runstream is configured to DISPLAY.

Checks

Scheduler CONS Mode

The reviewer will perform a @PRT,s on <qualifier>*SKDPRG.SAMS-RUN/EC. If this CONS level is anything other than DISPLAY, the IAO should work with the Scheduler point of contact to resolve the problem. The SRRPRT contains a @PRT,S <qualifier>*SKDPRG.SAMS-RUN/ECL.

Fixes

Scheduler CONS Mode

Configure Scheduler to restrict SAM commands to DISPLAY CONS.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.260.00 V0000559 CAT II Securing IQU Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.3.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.3.2

Vulnerability Access to IQU is not restricted or user access is not documented.

Vulnerability Discussion IQU is an extremely powerful database utility that allows users to bypass many database security mechanisms.
The IAO will ensure access to IQU is restricted and user access is documented in accordance with this STIG requirement.

Checks

Securing IQU

The reviewer will verify that on the ALN and CAMS CDB systems run the account (ALN/AIS) secured version of IQU (SYS$LIB$*IQU). The reviewer can use the Toolkit Account Shred Report and identify those userids that are under a Y or Z shred account. The IAO should have documentation for all userids under these accounts.
The reviewer will verify on systems that do not run the account secured version of IQU, this file is secured with an ACR. The ACR can be restricted by account or userid. The IAO should have documentation for all userids with access to the ACR.
If documentation is not available for a userid or if there are an excessive number of users with access to IQU, this would be a finding. If the non-secured version of IQU is being used and the file is not protected with an ACR, this is a finding.

Fixes

Securing IQU

Secure IQU and document user access in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.270.00 V0000598 CAT II ALN Unauthorized DA1A Accounts

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.3.1

Vulnerability There are unauthorized (ALN) DA1A accounts in the account summary file (ALN Sites Only).

Vulnerability Discussion Access to (ALN)DA1A accounts allows a user to bypass internal IQU security controls and gives a user the capability to modify any functional application schema within a particular ALN.
The IAO will ensure the 0000DA1A account is the only authorized <ALN>DA1A account in the account summary file.

Checks

ALN Unauthorized DA1A accounts

The reviewer will check the account summary file and locate any <ALN>DA1A account. If the system has the secured version of IQU installed and there are any <ALN>DA1A accounts this is a finding.

For accounts not running the SSO Montgomery modified version of IQU, this vulnerability does not apply.

Fixes

ALN Unauthorized DA1A Accounts

Remove all unauthorized (ALN)DA1A accounts from the account summary file.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.276.00 V0003912 CAT II Normal QLP & QLP with update exists on the system

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.2.1

Vulnerability Normal QLP and QLP with update exists on the system.

Vulnerability Discussion Normal QLP, Unisys Released version of QLP with no local code, allows unrestricted update to database files. If it is on the same system with QLP with Update, which has local code to restrict database update to specific users, it defeats the purpose of QLP with update. This can lead to logical database corruption and loss of data.
For DISA sites, The SA will ensure QLP with Update is not being combined with the standard QLP software product.

Checks

QLP and QLP with Update

The reviewer will verify that for sites running the QLP for updated modifications written by SSO Montgomery that the released SYS$LIB$*QLP file contains the Inquiry only version of QLP. The reviewer will check with SSO Montgomery to verify the version date of this QLP absolute if necessary. The reviewer will check to make sure unauthorized versions of QLP are not copied into side files since these absolutes may support the update version of QLP.

For sites not running the SSO Montgomery modifications to QLP this vulnerability does not apply.

Fixes

QLP and QLP with Update

Remove normal QLP from the system.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.280.00 V0000597 CAT II QLP with Update Access Restrictions

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.2.1

Vulnerability Access to QLP with Update is not restricted and user access is not documented as specified in the standard.

Vulnerability Discussion QLP with Update is an extremely powerful database utility that allows users to bypass many database security mechanisms.
For DISA sites, The IAO will ensure access to QLP with Update is restricted and user access is documented in accordance with this STIG requirement.

Checks

Securing Access QLP Update

For sites using the SSO Montgomery modified QLP with Update.
The reviewer will check the QLP with Update file to verify that it is restricted with an ACR. The reviewer can do an @PRT,F UDS$$SRC*QLP-UPDATE to see what ACR is attached. The reviewer will then look at the Toolkit ACR Restrictions Report and see what restrictions are applied to this ACR. ALN and CAMS CDB systems will restrict user access with an X shred account. The reviewer will check the Toolkit Account Shred Report and identify any userid under an X shred account. The IAO should have documentation for all userids under these accounts. This documentation should have the appropriate cross-coordination.

For DNMC and DFAS systems, the ACR restriction can be by account or userid. Documentation should be available as specified by the Unisys STIG.

If documentation is not available for a userid, if the documentation does not contain the proper cross-coordination, or if there are an excessive number of users with access to QLP with Update, this is a finding. If the QLP with Update file is not protected with an ACR, this is a finding.

For sites that do not use the SSO Montgomery Modified QLP with Update this vulnerability is not applicable.

Fixes

Securing Access QLP Update

Secure QLP with Update and document user access in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.290.00 V0000648 CAT II Unauthorized versions of DBE exist on the system

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1

Vulnerability Unauthorized versions of DBE exist on the system.

Vulnerability Discussion Specific security features are implemented in the DBE software to ensure access to this database editor is restricted to authorized users. If unknown or unauthorized versions of DBE exist on the system, then these security features may not be properly implemented. Users could gain unauthorized access to DBE and use this utility to modify or manipulate application databases. Improper or malicious updates can result in corrupted database files or compromised database integrity.
For DISA sites, the SA will ensure only the authorized version of DBE version released by SSO Montgomery is used.

Checks

Unauthorized DBE

For Sites running the SSO Montgomery modified DBE.
The reviewer will look at the Toolkit DBE/QLP Report to determine what DBE files are on the system. Authorized versions should be in DMS$0000*DBE or DMS*DBE. The reviewer can contact the DBE AIS manager if necessary to determine the current released version of DBE. The reviewer will execute the DBE processor to verify the version (DMS$0000*DBE.DBE or DMS*DBE.DBE). If it is not the current SSO Montgomery released version of DBE or if there are other unauthorized DBE files on the system, this is a finding.

For sites not running the SSO Montgomery modified version of DBE this vulnerability does not apply.

Fixes

Unauthorized DBE

Ensure only authorized versions of DBE exist on the system. For DISA Computing Services sites, SSO Montgomery is the only authorized releaser of DBE software.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.300.00 V0002670 CAT II DBE Source Restriction

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1

Vulnerability There are unauthorized DBE source files on the system.

Vulnerability Discussion DBE source files allow a user to perform a DBE software generation. If unauthorized DBE source files are on a system, a user could perform a DBE software generation without the proper security mechanisms in place.
For DISA sites, the SA will ensure the DBE source files are only available on SSO Montgomery development systems.

Checks

DBE Source Restriction

For DISA systems using SSO Montgomery modified DBE:
The reviewer will look at the Toolkit DBE/QLP Report to determine what DBE files are on the system. If there are (<DBE qualifier>*F1 through F5 or <DBE qualifier>*File1 through File5) files on the report, this is a finding.

For systems not useing SSO Montgomery Developed DBE this vulnerability is not applicable.

Fixes

DBE Source Restriction

Remove unauthorized DBE source files from the system.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.310.00 V0000749 CAT II DBE security is not implemented

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.1

Vulnerability DBE security is not implemented.

Vulnerability Discussion DBE is a database editor that can circumvent system security mechanisms at the database level.
The SA will ensure sites using DBE implement DBE security.

Checks

Securing DBE

The reviewer will verify this by looking at the Toolkit DBE/QLP Report for any DBESEC or DBE$SEC combinations. If this file is not listed on the report, the reviewer can try to execute DMS$0000*DBE.DBE or DMS*DBE.DBE. If DBE security is implemented and the DBE$SEC file is deleted, you will get a facility error 400010000000. If DBE security is not implemented, this is a finding.

Fixes

Securing DBE

Implement DBE security in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.310.10 V0006456 CAT II DBE with Normal Security User Access Documentation

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.1

Vulnerability User access to DBE with normal security is not documented as required in the STIG.

Vulnerability Discussion 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. Since this access is not limited by the software userids with access need to have their access requirements recertified yearly so that users whose duties no longer require this access can have the access removed.
The IAO will ensure User access is documented in accordance with the STIG requirements.

Checks

Normal DBE Update Access

The reviewer will interview the IAO to verify that all users that have update access to normal DBE have the need for update access annually reviewed and documented.

Fixes

Normal DBE Update Access

Review and recertify the DBE with Normal Security update access requirements for all users that have update access. Remove any userid owned by a user who no longer requires update access to DBE with Normal Security or if the requirement cannot be recertified.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.320.00 V0000599 CAT II DBE Access Restriction Schema Enhanced

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.2

Vulnerability Access to DBE is not restricted and user access is not documented as specified in the standard.

Vulnerability Discussion DBE is a powerful database editor and if access is not strictly controlled, unauthorized personnel can use this utility to modify or manipulate application databases. Improper or malicious updates can result in corrupted database files or compromised database integrity. 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 requirement.

Checks

DBE Access Restriction ALN

For ALN and CAMS CDB systems,
The reviewer will look at the contents of the DBE$SEC file. If the 0000JX1A account is entered in this file, the Toolkit will produce a DBE file (SRRDBE). If this file is empty, the reviewer can manually obtain a listing of this file. In this file the reviewer will locate all accounts with a U option. Update access (U option) should be restricted to ‘Z’ shred accounts. The IAO should look at the Toolkit Account Shred Report and identify all userids under a Z shred account. The IAO should have documentation for all userids under these accounts.
On DNMC and DFAS-IN systems, the version of DBE is restricted by userid rather than by account (except batch DBE, which is still controlled by account). The IAO should have documentation for all userids in these DBE$SEC files. If documentation is not available for a userid or if there are an excessive number of users with access to DBE, this is a finding.

For sites that do not run the SSO Montgomery modified DBE this vulnerability is not applicable.

Fixes

DBE Access Restriction ALN

Restrict access to DBE and ensure user access is documented in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.330.00 V0000649 CAT II DBE Master userid Access Restricted

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.1.2

Vulnerability Access to DBE Master userids are not restricted to the Security Officer and SIMAN Administrator userids (Normal DBE Only).

Vulnerability Discussion DBE is a powerful database editor and if access to the DBE Master userids is not strictly controlled, unauthorized personnel could update the DBE security file with erroneous information that could compromise or invalidate the DBE security mechanisms in place. The SA will ensure access to the DBE Master userids are restricted to the Security Officer and SIMAN Administrator userids.

Checks

DBE Master Userid Restriction

aaa

DBE Master Userid Restriction

aaa

DBE Master Userid Restriction

aaa

Fixes

DBE Master Userid Restriction

Restrict access to DBE Master userids to the Security Officer and SIMAN Administrator userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.340.00 V0000650 CAT II The DBEGEN userid is not disabled

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.1.1

Vulnerability The DBEGEN userid is not disabled and the run modes are not removed (Normal DBE Only).

Vulnerability Discussion The DBEGEN useridis the default installation userid for normal DBE security and if compromised, this userid could be used to add unauthorized users to the DBE security file. If unauthorized users gain access to DBE, they can use this utility to modify or manipulate application databases. Improper or malicious updates can result in corrupted database files or compromised database integrity.
The SA will ensure following the initial installation of normal DBE with userid security, the DBEGEN userid is disabled with no run modes.

Checks

DBEGEN Userid Deactivated

On systems not using the SSO Montgomery Modified DBE.
The reviewer will check the Toolkit SRRALL file and search for the DBEGEN user-ID. If the user-ID is found, the IAO should ensure this userid is disabled with no run modes. Alternately the reviewer can locate the userid in SIMAN and verify its settings. If it is not disabled or if it has TIP, batch or demand mode is enabled, this is a finding.

Fixes

DBEGEN Userid Disabled

Following the initial installation of DBE, the IAO should disable the DBEGEN user-ID and remove all run modes so unauthorized users can not use this user-ID.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.350.00 V0000651 CAT II Unatuthorized DBEGEN account exists

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.2.1.2

Vulnerability The unauthorized DBEGEN account exists in the account summary file. (DBE With Enhanced Schema Security Only)

Vulnerability Discussion The DBEGEN account is the default installation account for DBE with enhanced schema security, and if left in the account summary file, it could be used to add unauthorized users to the DBE security file. If unauthorized users gain access to DBE, they can use this utility to modify or manipulate application databases. Improper or malicious updates can result in corrupted database files or compromised database integrity.
The IAO will ensure the default DBE installation account (DBEGEN) is not be active in the account file.

Checks

DBEGEN Account restriction

On systems using the SSO Montgomery modified DBE.
The reviewer will check the account summary file (SRRACT) and search for this account. An alternate verifying this is to use SIMAN to display the DBEGEN account. If DBEGEN is in the account summary file, this is a finding..

Fixes

DBEGEN Account Restriction

Remove the DBEGEN account from the account summary file.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.360.00 V0000600 CAT II DBE Unauthorized (ALN)DA1A Account in DBE$SEC

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.2.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.2.2

Vulnerability The DBE$SEC file contains unauthorized (ALN)DA1A accounts. (DBE With Enhanced Schema Security Only)

Vulnerability Discussion DBE with enhanced schema security uses account information in the DBE$SEC file to limit update mode to a particular functional application database within an ALN. Inserting (ALN)DA1A accounts in the DBE$SEC file bypasses this enhanced schema security and allows a user to update any functional database within an ALN. Improper or malicious updates can result in corrupted database files or compromised database integrity.
For DISA sites, the IAO will ensure sites using DBE with Enhanced Schema Security use account 0000DA1A as the DBE Master Account.

Checks

DBE DA1A account restrictions

For systems using the SSO Montgomery modified DBE.
The reviewer will look at the contents of the DBE$SEC file. If the 0000JX1A account is entered in this file, the Toolkit will produce a DBE file (SRRDBE). If not, the IAO can manually produce a listing of this file. The IAO should verify that there are no <ALN>DA1A accounts, other than 0000DA1A, in this file (especially with the ‘U’ option). If there are any <ALN>DA1A accounts in the DBE$SEC file, this is a finding.

Fixes

DBE DA1A Account Restriction

Delete unauthorized (ALN)DA1A accounts from the DBE$SEC file.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.370.00 V0000633 CAT II DBE Master Account Restriction DBE Enhanced

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.1.2.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.3.1

Vulnerability Access to the DBE Master Account is not restricted to the Security Officers userid. (DBE With Enhanced Schema Security Only)

Vulnerability Discussion DBE is a powerful database editor and if access to the DBE Master Account, 0000DA1A, is not strictly controlled, unauthorized personnel could update the DBE security file with erroneous information that could compromise or invalidate the DBE security mechanisms in place.
For DISA sites, the IAO will ensure access to the DBE Master Account is restricted to the Security Officer and SIMAN Administrators.

Checks

Unisys S103.370.00

On systems not using the SSO Montgomery modified DBE.
The reviewer will review the contents of the DBE$SEC file. A DBE Master userid is indicated by the M option in the DBE$SEC file. If a userid is listed in the DBE$SEC file with the M option and this userid is not a Security Officer or a SIMAN Administrator, this is a finding.

For systems using the SSO Montgomery Modified DBE in an ALN or CAMS DBS environment.
The reviewer will look at the contents of the account summary file (SRRACT) and search for the 0000DA1A account. The reviewer will compare all userids under this account against the Toolkit Administrators Report. If these userids are not the Security Officer or SIMAN Administrator userids, this is a finding.

Fixes

Restrict access to the DBE Mas

Restrict access to the DBE Master Account to the Security Officer and SIMAN Administrator userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.380.00 V0000652 CAT I UREP Access Control

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.6

Vulnerability Unauthorized users have execute rights in the Universal Repository (UREP) Security Access Control List.

Vulnerability Discussion The UREP Security Access Control List (ACL) is used to control all UREP security-related commands. If users have execute rights in the Security ACL, they assume capabilities as UREP security officers, and can grant or deny other users unauthorized access to UREP database files, application schemas and files, RDMS views and tables, and other database functions and attributes.
The SA will ensure the Security Officer or SIMAN Administrator are the only userid allowed execute rights in the UREP Security Access Control List.

Checks

UREP Access Restriction

The reviewer will sign on to demand and do the following for each application group running on the system. Application groups are listed in the Unisys STIG, Paragraph 5.6.1.

```
@DD,DE ,,<application group name>
REPORT SECURITY OFFICERS.
@EOF
```

The reviewer will verify that the userid(s) listed are the Security Officer or SIMAN Administrators. If they are not, this is a finding.
If DMS, RDMS, or SF1100 are not being used this vulnerability is not applicable.

Fixes

UREP Access Restriction

Restrict execute rights in the UREP Security ACL to the Security Officer or SIMAN Administrator userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.380.10 V0006466 CAT II UREP Configuration Functions

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.6.4

Vulnerability User Groups are n ot being used to control access to the configuration functions of UREP.

Vulnerability Discussion By default the configurations functions are granted to ALL-USERS. If this is not restricted a unauthorized users could drop a schema definition creating a denial of service condition.
The SA will ensure user groups are used to control access to the configuration functions of UREP.

Checks

UREP Configuration Access

The reviewer will verify that only authorized userids are allowed to perform the UREP configuration functions.
The reviewer will execute the following.

```
  @DD,DE
   REPORT SECURITY OFFICERS.
   @EOF
```

Then the reviewer, with the assistance of the user who owns one of the above userids, will sign on to demand with that userid and execute the following.

```
 @DD,DE ,,<application group name>
         . Such as APPL01 or DMRP1
 ENTER SECURITY MODE.
 GET ACL FOR STATIC-CONTEXT
        PROCESS-CONFIGURATION.
 REPORT ACL.
 RETURN ACL.
 GET ACL FOR CONFIGURATION ALN.
         .  Replace with correct config
 REPORT ACL.
 RETURN ACL.
 LEAVE SECURITY MODE.
 EXIT.
```

Check the output.
For the ACL for STATIC-CONTEXT PROCESS-CONFIGURATION only authorized userids will have the EXECUTE right. Make note of all USER-GROUPs that have grant of EXECUTE right.

For ACL for CONFIGURATION ALN (corrected for the running configuration name) the following: APPEND-LINKS, CONTROL-DISCRETIONARY, CREATE, DELETE, and EXECUTE rights will be granted to authorized users. Make note of all USER-GROUPs granted any of these rights.
Using each of the USER-GROUP found above the reviewer will execute the following commands to list the members of the USER-GROUP. Only authorized userids will be members of these groups.

```
 @DD,DE
 ENTER SECURITY MODE.
 REPORT IMPACT USER-GROUP usergroupname.
 LEAVE SECURITY MODE.
```

If the user group ALL-USERS has the restricted rights or if any userid or user group member userid is not authorized to have access to the restricted rights and do not have this access documented in each user’s SAAR, this is a finding.

NOTE: There is no need to do an Impact report on the user-group ALL-USERS.

Fixes

UREP Configuration Access

Deny access for any unauthorized userid to restricted rights within the appropriate ACL, or, revoke any unauthorized userids membership in a USER-GROUPs that have access to the restricted rights within the appropriate ACL.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.390.00 V0000634 CAT II EZLOAD Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 6.2.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 6.2.2

Vulnerability Users have access to the EZLOAD processor without proper justification and documentation.

Vulnerability Discussion The EZLOAD processor provides access into the File Administration System based EZLOAD database and allows users to reload specific files. Improper or malicious use could result in corrupted files or unauthorized access to customer files.
The IAO will ensure users do not have access to the EZLOAD processor without proper justification and documentation.

Checks

EZLOAD Access

The reviewer will sign on to demand and perform a @EZLOAD ACCESS. The reviewer will select Option 5 to list the userids with EZLOAD access and print the resulting userid screen. The IAO should have documentation for all users with EZLOAD access. If the number of non-site users is excessive or if userids are not documented, this is a finding.

IF EZLOAD is not used this vulnerability is not applicable.

Fixes

EZLOAD Access

Ensure all user access to EZLOAD is properly justified and documented in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.400.00 V0000601 CAT II The MAPPER registration RID Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.1

Vulnerability The MAPPER registration RID and MAPPER system information files are not secured from access by unauthorized personnel.

Vulnerability Discussion The MAPPER registration RID and MAPPER system information files contain sensitive information and identification and authentication data. If unauthorized users access these files, userid and other sensitive information may be compromised or altered.
The SA will ensure the MAPPER registration RID and MAPPER system information file are secured with an ACR to protect them from unauthorized access.

Checks

MAPPER registration RID ACCESS

The reviewer will sign on to the system in demand, go into CONS, and do a T,B D. Then the reviewer will identify all the MAPPERs that are running on the system. The reviewer will do an RC on each MAPPER to find out what project-ID (Qualifier), account, and userid they are started with. If this is an ALN system, check the <MAPPER Qualifier>*M00001 and <MAPPER Qualifier>*M00002 files to make sure they are ACR protected and exclusively assigned (X-use). If the reviewer is using the SRRPRT run, the reviewer will update the runstream to reflect the correct qualifiers. For non-ALN systems, the file names that should be ACR protected and exclusively assigned are MAPER1 and MAPER2. If these files are not ACR protected and exclusively assigned, this is a finding.

NOTE: These files are only exclusively assigned when the particular MAPPER is online.

Fixes

MAPPER File access

Secure these MAPPER files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.402.00 V0003930 CAT II The HLDMAP, MAPER0, and MUPER files are not being

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.1

Vulnerability The HLDMAP, MAPER0, and MUPER files are not being secured in accordance with the Unisys STIG.

Vulnerability Discussion The HLDMAP file contains MAPPER configuration information that if modified can remove all internal security within the MAPPER software. The MAPER0 and MUPER files are working cache files used by MAPPER and may contain sensitive user data. Failure to secure these files from unauthorized access can lead to the release of sensitive information.
The SA will ensure HLDMAP MAPER0, MUPER1, and MUPER2 are secured with an ACR to protect them from unauthorized access.

Checks

MAPPER System File Access

The reviewer will verify that the required files are protected by an ACR that restricts access to the files. The files are normally <MAPPER Qualifier>*HLDMAP, <MAPPER Qualifier>*MAPER0, <MAPPER Qualifier>*MUPER1, and, <MAPPER Qualifier>*MUPER2. The IAO can add these particular files to the SRRPRT or the reviewer can manually check the Toolkit SRRFSM file for the presence of the ACR. If these files are not ACR protected, this is a finding.

Fixes

MAPPER File access

Secure these MAPPER files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.404.00 V0003931 CAT II All MAPPER database files are not being secured in

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.1

Vulnerability All MAPPER database files are not being secured in accordance with the Unisys STIG.

Vulnerability Discussion MAPPER database files contain data in ASCII clear text. If the files containing the MAPPER databases are not secured to prevent unauthorized access when MAPPER is not active; they are vulnerable to being read and/or modified by unauthorized users. This can lead to the compromising or corruption of sensitive data.
The SA will ensure all other MAPPER database files are secured with an ACR to protect them from unauthorized access.

Checks

MAPPER Database Access

The reviewer will verify that the MAPPER database files are protected with an appropriate ACR. If the IAO has added these particular files to the SRRPRT the reviewer can check the output from the run or the reviewer will manually check the SRRFSM for the presence of ACRs on the MAPPER files. The reviewer will also go into the <MAPPER Qualifier>*HLDMAP.MAPPER/PARAMETERS file and do a locate on FIL and DEV, but the files listed may not be a complete list. If there are MAPPER files that are not ACR protected, this is a finding.

Fixes

MAPPER File access

Secure these MAPPER files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.410.00 V0000602 CAT II MAPPER Security Parameters

8500.2 IA Control: ECSC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.2

Vulnerability The security related MAPPER parameters are not set in accordance with the standard.

Vulnerability Discussion Security related MAPPER parameters must be set correctly to ensure that MAPPER userid attributes comply with DISA security requirements. If these parameters are set incorrectly, there is a greater vulnerability for exposure and compromise, and unauthorized users may gain access to critical MAPPER applications.
The SA will ensure the MAPPER parameter PSWSIX is set to a value of 1.
The SA will ensure the MAPPER parameter SECCHG is set to a value of 90D or 3.
The SA will ensure the MAPPER parameter SECTIM is set to a value of 180 or less.
The SA will ensure the MAPPER parameter SECTRY is set to a value of 3.

Checks

MAPPER Security Parameters

Using the information obtained in S103.400.00, the reviewer will go into the <MAPPER Qualifier>*HLDMAP.MAPPER/PARAMETER element and locate each particular parameter to verify that it is set correctly.
Settings should be:
PSWSIX=1
SECCHG=3 or 90D
SECTIM=180 or less (but not zero)
SECTRY=3.
This information is also available in the SRRPRT. If these parameters are not properly set, this is a finding.

Fixes

MAPPER Security Parameters

Set the security related MAPPER parameters to the values specified in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.420.00 V0000603 CAT II MAPPER Batch Run Account

8500.2 IA Control: ECLP-1

References:

Vulnerability The MAPPER batch run is not started with a non-exempt account and project-ID. (ALN Sites Only)

Vulnerability Discussion If the MAPPER batch run is started with an exempt account or project-ID, MAPPER users can assume the attributes of the batch run and bypass many of the security mechanisms on the system.
The IAO will ensure MAPPER is started with a non-exempt project-ID and non-exempt account.

Checks

MAPPER Batch Run Account

Using the information obtained in S103.400.00, the reviewer will verify that each MAPPER run is being started with a non-exempt account and project-ID. If the MAPPER run does not reflect an authorized non-exempt account and project-ID, this is a finding.

Fixes

MAPPER Batch Run Account

Update operating procedures or the Scheduler database so the MAPPER batch run is started with a non-exempt account and project-ID.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.430.00 V0000604 CAT II MAPPER batch Run Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.3

Vulnerability The MAPPER batch run is not started with a userid that is restricted to non-exempt accounts and project-IDs. (ALN Sites Only)

Vulnerability Discussion If the MAPPER batch run is started with a userid that is not restricted to a specific non-exempt account and project-ID, MAPPER users can start batch jobs with these unauthorized accounts and project-IDs and bypass system security mechanisms.
The SA will ensure each MAPPER userid is set up with the userid attributes specified in this STIG and does not have access to non-exempt accounts or project-IDs.

Checks

MAPPER Batch Userid

Using the information obtained from S103.400.00, the reviewer will check the userid that is used to start the MAPPER run. The reviewer can look at the userid in the Toolkit SRRALL file and verify that it only has access to its authorized non-exempt project-ID and account. Also, the reviewer will check the account summary file (SRRACT) to see what accounts this userid can acces. It should only have access to its authorized non-exempt account. If the user-ID has access to any exempt accounts/project-IDs or access to any unauthorized non-exempt accounts/project-IDs, this is a finding.

NOTE: CBAS MAPPERs are authorized access to both the DB and T0 accounts and project-IDs.

Fixes

MAPPER Batch Userid

Ensure the userid used to start the MAPPER batch run is project-ID restricted, can not enter a project-ID or account, and is limited to a specific non-exempt project-ID and account.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.434.00 V0003932 CAT IV MAPPER File Creation

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.6.4

Vulnerability The runstreams that create MAPPER files do not secure them in accordance with the Unisys STIG.

Vulnerability Discussion If the MAPPER system files and database files are not created with the proper access restrictions they will be vulnerable to compromise or corruption of the data they contain. Though this could be done at a later time, it is better to create them initially with the proper access controls.
The SA will ensure runstreams creating MAPPER files attach appropriate ACRs to the created files.

Checks

MAPPER File Creation

The reviewer will review each runstream used by the site to ensure they properly secure all MAPPER files with an appropriate ACR attached. If these runstreams do not secure the MAPPER files, this is a finding. The MAPPER runstreams should be in SYS$LIB$*RUN$. but they may be located elsewhere, check with the IAO to verify the location of these runstreams. On SSO Montgomery supported systems, these runstreams should be MAPPER, PRESTR, PRESTR/FILE, and PRESTR/TAPE, but there may be others.

Fixes

MAPPER File Creation

Correct the runstreams that create MAPPER files so that the files are created with the proper access controls in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.440.00 V0000653 CAT II DPS Password Functions Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.9.3

Vulnerability Unauthorized users have access to Password Functions in the Display Processing System (DPS).

Vulnerability Discussion The DPS password file controls the maintenance of DPS userid information and application screen files. If unauthorized users have access to DPS Password Functions, they can add/delete other users in the DPS password file and grant users unauthorized access to DPS Password Functions. In addition, users with access to DPS Password Functions can view clear text passwords for any user in the DPS password file and can potentially change this password without the users knowledge.

In the DNMC environment, the DPS password file is also used to control logon access into the DNMC COMPOOL applications. If unauthorized DNMC users have access to DPS Password Functions, they can add/delete other user-IDs and grant users unauthorized access to DPS Password Functions or DNMC COMPOOL applications. DNMC users with access to DPS Password Functions can view clear text passwords for any user in the DPS password file and can potentially change this password without the users knowledge or logon to a DNMC COMPOOL application with another users userid and password.
The SA will ensure only documented authorized personnel have access to Password Functions in the Display Processing System.

Checks

DPS Password Functions

The reviewer will use the SRRDPS runstream to gather information for this finding.
For ALN systems, the SRRDPS should be run against ALN 0000 and each ALN that has a TCB file #247.
For non-ALN systems, the reviewer will check the Toolkit SRRCOM file to verify what DPS products are installed. The reviewer will then run the appropriate LISTER absolute for each DPS installed. Download the output for each run and process them though the SRRDPS macro. Next the reviewer will review the Excel spreadsheet to ensure all users have access to Password Functions (Indicated with a Y) have the appropriate documentation for access in the SAAR. If users have access to Password Functions and there is no documentation, this is a finding.

Fixes

DPS Password Functions

Review the DPS password file and ensure only authorized personnel have access to DPS Password Functions. Remove the DPS Password Function form any user who does not have a documented need.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.450.00 V0000654 CAT II DPS Forms Libraries Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.9.3

Vulnerability Unauthorized users have access to all Form Libraries in DPS.

Vulnerability Discussion The DPS password file controls the maintenance of userid information and application screen files. If unauthorized users have access to all Form Libraries, they can make improper or malicious updates to any screen file on the system, which can lead to corrupted database files or compromised database integrity.
The SA will ensure only documented authorized personnel have access to all Form Libraries in the Display Processing System.

Checks

DPS Forms Libraries

The reviewer will check the Excel spreadsheet from S103.440.00 to ensure only users have access to all Form Libraries who's need is documented on the SAAR. If users have access to all Form Libraries and there is no documentation, this is a finding.

Fixes

DPS Forms Libraries

Review the DPS password file and ensure only authorized personnel have access to all Form Libraries.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.460.00 V0000655 CAT II DPS Functional user access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.9.3

Vulnerability Functional user access to DPS is not limited to selected, high-level functional users.

Vulnerability Discussion The DPS password file controls the maintenance of userid information and application screen files. If functional users have uncontrolled access to their application screen files, unauthorized users could make improper or malicious updates, which can lead to corrupted database files or compromised database integrity.
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.

Checks

DPS Functional User

The reviewer will check the Excel spreadsheet from S103.440.00 to ensure only select, high level functional users have access to DPS and that they are restricted to the minimum DPS privileges needed to load their application screens or perform DPS programming tasks. The reviewer will verify that the Form Library belongs to that particular application. If there are an excessive number of functional users with access to DPS, if a functional user has unauthorized DPS privileges, if a functional user has access to another application’s Form Library, or if the access is not documented on the SAAR, this is a finding.

Fixes

DPS Functional Users

Review the DPS password file and ensure only authorized select, high-level functional users have access to their respective application screen file and that the need for access is documented.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.470.00 V0000656 CAT I DPS Password Requirements

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.9.3

Vulnerability Users are using their SIMAN password as their DPS password.

Vulnerability Discussion The DPS processor has a password database, making passwords available for viewing by a privileged user or any user with access to DPS Password Functions. If a user utilizes their SIMAN password as their DPS password, the risk of their SIMAN password being compromised is increased and an unauthorized user could use this password to gain access to the system.
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.

Checks

DPS Passwords

The reviewer, using the Excel spreadsheet from S103.440, will dump the userids/passwords into a comma delimited text file. Then the reviewer will use the Infoconnect CASL Macro HLC or DCP script to sign onto the system with the individual's DPS userid and password. The will review the output from this macro to ensure none of the sign on attempts were successful. If there is a successful sign on, this is a finding. This check can be manually made if the Infoconnect macro is not available by selecting a few random userids and password pairs and manually trying to sign on with them.

NOTE: Take care when running the CASL Macro to ensure active user-IDs are not disabled. Also, if the DPS password does not match the criteria for a valid SIMAN password, that particular user-ID/password combination could be eliminated. For example, if a user-ID has signed onto the system, a DPS password of A would not be valid for a SIMAN password. If a DPS password is the same as the userid and the userid has signed onto the system, this DPS password would not be valid for a SIMAN password.

Fixes

DPS Passwords

Advise users of the risks associated with using their SIMAN password as their DPS password since the DPS password file can be viewed by privileged users. Instruct users to use a password other than their SIMAN password for their DPS password to avoid a compromise of their SIMAN userid.

Since with TIP Session control on and Demand access passwords controlled, the DPS password has no use. It is recommended that it be set initiallly to a value that is easily checked but cannot be a SIMAN password because of its length. An example would be "NONE", this cannot be a SIMAN password since it is not long enough.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.480.00 V0000554 CAT II Unauthorized users have access to Master Account

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.3

Vulnerability Unauthorized users have access to the Master Account or the SSMASTERACCT privilege.

Vulnerability Discussion There is a local code change that can be applied to the operating system that allows SIMAN Administrators to perform account maintenance functions if they have access to the Master Account. Unauthorized users with access to the Master Account can potentially assign unauthorized accounts to a user and allow this user to bypass ALN boundaries, gain access to privileged system processors and ACRs, or create erroneous fee for service billing information. Additionally, in CP2200 7.0 and above the SSMASTERACCT privilege gives a userid the ability to update account entries.
The SA will ensure only the Master userid and security administrators has access to the Master account or the SSMASTERACCT privilege.

Checks

Master Account Access

The reviewer will check the system level.

For sites all supported OS levels.
The IAO should be aware of what the Master Account is. Usually, this account is listed in the SRRALL under the Security Officer’s userid. When reviewer has this information, the reviewer can inspect the account summary file (SRRACT) and locate all userids under this account. The reviewer will compare this list against the Toolkit Administrators Report verifying that only the Security Officer and SIMAN Administrators are under this Master Account.

On HMP IX 7.0 and higher systems, the reviewer will also run the SSO Montgomery provided SQL query FIND-PRV-ALL to locate those users with the SSMASTERACCT privilege. The reviewer wile update this query to select ~ZD. If non-administrator userids have this privilege this is a finding.

Fixes

Master Account Access

Remove unauthorized users from the Master Account and/or remove the SSMASTERACCT privlege from the userid.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.490.00 V0002671 CAT I SIMAN Environment Update Restrictions

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.3.2

Vulnerability Unauthorized users can update the SIMAN environment.

Vulnerability Discussion Users who can update the SIMAN environment can deactivate critical security parameters within SIMAN, including the extended security parameter. Deactivating certain SIMAN parameters allows users to bypass discretionary access controls on the system and could jeopardize the entire security environment.
The SA will ensure only the Master userid and SIMAN administrator userids are allowed to update the SIMAN environment.

Checks

SIMAN Environment Update

The reviewer will manually inspect the SRRALL and identify any userid that has ‘Siman Environment Parameters’ listed in their userid record. An alternate way to perform this check is for the reviewer to run the SSO Montgomery provided SQL query SIMAN-ENV to identify any userid that has ‘Siman Environment Parameters’ listed in their userid record. Only the Security Officer and SIMAN Administrators should have this capability. If non-SIMAN Administrators have this capability, this is a finding.

Fixes

SIMAN Environment Update

Ensure that only the Security Officer and SIMAN Administrator userids have the ability to update the SIMAN environment.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.500.00 V0000723 CAT I Pre-installed Software Userids Deactivated

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.3

Vulnerability There are standard, pre-installed software userids on the system that are not secured properly.

Vulnerability Discussion Standard system userids and default passwords are commonly known and can provide a means of unauthorized access.
The IAO will ensure standard, pre-installed userids on the system are secured properly.

Checks

Default Userids

The reviewer will review the Toolkit Dormant (All) Report. If there are system type userids on this report, such as DPS, DPSSYS, Fixed Gate Subsystem Userids, STAR, etc., the reviewer will try to sign on with the default password (or an easily guessed password). If the reviewer can sign on to the system all the way, this is a finding. If the reviewer fails to sign on for not having a valid account or any reason other than invalid userid/password, is a finding.
This finding should not apply to normal end-user userids since they are not considered default or standard, pre-installed software userids.

Fixes

Default Userids

Change the password from the default and ensure the userid has the minimum access required to accomplish its functions.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.510.00 V0000744 CAT II The System Environment Tape Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.4.2

Vulnerability The system environment allows personnel to access or modify tapes outside of their application group.

Vulnerability Discussion If users can access or modify tapes without proper authorization, system integrity could be compromised.
The SA will ensure the tape management system environment does not allow personnel to access or modify tapes outside of their application group.

Checks

Tape Access System Environment

The reviewer will verify this by checking the BYPASS value in the STAR Page Zero. This information is available in the SRRPRT. Otherwise, the reviewer will go privileged and execute SYS$LIB$*STAR.STRUTIL. Perform a FUNC=DPGZER.
The BYPASS field should be decimal 12 for ALN and DFAS-IN systems.
The BYPASS field will be a decimal 4 (octal 004) or decimal 12 (octal 014) for DNMC systems.
If these values are incorrect, this is a finding.

Fixes

Tape Access System Environment

Restrict users to tapes within their own application group by setting the BYPASS field in the STAR Page Zero to the value specified in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.510.10 V0006488 CAT II STAR BYPASS Non-DISA systems

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.4.2

Vulnerability The STAR BYPASS value for non-DISA sites is not set to octal 004 (decimal 4).

Vulnerability Discussion By setting the STAR BYPASS value to octal 004, tape bypass is controlled by the userid privileges SSMMGRILES1, SSMMGRILES2, SMMGRILES3, and SSMMGRBYPASS. This removes operations from the process of verifying and granting tape security override functions lessening the chance of human error
The SA will ensure the STAR BYPASS value on non DISA systems is set to octal 004 (decimal 4).

Checks

Unisys STAR Bypass

The reviewer will verify this by checking the BYPASS value in the STAR Page Zero. This information is available in the SRRPRT. Otherwise, the reviewer will go privileged and execute SYS$LIB$*STAR.STRUTIL. Perform a FUNC=DPGZER. The BYPASS field should be decimal 4. If this value is incorrect, this is a finding.

Fixes

Tape Access System Environment

Restrict users to tapes within their own application group by setting the BYPASS field in the STAR Page Zero to the value specified in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.520.00 V0000657 CAT II CSC Configuration

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.4.2

Vulnerability The Client System Component (CSC) parameter element is not set up in accordance with the standard.

Vulnerability Discussion The CSC parameter element contains settings, which limit the CSC commands that can be executed from a demand terminal. If these parameters are not set correctly, unauthorized users may be allowed to interface with the CSC software.
The SA will ensure the CSC parameter file is not modified from the settings specified in this STIG.

Checks

CSC Configuration

The reviewer will verify the CSC configuration element. This information is available in the SRRPRT. The reviewer can use IPF and look at the SYS$LIB$*CSC.CSC$PARAM element. Do a locate on SEC_LEVEL. On ALN and DFAS-IN systems, On ALN and DNMC systems, there should be one SEC_LEVEL statements: SEC_LEVEL_4 QUERY,EJECT,ENTER,MOUNT,DISMOUNT. For all other sites there should be no SEC_LEVEL statements. If there is anything else, unless the change is documented, this is a finding.

Fixes

CSC Configuration

Set up the CSC parameter element in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.530.00 V0000658 CAT II The Client Direct Interconnect (CDI) Config

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.4.3

Vulnerability The Client Direct Interconnect (CDI) parameter element is not set up in accordance with the standard.

Vulnerability Discussion The CDI parameter element contains settings, which limit the CDI commands (e.g. TCP commands) that can be executed from a demand terminal. If these parameters are not set correctly, unauthorized users may be allowed to interface with the CDI software. The SA will ensure the CDI parameter file is not modified from the settings specified in this STIG that are the system default settings.

Checks

CDI Configuration

The reviewer will verify the CDI configuration element. This information is available in the SRRPRT. The IAO can use IPF and look at the SYS$LIB$*STRPARM.CDI$PARAM element or SYS$LIB$*CDI.CDI$PARAM element. No SEC_LEVEL statements should exist. If there are SEC_LEVEL statements this is a finding.

Fixes

CDI Configuration

Set up the CDI parameter element in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.540.00 V0000659 CAT II The Vault Management System (VMS) MCYCLE value is

8500.2 IA Control: CODB-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.3

Vulnerability The Vault Management System (VMS) MCYCLE value is not set in accordance with the standard. (Shared Library System Sites Only)

Vulnerability Discussion If the VMS MCYCLE value is not set correctly, critical files will not be properly identified for offsite storage and this could adversely impact the recovery of these applications following a contingency or emergency situation.
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

Checks

SLS VMSCYCLE Flag

The reviewer will verify that the VMSCYCLE flag is set in accordance with the Unisys STIG. This information is available in the SRRPRT. The reviewer find out if the site is using a combined vault on the Master SLS Host or a vault on each individual host and whether the Master SLS Host is an ALN or DNMC system.

If the site is using a combined vault and the SLS Master Host is an ALN system, the reviewer will verify that the SLS Host VMSRUN element in SYS$LIB$*STAR and SYS$LIB$*RUN$ has the MCYCLE set to 0 (FALSE).

If the site is using a combined vault and the SLS Master Host is a DNMC system, the reviewer will verify that the MCYCLE statement in the SLS Host vault parameter file (SYS$LIB$*STRPARM.VAULT) is set to 0 (FALSE).

If the site is using individual vaults, the reviewer will verify that all the ALN system VMSRUN elements in SYS$LIB$*STAR and SYS$LIB$*RUN$ have the MCYCLE set to 1 (TRUE).

If the site is using individual vaults, the reviewer will verify that the MCYCLE statement in all DNMC vault parameter files (SYS$LIB$*STRPARM) are set to 1 (TRUE).

If the MCYCLE value is not set correctly, this is a finding.

Fixes

SLS VMSCYCLE Flag

Set the VMS MCYCLE value in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.550.00 V0000558 CAT II System Software Security Attributes

8500.2 IA Control: DCSL-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3

Vulnerability Unauthorized personnel are removing or modifying security attributes associated with system software files.

Vulnerability Discussion Certain programs within system files can cause grave damage to the system. Before these files are released to operational sites, specific security attributes are attached so only authorized individuals can execute these programs. Removal or modification of these security attributes allows unhampered access to these dangerous programs and can result in grave damage to the system and potential denial of service to customers.
The IAO will ensure the security attributes associated with system software files are not modified or removed.

Checks

System Software ACR

If SRRPRT is not available check the element SYS$*DATA$.CO$INSTALL$/COMUS.
For every FILE statement within the element do an @PRT,F and verify that the file is protected by a ACR that restricts WRITE and DELETE. NOTE: SYS$LIB$*RUN$ should be Read Only Mode with a Write Key.

On DNMC systems, spot-check certain LIBLOAD files for ACRs.

The Toolkit SRRFSM may prove useful for checking file owners and ACRs.
Note: Some system software will be controlled with ACRs that also restrict READ and EXECUTE, these permissions are checked in other vulnerabilities.

If these files are not protected, this is a finding.

Fixes

System Software ACRs

Do not allow individuals to remove or modify the security attributes of system files. This includes not granting bypass and modify privileges to unauthorized individuals.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.560.00 V0000605 CAT II System Software Unauthorized executables

8500.2 IA Control: DCSL-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.3

Vulnerability Unauthorized programs have been added to site CCB files, released system software, or software library files.

Vulnerability Discussion SSO Montgomery personnel perform testing and security certification of all system software and library files prior to their release to operational sites. The site CCB can also approve the loading of certified software on the system. Finally, vendors verify system software they provide. If unknown programs are loaded into these files, individuals assume these programs are authorized and contain no malicious code. Individuals can then unknowingly execute these programs and potentially cause severe damage to the system or processing environment.
The SA or IAO will ensure unauthorized programs are not added to system software or library files or the site CCB.

Checks

System Library Changes

The IAO should check the file SYS$LIB$*ALTLIB, SYS$LIB$*LOCAL$LIB, and possibly, SYS$LIB$*RUN$ for unusual absolutes (for example, FANG, UDSMON, SMQ, PMP, etc.). Random checks should be made for all files found in the SYS$*DATA$.CO$INSTALL$/COMUS$. Unauthorized executables can be identified in these files noting that any executable found after the last omnibus element where not in the file at the time of the COMUS or SOLAR install. If unauthorized programs are found, this is a finding.

Fixes

System Library Changes

Do not add unauthorized programs into SSO Montgomery or site CCB released system software or library files. If the site develops certain utilities, they should be tested, certified, approved by the site CCB, and loaded into a site unique file. If needed, this file should be protected from unauthorized access.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.564.00 V0003933 CAT II Unauthorized System Software Installed

8500.2 IA Control: DCSL-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3

Vulnerability Unauthorized system software and products have been installed on the system.

Vulnerability Discussion Unauthorized software or products may contain malicious code. Additionally they may violate licensing agreements.
The IAO will ensure only authorized system software and products is installed on the system.

Checks

Unauthorized Software

The reviewer will interview the IAO to verify that only licensed software or software that has been tested for malicious code is installed on the system. The IAO will review the SRR Toolkit Installed Products Report to ensure only authorized system software and products have been installed on the system. For SSO Montgomery supported sites, there are elements in SYS$LIB$*LIB$DATA (for example, BL-DFAS/IX5-1) that contain a list of required, optional, third party, and available products. This may help the IAO to determine if any unauthorized system software has been installed on the system.

Fixes

Unauthorized Software

Remove the software from the system. Optionally if there is a need for the software, verify the safety of the software and if SSO Montgomery supported site, authorized by SSO Montgomery.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.570.00 V0000741 CAT II The system has anonymous DDP configured

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.4.1

Vulnerability The system has anonymous DDP configured.

Vulnerability Discussion Without positive user authentication and identification there is no means to track the activities of an individual for recovery or investigative purposes.
The SA will ensure the system does not have Anonymous DDP configured.

Checks

Anonymous DDP

The reviewer will verify that Anonymous DDP is not configured on the system. This information is available in the SRRPRT. Otherwise, the reviewer find out the host name for the system and then perform the following in a privileged Demand session.

```
@SYS$LIB$*DDP-PPC.CSUPDT,LZ  <xmit>
READ HOST NAME = GNMC ;  <xmit>(GNMC is an example)
@EOF
```

If FJT-USER-ID and FJT-PASSWORD are displayed, then anonymous DDP is configured and this is a finding.

Fixes

Ananymous DDP

Disable the FJT-USER-ID and FJT-PASSWORD fields in the DDP configuration file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.580.00 V0000571 CAT III The system allows anonymous FTP

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability The system allows anonymous FTP.

Vulnerability Discussion Without positive user authentication and identification, there is no means to track the activities of an individual for recovery or investigative purposes.
The IAO will ensure the system does not allow Anonymous FTP connections.

Checks

ANONYMOUS FTP

The reviewer will try to create an FTP session to the Unisys system using:

1) A userid of ANONYMOUS with a password of Guest.
2) A userid of FTPUSER with a password of Guest.
3) A userid of ANONYMOUS with a password of MAIL@MAIL.COM.

If any of these sessions is successfully login to FTP, then anonymous FTP is configured and this is a finding.

Check to see if there is a userid in SIMAN named ANONYMOUS. IF the FTP is used, userid exists and it is not deactivated, this is a finding.

Fixes

ANONYMOUS FTP

If the site is using TAS FTP as modified by SSO Montgomery to allow Anonymous FTP, consult with SSO Montgomery on how to disable Anonymous FTP.

If the site is using CpFTP, remove the A option from the processor execution in the background batch run.

In either case, if the userid Anonymous exists in the SIMAN, deactivate it.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.590.00 V0000743 CAT I TIP users single-user authentication

8500.2 IA Control: IAGA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.4.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.2

Vulnerability TIP users are not authenticated to single-user granularity (e.g., TIP Session Control or application identification and authentication).

Vulnerability Discussion Without positive user authentication and identification, there is no means to track the activities of an individual for recovery or investigative purposes.
The IAO will ensure TIP Session Control is configured on for all application groups and the IAO will ensure each TIP user has a unique userid.

Checks

TIP Userids

The reviewer will sign into each TIP application group configured. If the system prompts for a user-ID/password, then a user is authenticated to single-user granularity via TIP Session Control.

TIP Userids

The reviewer will interview the IAO to verify that each user needing access to a TIP application is given a unique userid and that they are instructed not to share their userid with anyone else.

Fixes

TIP Userids

Implement TIP Session Control, issue each authorized user a unique userid, and instruct all users that they will not share their userid with anyone.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.600.00 V0000748 CAT II Unauthorized users can execute the TIP utilities

8500.2 IA Control: DCSL-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.5

Vulnerability Unauthorized users can execute the TIP utilities (e.g., DREG, TREG, etc.)

Vulnerability Discussion The TIP utilities allow users to register, deregister, and delete online databases, transactions, etc. This makes these utilities extremely dangerous and they should be tightly controlled.
The SA will ensure dangerous TIP utilities are secured in accordance with this STIG requirements.

Checks

TIP Utilities

The reviewer will verify that the TIP$*TIPRUN$ file has an owner of -CHAMELEON- and the ACR PUBRD. Additionally the reviewer will verify that the FCREG$ interface is enforced and only given to Profile 1 – 6 users. If these conditions are not met, this is a finding.

Fixes

TIP Utilities.

Secure the TIP utilities (usually found in TIP$*TIPRUN$) in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.00 V0000750 CAT II The PSERVR routing tables are not protected from m

8500.2 IA Control: ECCD-1, ECCD-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.6

Vulnerability The PSERVR routing tables are not protected from modification by unauthorized users.

Vulnerability Discussion If the PSERVR routing tables are not secured, users could modify them to re-route print to inappropriate destinations resulting in disclosure of sensitive information, aggregation of data, or destruction of critical information.
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.

Checks

PSERVER Routing tables

The reviewer will verify that the PSERVER routing tables are protected. This information is available in the SRRPRT. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. The reviewer will locate the correct file and do a @PRT,F on the file to see if there is an ACR attached. This ACR should be a READ-ONLY ACR as a minimum. If there is no ACR on the file, this is a finding.

Fixes

PSERVR Routing Table

Protect the PSERVR routing table in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.01 V0003934 CAT II PSERVER KEYTYPE statment

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.1

Vulnerability There is no KEYTYPE statement in the PSERVER configuration.

Vulnerability Discussion The KEYTYPE statement in the PSERVER configuration controls the console interface to the PSERVER background run. If the statement does not exist in the configuration; the value will default to a known value of PS. This can lead to destructive PSERVER console keyins performed via the CONNS interface leading to denial of service or print files being distributed to unauthorized locations.
The SA will ensure there is a KEYTYPE statement in PSERVER configurations.

Checks

PSERVER KEYTYPE

The reviewer will verify that the KEYTYE card exists in the PSERVER configuration source element. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. The reviewer will use IPF and do a locate on KEYTYPE. There should be a KEYTYPE statement in the PSERVER element. If there is no KEYTYPE statement, this is a finding.

Fixes

PSERVER KEYTYPE

Insert a KEYTYPE statement into the PSERVER configuration. Stop the running copy of PSERVER and restart it applying the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.02 V0003935 CAT II The PSERVER KEYTYPE field is set to PS

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.1

Vulnerability The PSERVER KEYTYPE field is set to PS.

Vulnerability Discussion The default value for the PSERVER KEYTYPE field is PS. The KEYTYPE field is the consol command string used to communicate with the PSERVER background run. The use of the default known value of PS can lead to destructive PSERVER commands being submitted via the CONS interface leading to a denial of service or print files being routed to unauthorized locations.
The SA will ensure the value of the second field of the KEYTYPE field is not be PS.

Checks

PSERVER KEYTYPE field

The reviewer will verify that the KEYTYE card in the PSERVER configuration source element does not contain the value PS. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. The reviewer will use IPF and do a locate on KEYTYPE. There should be a KEYTYPE statement in the PSERVER element. If there is a KEYTYPE statement and it contains the value PS, this is a finding.

Fixes

PSERVER KEYTYPE Field

Change the value of the KEYTYPE field in the PSERVER configuration to a different value than PS. Stop the PSERVER background run and restart it applying the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.03 V0003936 CAT II PSERVER Receive Statement

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.2

Vulnerability There are configurations statements related to the RECEIVE statement in the PSERVER configuration.

Vulnerability Discussion The statements related to the PSERVER RECEIVE statement are only used during Unisys to Unisys mainframe print file transfer. Since printers are no longer attached to the Unisys mainframes, there is no need for a print file transfer. Any use of the print file transfer functionality is therefore an anonymous file transfer, which is not allowed. Therefore there is no longer a need for these configuration statements and their existence would allow an anonymous file transfer to occur.
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.

Checks

RECEIVE Related statements

The reviewer will verify that the PSERVER configuration source element does not contain any of the following statements. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. PSERVER should only be used on systems that support the Tape Transfer Utility. The reviewer will use IPF and do a locate on the following configuration statements: ASG-DEVICE, ASG-PACKID, ASG-SIZE, FILE-ACCESS, and QUAL-FILE. None of these statements should be in the PSERVER configuration. If they are found, this is a finding.

Fixes

RECEIVE Related Statements

Remove the offending statements from the configuration. Stop the PSERVER background run and restart it using the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.04 V0003937 CAT II PSERVER RECEIVE Statement

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.2

Vulnerability There is a RECEIVE statement that does not contain a receive application name in the PSERVER configuration.

Vulnerability Discussion The RECEIVE statement without a receive application name will allow a connection from any sending PSERVER application. This could lead to a denial of service attack by a unauthorized system sending multiple files to the PSERVER tape file transfer interface.
The SA will ensure the RECEIVE statement contains a receiver application name.

Checks

PSERVER RECEIVE statement

The reviewer will verify that there is no RECEIVE statement in the PSERVER configuration source element does not contain a receive application name.
On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00.
The reviewer will use IPF and do a locate on RECEIVE. There should be a receiver application name (for example, TXFR-REL) on the RECEIVE statement. If the RECEIVE statement is blank, this is a finding.

Fixes

PSERVER RECEIVE Statement

Remove any RECEIVE statements without a receive application name or update the statement to contain an authorized receive application name. Stop the PSERVER background run and restart the background run using the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.05 V0003938 CAT II PSERVER SEND Statement

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.3

Vulnerability There are unauthorized SEND statements in the PSERVER configuration.

Vulnerability Discussion Unauthorized SEND statements in the PSERVER configuration can be used for anonymous file transfers to unauthorized systems. This can lead to the compromise of sensitive information.
The SA will ensure the PSERVER configuration file only contains SEND statements identify a sending Tape File Transfer queue.

Checks

PSERVER SEND Tape Queue

The reviewer will verify that there are no SEND statements in the PSERVER configuration element that do not include a destination tape transfer queue. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. PSERVER will only be used on systems that support the Tape Transfer Utility. The IAO can go into IPF and do a locate command on all SEND statements. All SEND statements should contain a Tape File Transfer queue (for example, SEND TXFR02 TO OGHI,TXFR02 USING TXFR-REL). If the SEND statement contains a queue name other than a Tape File Transfer queue, this is a finding.

Fixes

PSERVER SEND Tape Queue

Remove any unauthorized SEND statements from the PSERVER configuration. Stop the PSERVER background run and restart the background run using the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.06 V0003939 CAT II PSERVER SEND no Destination

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.2.3

Vulnerability There is a SEND statement in the PSERVER configuration that does not contain a destination application name.

Vulnerability Discussion A SEND statement in the PSERVER configuration that does not contain a destination application name can be used to transfer files to an unauthorized location leading to the compromise of sensitive data.
The SA will ensure each SEND statement contains a destination application name.

Checks

PSERVER SEND Destination

The reviewer will verify that there are no SEND statements in the PSERVER configuration file. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. PSERVER will only be used on systems that support the Tape Transfer Utility. The reviewer will use IPF and do a locate command on all SEND statements. All SEND statements will contain a destination application name (for example, SEND TXFR02 TO OGHI,TXFR02 USING TXFR-REL). If the SEND statement does not contain a destination application name, this is a finding.

Fixes

PSERVER SEND Destination

Remove any unauthorized SEND statements from the PSERVER configuration. Stop the PSERVER background run and restart the background run using the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.07 V0003940 CAT II The PSERVER Batch Run Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.13

Vulnerability The PSERVER batch run userid is not configured as batch only.

Vulnerability Discussion If the PSERVER batch run userid is not configured as batch only an unauthorized access may occur.
The SA will ensure the PSERVER batch run userid is batch only.

Checks

PSERVER Batch Run Userid

The reviewer will sign on to the system in demand and do an @@CONS RC on the PSERVER batch job. Once the user-ID is identified, the reviewer will look in the Toolkit SRRALL file to verify the user-ID has only batch run access. PSERVER can be started with the system standard batch user-ID (for example, OPR or OCJZ00).

Fixes

PSERVER Batch Run Userid

Configure the PSERVER batch run userid in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.08 V0003941 CAT II The PSERVER background run account realtime

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.4

Vulnerability The PSERVER background run account does not have the realtime privilege or is not ALN exempt.

Vulnerability Discussion If the PSERVER background run account does not have the realtime privilege, file transfers will take an inappropriate amount of time. If the account is not ALN exempt, the tape file transfer will fail.
The SA will ensure the PSERVER background run account is allowed realtime privilege.

Checks

PSERVER Batch Run Account

The reviewer will verify that the account used by PSERVE will have realtime privilege The reviewer will sign on to the system in demand and do an @@CONS RC on the PSERVER batch job. Once the account is identified, the reviewer will check in SIMAN and verify that the account is allowed a maximum real-time level of 2 – 35. On ALN systems, this account will be an ALN exempt account (for example, 0000JZ1A).

Fixes

PSERVER Batch Run Account

Configure the PSERVER background run account in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.09 V0003942 CAT II The execution of PSERVER Options

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.5

Vulnerability The execution of PSERVER does not have the required options set.

Vulnerability Discussion Failure to have the required options set will cause tape file transfers to fail.
The SA will ensure the background batch run execution of PSERVER has the “BOU” execute options set.

Checks

PSERVER Execute Options

The reviewer will verify that the execute options on the PSERVER absolute in the PSERVER runstream has only the B, O, and U options set. On ALN, DFAS-IN, and CAMS CDB systems, this element should be in PS$$0000*00 or SYS$*PS. On DNMC systems, this element could also be in PS$$0000*00. The runstream may also be in SYS$LIB$*RUN$. PSERVER will only be used on systems that support the Tape Transfer Utility. The reviewer will use IPF and do a locate command on the execution of the PSERVER absolute. The options on the execute statement should be BOU.

Fixes

PSERVER Execute Options

Correct the PSERVER background runs runstream giving the execution of the PSERVER program the correct options. Stop the PSERVER background run and restart it using the corrected runstream.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.11 V0006491 CAT II PSERVER Batch Run Userid Disabled

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.3

Vulnerability The PSERVER batch run Userid is not disabled.

Vulnerability Discussion A disabled userid cannot be used to sign on to an interactive Demand or TIP session. Since the PSERVER batch runs userid does not need this ability it will not have it.
The SA will ensure the PSERVER batch run userid is disabled.

Checks

PSERVER Userid Disabled

The reviewer will sign on to the system in demand and do an @@CONS RC on the PSERVER batch job. Once the userid is identified, the reviewer will look in the Toolkit SRRALL file to verify the userid is disabled. PSERVER can be started with the system standard batch userid (for example, OPR or OCJZ00).

Fixes

PSERVER Userid Disable

Disable the PSERVER userid using SIMAN.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.12 V0006494 CAT II PSERVER Userid Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.1.3

Vulnerability The PSERVER batch run userid does not have the required privileges.

Vulnerability Discussion Without the correct privileges the PSERVER run may fail creating a denial of service for the updating of system software.
The SA will ensure the PSERVER batch run userid has the privileges required by this STIG.

Checks

PSERVER Batch Run Privileges

The reviewer will verify that the PSERVER batch userid will have the correct privileges. The reviewer will find out what the PSERVER's runid is and @@CONS RC the runid to discover the userid that is being used by the PSERVER run. The reviewer will look in the Toolkit SRRALL file for this userid and verify it has these privileges:

BYACR
BYCOMPMT
BYOWNER
BYCL
BYPRVFLC
BYRWKEY
BYRWMODE
COM$PRV
CREEXCLG
MODRECCL
SMOQUE
SSSSCALLANY

If it does not match have the above privileges, this is a finding.

Fixes

PSERVER Batch Run Privileges

Using SIMAN grant the PSERVER batch run userid the privileges in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.610.13 V0006497 CAT II Tape File Transfer Configuration File

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.2.2

Vulnerability The Tape File Transfer Configuration file is not secured with ACR ACRRO or an ACR like ACRRO to protect it from modification.

Vulnerability Discussion If the Tape File Transfer Configuration file is not protected, unauthorized users could update or delete the configuration causing the TAPE FILE Transfer software to fail. This could lead to a denial of service waiting for a software update to be transferred to the system.
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.

Checks

Tape File Transfer Config

The reviewer will verify that the Tape File Transfer Configuration file (SYS$LIB$*TXFR-CONFIG) is protected with the ACR ACRRO or an ACR with restrictive write access. The reviewer can do this by doing an @PRT,F on the file and if the ACR is not ACRRO use SIMAN to check that the ACR only allows authorized users write access to the file.

Fixes

TAPE File Transfer Config

Attach the ACR ACRRO or an ACR with that restricts write access to authorized users to the Tape File Transfer Configuration file.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.620.00 V0000754 CAT II QTPIE Routing Table Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.3.2

Vulnerability The QTPIE routing table is not protected from unauthorized users.

Vulnerability Discussion If the QTPIE routing tables are not secured, users could modify them to re-route print to inappropriate destinations resulting in disclosure of sensitive information, aggregation of data, or destruction of critical information.
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.

Checks

QTPIE Routing Tables

The reviewer will verify that the QTPIE routing tables are protected by a read only ACR. This information is available in the SRRPRT. Some ALN systems have this element in PS$$0000*00. Others have this element in 0DP00000*PMSCRQ055-DP. The reviewer will do a @PRT,F on the file to see if there is an ACR attached. The ACR should be a READ-ONLY ACR as a minimum. Some sites do not have this file on the system at all. DNMC, DFAS-IN, and CAMS CDB systems do not use QTPIE.

Fixes

QTPIE Routing Table

Secure the file containing the QTPIE routing tables with a read only ACR.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.630.00 V0000755 CAT II The PDQ Routing Tables Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.4.2

Vulnerability The PDQ routing tables are not protected from unauthorized users.

Vulnerability Discussion If the PDQ routing tables are not secured, users could modify them to re-route print to inappropriate destinations resulting in disclosure of sensitive information, aggregation of data, or destruction of critical information.
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.

Checks

PDQ Routing Tables

The reviewer will verify that the PDQ routing tables are in a file that is protected by a read only ACR. This information is available in the SRRPRT. The reviewer will check SYS$LIB$*PDQ.PDQ to see where the runstream is @ADD'ing the PDQ/PARM element from. On ALN systems, this element and the PDQ runstream can be in PS$$0000*00, SYS$LIB$*STRPARM, or SYS$*PS. On DNMC, DFAS-IN, and CAMS CDB systems, this element may also be in PS$$0000*00. On some systems this runstream will be in SYS$LIB$*RUN$. The reviewer will do a @PRT,F on the file to see if there is an ACR attached. The ACR should be a READ-ONLY ACR as a minimum.

Fixes

PDQ Routing Tables

Secure the file containing the PDQ routing tables with a read only ACR.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.00 V0000606 CAT II DEPCON Routing Tables Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.5

Vulnerability The DEPCON routing tables are not protected from unauthorized users.

Vulnerability Discussion If the DEPCON routing tables are not secured, users could modify them to re-route print to inappropriate destinations resulting in disclosure of sensitive information, aggregation of data, or destruction of critical information.
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.

Checks

DEPCON Routing Table

The reviewer will verify that the file containing the DEPCON routing tables is protected by a read only ACR. This information is available in the SRRPRT. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. For other sites the runstream will be in SYS$LIB$*RUN$. The reviewer do a @PRT,F on the file containing the DEPCON routing tables and verify that there is an read only ACR attached to the file.

Fixes

DEPCON Routing Table

Secure the file containing the DEPCON routing tables by attaching a read only ACR.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.01 V0003943 CAT II The DEPCON no KEYTYPE statement

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.1

Vulnerability The DEPCON configuration contains no KEYTYPE statement or more than one KEYTYPE statement.

Vulnerability Discussion IF the DEPCON configuration contains no KEYTYPE statement, the KEYTYPE will default to DEPCON. The KEYTYPE value is used as the start of the consol command sequence to access DEPCON. This can lead to loss of service if a destructive command is entered via the CONS console interface. If there is more than one KEYTYPE statement in the DEPCON configuration, the last statement is used. This can lead to confusion as to what is the correct start of the consol command sequence to access DEPCON.

Checks

Unisys S103.640.01

The reviewer will review the DEPCON configuration to verify that there is one and only one KEYTYPE statement in the configuration.

Fixes

DEPCON Number of KEYTYPE State

Update the DEPCON configuration so that there is one and only one KEYTYPE statement in the configuration. Stop the DEPCON background run and restart it using the updated configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.02 V0003944 CAT II DEPCON KEYTYPE Value

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.1

Vulnerability There is a KEYTYPE statement in the DEPCON configuration that has a KEYTYPE value of DEPCON.

Vulnerability Discussion The known default value of the KEYTYPE field is DEPCON. The KEYTYPE value is used as the start of the consol command sequence to access DEPCON. Use of a KEYTYPE value set to the known default value can lead to loss of service if a destructive command is entered via the CONS console interface.
The SA will ensure the value of the second field of the KEYTYPE field is not DEPCON.

Checks

DEPCON KEYTYPE Value

The reviewer will verify that the second filed of the KEYTYPE statement in the DEPCON configuration is not DEPCON. For ALN systems, the configuration and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. For other systems check SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on the KEYTYPE statement. There value of the second field on the KEYTYPE statement will not be DEPCON

Fixes

DEPCON KEYTYPE Value

Update the DEPCON configuration so that the KEYTYPE value is something other than DEPCON.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.03 V0003945 CAT II There is a RECEIVE and QUAL-FILE

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.2

Vulnerability There is a RECEIVE statement in the DEPCON configuration but there is not a QUAL-FILE statement.

Vulnerability Discussion A RECEIVE statement without a QUAL-FILE statement can allow files to be transferred with the name change on the receiving system losing the original name of the file from the sending system.
The SA will ensure, if the RECEIVE statement is used, a QUAL-FILE statement is also used.

Checks

DEPCON RECEIVE

The reviewer will verify that if DEPCON has a RECEIVE statement it also has a QUAL-FILE statement in the configuration. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on the RECEIVE statement. If there is a RECEIVE statement, there will be a QUAL-FILE statement in the DEPCON configuration.

Fixes

DEPCON RECEIVE

Create a correctly formatted QUAL-FILE statement in the DEPCON configuration. Stop the DEPCON background run and restart it using the updated configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.04 V0003946 CAT II DEPCON QUAL-FILE Statement Format

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.2

Vulnerability The QUAL-FILE statement is incorrectly formatted.

Vulnerability Discussion Without a correctly formatted QUAL-FILE statement, the file name is not maintained from the sending system to the receiving system.
The SA will ensure the QUAL-FILE statement has one of the following the following formats:

```
   QUAL-FILE QUAL-H1,QUAL-H2, FILE-H1,FILE-H2.
                           or
   QUAL-FILE QUAL-H1,QUAL-H2, FILE-H1,TIME.
```

Checks

DEPCON QUAL-FILE

The reviewer will verify that the QUAL-FILE statement, if needed in the DEPCON configuration, has the correct format. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on the QUAL-FILE statement. The QUAL-FILE statement will have one of the following formats.

```
QUAL-FILE QUAL-H1,QUAL-H2, FILE-H1,FILE-H2
QUAL-FILE QUAL-H1,QUAL-H2, FILE-H1,TIME
```

Fixes

DEPCON QUAL-FILE

Create a correctly formatted QUAL-FILE statement in the DEPCON configuration or modify the existing QUAL-FILE to have the correct format. Stop the DEPCON background run and restart it using the updated configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.05 V0003947 CAT II DEPCON Example Passwords

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.3

Vulnerability Example passwords are being used in the DEPCON configuration.

Vulnerability Discussion Passwords for the TCP-PROCESS, TSAM-PROCESS, or LPR-PROCESS statements in the DEPCON configuration were taken from DEPCON documentation. The use of passwords from documentation can allow malicious code to hijack a Unisys proprietary communications interface causing the communications software to fail, DEPCON initialization to fail, or a compromise of the system security by initializing an unauthorized communications link.
The SA will ensure the PASSWORD field of these statements does not contain any value found in any example configurations.

Checks

DEPCON PROCESS Passwords

The reviewer will verify that non of the passwords used for the PASSWORD values on the TCP-PROCESS, TSAM-PROCESS, and LPR-PROCESS Statements are from the documentation examples. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on all PROCESS statements. All PROCESS statements should contain a PASSWORD field. If there is a password in the PASSWORD field that matches any password in documented examples, this is a finding. Known passwords in documented examples include DEPCON, TCP123, and LPR123.

Fixes

DEPCON PROCESS Passwords

Replace the passwords found in the DEPCON configuration that match documentation passwords with passwords using the password construction rules. Find the corresponding entries in the CMS1100 or CPcom configuration and update them to match the new passwords in DEPCON. Stop the DEPCON background run. Follow local documented procedures to take down the communication programs CMS1100 or CPcom. Restart CMS1100 or CPcom using the modified configurations. Restart the DEPCON background run using the new configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.06 V0003948 CAT II TSEL-NAME Values from Documentation Examples

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.3

Vulnerability The TSEL-NAME values from documentation examples are being used in the TSAM-PROCESS statement of the DEPCON configuration.

Vulnerability Discussion Use of a known TSEL-NAME can lead to a denial of service attack on the DEPCON software by an outside agent.
The SA will ensure the TSEL-NAME field of the TSAM-PROCESS statement does not contain any value found in any example configurations.

Checks

DEPCON TSEL-NAME TSAM-PROCESS

The reviewer will verify that no value found on the TSEL-NAME field within the DEPCON configuration is a known value from an example in the documentation. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The will use IPF and do a locate command on all TSAM-PROCESS statements. The TSAM-PROCESS statement can contain a TSEL-NAME field. If there is a value in the TSEL-NAME field that matches any value in documented examples, this is a finding. The only known value in documented examples is DEPCON. If there is no TSEL-NAME field in the TSAM-PROCESS statement, then the TSEL-NAME in the TSAM-PEER statement is used.

Fixes

DEPCON TSEL-NAME TSAM-PROCESS

Replace the TSEL-NAME found in the DEPCON configuration that match documentation TSEL-NAME fields with values using the password construction rules. Find the corresponding entries in the CMS1100 or CPcom configuration and update them to match the new values in DEPCON. Update the corresponding fields in any remote DEPCON implementation that uses this TSEL-NAME. Stop the DEPCON background run. Follow local documented procedures to take down the communication programs CMS1100 or CPcom. Restart CMS1100 or CPcom using the modified configurations. Restart the DEPCON background run using the new configuration. Stop and restart any corresponding remote DEPCON implementations effected.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.07 V0003949 CAT II DEPCON TSEL-NAME TSAM-PEER

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.1.4.2

Vulnerability The TSEL-NAME values from documentation examples are being used in the TSAM-PEER statement of the DEPCON configuration.

Vulnerability Discussion Use of a known TSEL-NAME can lead to a denial of service attack on the DEPCON software by an outside agent.
The SA will ensure the TSEL-NAME field on the TSAM-PEER statement does not contain any value found in a sample configuration.

Checks

DEPCON TSEL-NAME TSAM-PEER

The reviewer will verify that no value found on the TSEL-NAME field within the DEPCON configuration is a known value from an example in the documentation. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on all TSAM-PEER statements. The TSAM-PEER statement can contain a TSEL-NAME field. If there is a value in the TSEL-NAME field that matches any value in documented examples, this is a finding. The only known value in documented examples is DEPCON

Fixes

DEPCON TSEL-NAME TSAM-PEER

Replace the TSEL-NAME found in the DEPCON configuration that match documentation TSEL-NAME fields with values using the password construction rules. Find the corresponding entries in the CMS1100 or CPcom configuration and update them to match the new values in DEPCON. Update the corresponding fields in any remote DEPCON implementation that uses this TSEL-NAME. Stop the DEPCON background run. Follow local documented procedures to take down the communication programs CMS1100 or CPcom. Restart CMS1100 or CPcom using the modified configurations. Restart the DEPCON background run using the new configuration. Stop and restart any corresponding remote DEPCON implementations effected.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.08 V0003950 CAT II DEPCON Batch Run Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.2

Vulnerability The DEPCON background batch run userid is not configured correctly.

Vulnerability Discussion An improperly configured userid can lead to the corruption or compromise of data. Additionally, it could lead to an interruption of service.
The SA will ensure the DEPCON batch run userid is batch only, disabled and privileges are limited to those described in this STIG.

Checks

DEPCON Batch Run Userid

The reviewer will sign on to the system in demand and do an @@CONS RC on the DEPCON batch job. Once the userid is identified, the reviewer will look in the Toolkit SRRALL file to verify that the userid has only those privileges identified in the Unisys STIG. These privileges are BYOWNER, COM$PRV, CREEXCLG, MODRECCL, and SMOQUE. The userid will have only batch access and it will be disabled. No interfaces are required for this userid.

Fixes

DEPCON Batch Run Userid

Configure the DEPCON background runs userid in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.09 V0003951 CAT II DEPCON Batch Run Account

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.3

Vulnerability The DEPCON background run account is not configured in accordance with the Unisys STIG.

Vulnerability Discussion If the background run account is not configured correctly it can lead to an interruption of service.
The SA will ensure the DEPCON background run account is allowed realtime privilege. For ALN sites this will be an exempt account.

Checks

DEPCON Batch Account

The reviewer will sign to the system in demand and do an @@CONS RC on the DEPCON batch job. Once the account is identified, the reviewer will go into SIMAN and verify that the account is allowed a maximum real-time level of 2 – 35. On ALN systems, this account will be an ALN exempt account (for example, 0000JZ1A).

Fixes

DEPCON Batch Account

Configure the DEPCON background runs account in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.10 V0003952 CAT II DEPCON Program Options

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.1.4

Vulnerability The DEPCON background run program executions do not have the required execute options or have the restricted execute option.

Vulnerability Discussion If the DEPCON background run program does not have the required execute options, DEPCON will not function correctly. If the DEPCON background run program has the restricted option, this would allow unauthorized users to reconfigure DEPCON interactively which can lead to print files distributed to unauthorized locations.
The SA will ensure the background batch run execution of DEPCON does not have the “Y” execute option set but does have the "O" and "S" options.

Checks

DEPCON Batch Execute Options

The reviewer will verify that the execution of the DEPCON program in the DEPCON background runstream has the “O” and “S” options and does not have the Y option. For ALN systems, the routing table and the DEPCON runstream could be in PS$$0000*00, SYS$*PS, or JT$$0000*00. For DNMC, DFAS-IN, and CAMS CDB systems, check PS$$0000*00 and SYS$LIB$*RUN$. The reviewer will use IPF and do a locate command on the execution of the DEPCON absolute. The options on the execute statement will contain an “O” and an “S” but not a “Y”. Other execute options can be used if desired by the site.

Fixes

DEPCON Batch Execute Options

Modify the DEPCON background run runstream to have the execute options required in accordance with the Unisys STIG and not have any options prohibited by the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.12 V0003954 CAT II DEPCON Windows Directory Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.2.1

Vulnerability The DEPCON system directories and the Group Print Hold directories are not secured in accordance with the Unisys STIG.

Vulnerability Discussion Failure to secure the system or Group Print Hold directories as required can lead to an interruption of service or the compromise of sensitive data.
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.

Checks

DEPCON Windows Access

The reviewer will contact the System Administrator for the DEPCON desktop(s) and with their assistance verify that the DEPCON system directories and the Group Print Hold directories are secured. All DEPCON system directories and the Group Print Hold directories should be restricted to the user(s) allowed to run the DEPCON server software.

Fixes

DEPCON Windows Access

Secure the DEPCON system directories and the Group Print Hold directories in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.13 V0003955 CAT II The DEPCON Windows Server Physical Security

8500.2 IA Control: PECF-1, PECF-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.2.1.1

Vulnerability The DEPCON Windows server is not adequately physically secured.

Vulnerability Discussion Since the DEPCON Windows component will not run as a service it is necessary for the personnel responsible for the day to day operations of the DEPCON Windows component to use a group userid with many high level privileges. To mitigate the vulnerability created by this group userid, the DEPCON Windows server must be placed in an area that meets the security requirements of the highest security level of objects transferred.
The IAO will ensure the DEPCON Windows is physically secured to the level required of the highest security objects transferred.

Checks

DEPCON Physical Security

The reviewer will interview the IAO to verify that the DEPCON Windows server is physically protected in the manner required for by the highest classification of the data that is processed by DEPCON Windows.

Fixes

DEPCON Physical Security

Locate the DEPCON Windows server in an area that meets the security requirements in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.15 V0003957 CAT II DEPCON Windows Configuration Password

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.2.1.3.1

Vulnerability DEPCON Windows does not have a configuration password.

Vulnerability Discussion If DEPCON Windows does not have a configuration password, the DEPCON Windows configuration can be modified by unauthorized users leading to an interruption of service or the compromise of sensitive data.
The SA will ensure DEPCON has a configuration password.

Checks

DEPCON Configuration Password

The reviewer will try to access a configuration item from the DEPCON Windows Management interface. Without modifying the item save it. If during these actions you are not challenged for a configuration password this is a finding.

Fixes

DEPCON Configuration Password

Create a DEPCON Windows configuration password in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.16 V0003958 CAT II Unauthorized Access to the DEPCON Windos Config

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.2.1.3.1

Vulnerability Unauthorized users have access to the DEPCON Windows configuration.

Vulnerability Discussion If the DEPCON Windows configuration password is known by users not responsible for the configuration, the DEPCON Windows configuration can be modified by unauthorized users leading to an interruption of service or the compromise of sensitive data.
The SA will ensure the DEPCON configuration password is known only to personnel who configure DEPCON.

Checks

DEPCON Windows Configuration P

The reviewer will interview the SA to verify that the DEPCON Configuration Password is only known by users who configure DEPCON.

Fixes

DEPCON Configuration Password

Change the DEPCON Windows configuration password and distribute it only to individuals responsible for the configuration of the DEPCON Windows component.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.640.17 V0003959 CAT II Change the DEPCON Windows Config Password

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.6.2.1.3.1

Vulnerability There is no policy for changing the DEPCON Windows configuration password.

Vulnerability Discussion Changing of passwords on a regular basis limits the window of vulnerability when a password is compromised but the compromise is not discovered.
The DEPCON SA will establish a procedure to ensure the password is changed every 90 days.

Checks

DEPCON Password Change

The reviewer will interview the SA to verify that there is a process in place to change the DEPCON Configuration at least every 90 days.

Fixes

DEPCON Password Change

Establish a procedure to ensure that the DEPCON Windows configuration password is changed in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.650.00 V0000660 CAT II AB Routing Tables Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.5.2

Vulnerability The AB routing tables are not protected from unauthorized users.

Vulnerability Discussion If the AB routing tables are not secured, users could modify them to re-route print to inappropriate destinations resulting in disclosure of sensitive information, aggregation of data, or destruction of critical information.
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.

Checks

AB Routing Table Access

The reviewer will verify that the file(s) containing AB routing tables are protected by a read only ACR. The review will use the Toolkit SRRFSM file or a @PRT,L listing and locate all AB, AB$$, AABP0D, and AABP0M files. The will do a @PRT,F on these files to see if there is an ACR attached. There should be a READ-ONLY ACR as a minimum.

Fixes

AB Routing Table Access

Secure the AB routing tables in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.660.00 V0000607 CAT II DDP Configuration File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.4.2.2

Vulnerability The DDP configuration file (DDP*CS$CONFIG) is not protected from unauthorized users.

Vulnerability Discussion If the DDP configuration file is not secured, unauthorized users can obtain or modify sensitive information concerning the File Transfer userid and distributed data processing configuration. Improper or malicious modifications could result in the termination of file transfers or misrouting of files to unauthorized personnel.
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.

Checks

DDP Access

The reviewer will verify that the DDP configuration file is protected from unauthorized users.
For ALN sites:
This information is available in the SRRPRT. The secured version of CSUPDT has been released to all ALN, DNMC, DFAS-IN, and CAMS CDB systems. The will obtain the latest version date of the CSUPDT processor from SSO Montgomery and do a @PRT,TL SYS$LIB$*DDP-PPC.CSUPDT to ensure they match. The CS$CONFIG file should also be secured with ACRRO.
The IAO can do a @PRT,F DDP*CS$CONFIG to ensure the ACR is attached.
For non-ALN sites:
Do an @PRT,FL on the CS$CONFIG file. An restrictive ACR should be attached to the file allowing access to authorized userids. Note: the userid that owns the DDP subsystem will have read and write access to this file.

Fixes

DDP Access

Secure the DDP configuration file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.662.00 V0003960 CAT II The DDP Log and Trace File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.4.3

Vulnerability The DDP Log and Trace files are not protected in accordance with the Unisys STIG.

Vulnerability Discussion The DDP Log and Trace files can contain sensitive data. Failure to secure them in accordance with the Unisys STIG can lead to the compromise of sensitive data.
The SA will ensure the DDP Log and Trace files are secured with an ACR to protect from unauthorized access.

Checks

DDP Loge And Trace Access

The reviewer will verify that the DDP log and trace files are protected by restrictive ACR. This information is available in the SRRPRT. The reviewer will do a @PRT,F on the following files to make sure they have an ACR attached to them: SYS$LIB$*DDP$BNKLIST, SYS$LIB$*DDP$LOG, and SYS$LIB$*DDP$TRC. The attached ACR must be owned by -DDP-PPC- and read and write access must be restricted to userid –DDP-PPC-. The content of the CS$CONFIG file must also reflect this ACR in the statement ACR-NAME. The reviewer will find out the host name for the system and then perform the following:

```
    @SYS$LIB$*DDP-PPC.CSUPDT,LZ  <xmit>
    READ HOST NAME = GNMC ;  <xmit>(GNMC is an example)
    @EOF
```

The ACR-NAME value displayed will match the ACR that is attached to the above file.

Fixes

DDP Log and Trace Access

Secure the DDP Log and Trace files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.670.00 V0002672 CAT II Virtual FTP Userids and Password File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3.2.2

Vulnerability The file containing the Virtual FTP userids and passwords is not secured in accordance with the standard.

Vulnerability Discussion The Virtual FTP userids and passwords can be used for FTPs to the Unisys system. Although these userids are not SIMAN userids and cannot be used for interactive sessions, they are stored in clear text in a file named SYS$LIB$*TASANON$ and must be protected from access and/or modification. If these userids and passwords are compromised, unauthorized users could use them to FTP files to the Unisys system or if they are modified, authorized FTPs would cease to work properly.
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.

Checks

TAS FTP Virtuial Userids

The reviewer will verify that for sites running the SSO Montgomery modified TAS, the virtual userid file is protected from modification by unauthorized users with an ACR. This information is available in the SRRPRT. For ALN, DFAS-IN, CAMS CDB, and DNMC systems, the will do a @PRT,F SYS$LIB$*TASANON$ to see if ACRNA is attached.

Fixes

TAS FTP Virtual Userids

Secure the file containing the Virtual FTP userids and passwords in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.680.00 V0000608 CAT II TELCON's CMS files Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.3

Vulnerability The Telecommunications Configuration (TELCON)/Communications Management System (CMS) file is not secured in accordance with the standard.

Vulnerability Discussion If the TELCON/CMS file is not secured, unauthorized users could obtain or modify sensitive information concerning the CMS Administrator userid or the network configuration. Improper or malicious modifications could result in the unauthorized use of CMS commands, misrouting of files to unauthorized personnel, or denial of service to users on the network.
The SA will ensure the Telecommunications Configuration (TELCON)/Communications Management System (CMS) file (SYS$LIB$*FEPLOAD) is secured with the ACR ACRNA to protect it from access by unauthorized personnel.

Checks

Telcon Load File Access

The reviewer will verify that the Telcon load file is secured with the ACR ACRNA. This information is available in the SRRPRT. For ALN, DFAS-IN, CAMS CDB, and DNMC systems, the reviewer will do a @PRT,F SYS$LIB$*FEPLOAD to see if ACRNA is attached. For other systems, the reviewer can look at SYS$LIB$*RUN$.CMS to see where the runstream is getting the CONFIG element from then check the configuration and find the LOAD field of the FEP statement. The Load field contains the name of the TELCON load file. Once identified, check the file for the ACR.

Fixes

TELCON Load File Access

Secure the TELCON/CMS file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.690.00 V0000609 CAT II The CMS word addressable configuration Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.6

Vulnerability The CMS word addressable configuration is cataloged as a public file.

Vulnerability Discussion If the CMS word addressable configuration file is not private, an unauthorized users could obtain or modify sensitive information concerning the CMS Administrator userid or the network configuration. Improper or malicious modifications could result in the unauthorized use of CMS commands, misrouting of files to unauthorized personnel, or denial of service to users on the network. This also causes CMS 1100 to catalog all log, dump, and trace files private, protecting them from unauthorized browsing.
The SA will ensure the CMS 1100 word addressable configuration file is cataloged private and owned by the CMS 1100 batch run userid.

Checks

CMS WAD Access

The reviewer will verify that the CMS 1100 word addressable configuration file is cataloged private and is owned by the CMS1100 batch run userid. This information is available in the SRRPRT. For ALN, DFAS-IN, CAMS CDB, and DNMC systems, the reviewer will do a @PRT,F SYS$*NCO to see if the file is private and owned by the userid used to start CMS. For other systems, the reviewer look at SYS$LIB$*RUN$.CMS to see what word addressable file is being generated by CMS. Once identified, check to see if the file is private and owned by the userid used to start CMS
NOTE: If the CMS word addressable file is owned and private, other files created by the CMS batch run will be owned and private. These include SYS$*CONF (SSO Montgomery supported sites only), SYS$LIB$*CMS1100-PMD, SYS$LIB$*CMS1100-SNAP, SYS$LIB$*LOG$FILE, SYS$LIB$*TRACE$FILE, and any TELCON dumps, if generated.

Fixes

CMS WAD Access

Secure the CMS file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.700.00 V0000610 CAT II TELCON Source File

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.3

Vulnerability The TELCON source file is not secured in accordance with the standard.

Vulnerability Discussion If the TELCON file is not secured, then unauthorized users could modify sensitive information concerning the network configuration. Improper or malicious modifications could result in the unauthorized establishment of network devices, misrouting of data to unauthorized personnel, or denial of service to users on the network.
The SA will ensure the Telecommunications Configuration (TELCON) source file is secured with the ACR ACRRO to protect it from modification by unauthorized personnel.

Checks

TELCON Source Access

The reviewer will verify that the TELCON Source file is protected by an ACR that restricts write access. This information is available in the SRRPRT. This source file may be DCFS*TELCON or another filename. The reviewer will check with Technical Support personnel if unsure about the filename. The reviewer will then do an @PRT,F on the file and verify that a restrictive ACR is attached.

Fixes

Telcon Source Access

Secure the TELCON source file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.710.00 V0000661 CAT II TELCON Remote Concentrator and DCP load file

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.3

Vulnerability The TELCON file containing Remote Concentrator and/or Distributed Communications Processor (DCP) load elements is not secured in accordance with the standard.

Vulnerability Discussion If the TELCON file containing Remote Concentrator and/or DCP load elements is not secured, unauthorized users could delete or modify sensitive information concerning the network configuration. Improper or malicious deletions or modifications could result in denial of service to users on the network.
The SA will ensure the Telecommunications Configuration (TELCON) file (SYS$LIB$*LOAD is secured with the ACR ACRNA to protect it from access by unauthorized personnel.

Checks

TELCON Remote Concentrator

The reviewer will verify that the TELCON Remote Concentrator load file is protected with the ACR ACRNA. This information is available in the SRRPRT. This file may be SYS$LIB$*LOAD or another filename. The reviewer will check with Technical Support personnel if unsure of the file name. The reviewer will then perform an @PRT,F of the file and verify that the ACR ACRNA is attached.

Fixes

TELCON Remote Concentrator

Secure the TELCON file containing Remote Concentrator and DCP load elements in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.720.00 V0000611 CAT II The Site Unique Configuration File

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.8.2

Vulnerability The Site Unique Configuration file (SYS$LIB$*STRPARM) is not secured in accordance with the standard.

Vulnerability Discussion If the Site Unique Configuration file is not secured, unauthorized users could modify sensitive information concerning offsite file identifiers, site unique tape devices, automated job identifiers, print routing information, etc. Erroneous or malicious modifications could result in the disruption of service to end users, improper offsite storage, or termination of critical system jobs.
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.

Checks

Site Configuration File

The reviewer will do a @PRT, F SYS$LIB$*STRPARM and verify that the ACR ACRRO is attached to the file. Sites not supported by SSO Montgomery may use additional files with configuration parameters. Alternately, an ACR that restricts update to authorized users can be used. This information is available in the SRRPRT.

Fixes

Site Configuration File

Secure the Site Unique Configuration file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.730.00 V0000612 CAT II Critical Sightline and Torch files Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.7.1

Vulnerability Critical Sightline and Torch files are not secured in accordance with the standard.

Vulnerability Discussion If critical Sightline and Torch files are not secured, unauthorized users could delete or modify fee for service information. These actions could result in the processing of erroneous billing charges to supported customers.
For DISA sites, The SA will ensure Sightline and Torch files are properly secured to protect them from access by unauthorized personnel.

Checks

Sightline and Torch Files

The reviewer will verify that all Sightline and Torch files are protected with an ACR. This information is available in the SRRPRT. Sightline and Torch files include: DATAMETRICS*DENVER, DATAMETRICS*TORCH, and one DATAMETRICS*PMS-xxxx (where xxxx are the domain codes). These files will have ACR DEVP99 attached. Additionally Torch and Sightline files including SYS$LIB$*TORCH, SYS$LIB$*TORCH-RPTS, SYS$LIB$*TORCH-AUTO, SYS$LIB$*SIGHTLINE, and SIGHTLINE*RUNS will have ACR PUBRD, Owner -CHAMELEON- attached to them.

Fixes

Sightline and Torch Files

Secure Sightline and Torch files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.740.00 V0000635 CAT II The QUICKSTART file (SYS$*QRUNS) Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.1.2

Vulnerability The QUICKSTART file (SYS$*QRUNS) is not secured in accordance with the standard.

Vulnerability Discussion If the QUICKSTART file is not properly secured, unauthorized users could add unsecured jobs to the database that can be started with a privileged userid. These unauthorized, unsecured jobs could compromise user data or result in denial of service to the customer.
The SA will ensure the QUICKSTART file SYS$*QRUNS is secured with ACR ACRNA to protect it from access by unauthorized personnel.

Checks

QUICKSTART File

The reviewer will verify that the file SYS$*QRUNS has the ACR ACRNA attached. The reviewere will do an @PRT,F SYS$*QRUNS to see if ACRNA is attached. If a system is running NJZMON, then this file is on the system and has to be protected. This information is available in the SRRPT.

Fixes

QUICKSTART File

Secure the QUICKSTART file in accordance with the standard.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.750.00 V0000560 CAT II DFAS LOUIS II/LOUIS LINK Master File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.4.2

Vulnerability Access to the DFAS LOUIS II/LOUIS LINK Master file is not restricted in accordance with the standard.

Vulnerability Discussion LOUIS II/LOUIS LINK is a powerful retrieval utility and the Master file contains user-IDs that can execute this utility. If access to the Master file is not restricted, unauthorized users could be added to this file and allowed to use this utility to obtain sensitive database information.
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.

Checks

Louis/Louis Link Master Files-

The reviewer will, for ALN systems, use the SRRFSM to identify what DMS$77xx files are on the system so the DFAS Field Organization ALNs can be identified. Then the reviewer will do an @PRT, F 0QU0<Field Organization ALN>*MASTER to see if the file has an ACR on it. If there are multiple DFAS Field Organizations on the system, the will verify that each ACR is unique. The reviewer will also verify that the restrictions on this ACR are as follows: Read access can be PUBLIC, but Delete and Write Access should be restricted to an L Shred Account. The reviewer will then look at the account summary file and verify who has access to each L Shred Account. For DNMC and DFAS-IN systems, the reviewer will check the Toolkit SRRCOM to verify that LOUIS II/LOUIS LINK is installed on the system. If installed, the LOUIS II/LOUIS LINK Master file will be 0QU09042*MASTER and it should have an ACR attached that restricts access to authorized Application Administrators. This information is available in the SRRPRT.

Fixes

Louis/Louis Link Master File

Restrict access to the LOUIS II/LOUIS LINK Master file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.760.00 V0002673 CAT II Unauthorized users can access the LOUIS II/LOUIS L

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.4.1

Vulnerability Unauthorized users can access the LOUIS II/LOUIS LINK software. (ALN Sites Only)

Vulnerability Discussion On Access and Location Number (ALN) systems supporting both DFAS Field Organizations and non-DFAS Field Organizations, the LOUIS II/LOUIS LINK software is only authorized and licensed for DFAS Field Organization users and access to this software is controlled by ALN specific Master files. If Master files are not established for the non-DFAS Field Organization ALNs and the default ALN 9042, or if they are not properly populated with the basic LOUIS II/LOUIS LINK syntax statements, unauthorized users could execute this software without the proper licensing agreement.
The IAO will ensure default non-Field Organization Master Files exist on those systems where Field Organization workload coexists with non-Field Organization workload.
The IAO will ensure the default Master File 0QU09042*MASTER exist on system.

Checks

LOUIS/LOUIS Link Default

The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are catalogued. The will do an @PRT, F 0QU09042*MASTER to see if this file is catalogued. Also, the will verify that these files are not empty and that they contain the basic LOUIS II/LOUIS LINK syntax statements. If these files are not catalogued on the system or if they are not set up correctly, this is a finding.
NOTE: If site personnel are performing exempt queries on behalf of DFAS requirements, the 0QU09042*MASTER file can contain site personnel userids. This information is available in the SRRPRT.
<br>The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are restricted to ACRRO. The will do an @PRT, F 0QU09042*MASTER to see if this file is restricted to ACRRO.

LOUIS/LOUIS Link Default

The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are catalogued. The will do an @PRT, F 0QU09042*MASTER to see if this file is catalogued. Also, the will verify that these files are not empty and that they contain the basic LOUIS II/LOUIS LINK syntax statements. If these files are not catalogued on the system or if they are not set up correctly, this is a finding.
NOTE: If site personnel are performing exempt queries on behalf of DFAS requirements, the 0QU09042*MASTER file can contain site personnel userids. This information is available in the SRRPRT.
<br>The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are restricted to ACRRO. The will do an @PRT, F 0QU09042*MASTER to see if this file is restricted to ACRRO.

Fixes

LOUIS/LOUIS LINK default

Ensure LOUIS II/LOUIS LINK Master files are established for each non-DFAS Field Organization ALN and the default ALN 9042. Verify that these Master files are not empty and that they contain the basic LOUIS II/LOUIS LINK syntax statements.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.770.00 V0002674 CAT II Non-DFAS LOUIS II/LOUIS LINK Master Files

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.4.1

Vulnerability The non-DFAS LOUIS II/LOUIS LINK Master files are not secured in accordance with the standard. (ALN Sites Only)

Vulnerability Discussion On Access and Location Number (ALN) systems supporting both DFAS Field Organizations and non-DFAS Field Organizations, if the non-DFAS Field Organization LOUIS II/LOUIS LINK Master files are not properly secured, these files could be deleted or modified and unauthorized users could execute this software without the proper licensing agreement.
The IAO will ensure default non-Field Organization Master Files is secured with ACR ACRRO to protect them from modification by unauthorized personnel.

Checks

LOUIS/LOUIS Link Default

The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are catalogued. The will do an @PRT, F 0QU09042*MASTER to see if this file is catalogued. Also, the will verify that these files are not empty and that they contain the basic LOUIS II/LOUIS LINK syntax statements. If these files are not catalogued on the system or if they are not set up correctly, this is a finding.
NOTE: If site personnel are performing exempt queries on behalf of DFAS requirements, the 0QU09042*MASTER file can contain site personnel userids. This information is available in the SRRPRT.
<br>The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are restricted to ACRRO. The will do an @PRT, F 0QU09042*MASTER to see if this file is restricted to ACRRO.

LOUIS/LOUIS Link Default

The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are catalogued. The will do an @PRT, F 0QU09042*MASTER to see if this file is catalogued. Also, the will verify that these files are not empty and that they contain the basic LOUIS II/LOUIS LINK syntax statements. If these files are not catalogued on the system or if they are not set up correctly, this is a finding.
NOTE: If site personnel are performing exempt queries on behalf of DFAS requirements, the 0QU09042*MASTER file can contain site personnel userids. This information is available in the SRRPRT.
<br>The reviewer will check the Toolkit SRRCOM to see if LOUIS II/LOUIS LINK is installed on the system. For contractual reasons, LOUIS II/LOUIS LINK should only be installed on systems supporting DFAS Field Organization workload. If a system is supporting DFAS Field Organizations and SBLC workload, the reviewer will use the SRRFSM and check the DMS$<ALN>* and <MAPPER QUALIFIER>*HLDMAP files to identify all valid non-DFAS Field Organization ALNs on the system. The reviewer will do an @PRT,F 0QU0<ALN>*MASTER file for all the Non-DFAS Field Organization ALNs to see if these files are restricted to ACRRO. The will do an @PRT, F 0QU09042*MASTER to see if this file is restricted to ACRRO.

Fixes

LOUIS/LOUIS LINK Default Maste

Secure the non-DFAS LOUIS II/LOUIS LINK Master files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.780.00 V0002675 CAT II LOUIS II/LOUIS LINK non ALN Default Master File

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 5.4.1

Vulnerability The default LOUIS II/LOUIS LINK Master file is not secured in accordance with the standard (ALN Sites Only).

Vulnerability Discussion On Access and Location Number (ALN) systems supporting both DFAS Field Organizations and non-DFAS Field Organizations, if the default (ALN 9042) LOUIS II/LOUIS LINK Master file is not properly secured, this file could be deleted or modified and unauthorized users could execute this software without the proper licensing agreement.
The IAO will ensure the default Master File 0QU09042*MASTER is secured with ACR ACRRO to protect it from modification by unauthorized personnel.

Checks

Lous/Lous Link OQU09042*Master

The reviewer will verify that the default LOUIS II/LOUIS LINK file OQU09042*MASTER is restricted to ACRRO. This information is available in the SRRPRT.

Fixes

Lous/Lous Link OQU09042*Master

Secure the default (ALN 9042) LOUIS II/LOUIS LINK Master file in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.790.00 V0002676 CAT II File JX$$0000*00 Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 4.1.6

Vulnerability The Standard Security Profile file is not secured in accordance with the standard.

Vulnerability Discussion The Standard Security Profile file contains the approved STIG compliant profiles and if this file is not properly secured, unauthorized changes could be made to the standard profiles. This can result in users being improperly profiled and possibly given more capabilities than authorized for their particular job.
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.

Checks

File JX$$0000*00 Access

The reviewer will do a @PRT, F JX$$0000*00 to verify that the ACR ACRRO is attached. This information is available in the SRRPRT.

Fixes

File JX$$0000*00 Access

Attache the ACR ACRRO to the Standard Security Profile file, JX$$0000*00.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.800.00 V0000662 CAT II NAPZ00 Terminal Configuration File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.4.2

Vulnerability The NAPZ00 Terminal Configuration file is not secured in accordance with the standard. (ALN Sites Only).

Vulnerability Discussion The NAPZ00 Terminal Configuration file is used to match terminal-IDs with Position Identifier (PID) numbers, and assigns these terminals to specific Automated Information Systems (AISs). If this file is not properly secured, changes could be made and unauthorized users could gain access to AISs.
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.

Checks

S103.800.00 NAPZ00 File Access

The reviewer will perform an @PRT,F on the NAPZ00 Terminal Configuration file, SYS$*PMSCBP104FNP, and verify that it is secured with the ACR ACRRO or a similar site unique ACR to protect it from modification by unauthorized personnel.

Fixes

NAPZ00 File Access

Attach the ACR ACRRO, or a similar site unique ACR to protect it from modification by unauthorized personnel, to the NAPZ00 Terminal Configuration file, SYS$*PMSCBP104FNP.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.810.00 V0000663 CAT II CSC and CDI File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.4

Vulnerability The file containing the Client System Component (CSC) and Client Direct Interconnect (CDI) parameter elements is not secured in accordance with the standard.

Vulnerability Discussion The CSC and CDI parameter elements contain settings, which are used to limit CSC and CDI commands to authorized users. If this file is not properly secured, any user could modify these parameter elements and remove or relax existing security controls.
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.

Checks

CSC and CDI File Access

The reviewer will check the SYS$LIB$*RUN$.CSC element and the SYS$LIB$*RUN$.CDI element to locate where the local CSC and CDI parameters, if any, are stored. If there are local parameters and they are not found in the start rustreams the reviewer will perform an @PRT, F on the files that contain the parameters. For ALN and DFAS-IN systems these files are SYS$LIB$*CSC and SYS$LIB$*STRPARM. The reviewer will verify that the owner is -CHAMELEON- and the ACR is PUBRD or other restrictive ACRs are attached to the files. This information is available in the SRRPRT.

Fixes

CSC and CDI File Access

Secure the file containing the CSC and CDI parameter elements in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.820.00 V0000664 CAT II UOSS File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.10.2

Vulnerability The Unattended Operations Support Software (UOSS) Control file is not secured in accordance with the standard.

Vulnerability Discussion The UOSS Control file contains the userid/password that is used to automatically bring the system up and down, and recover from system aborts. This userid is a highly privileged userid and must be protected from possible compromise.
The SA will ensure the UOSS Control file (SYS$LIB$*UOSS$C) is secured with the ACR ACRNA to protect it from access by unauthorized personnel.

Checks

UOSS File Access

The reviewer will perform an @PRT,F on the UOSS Control file, SYS$LIB$*UOSS$C, and verify that the ACR ACRNA is attached.

Fixes

UOSS File Access

Attach the ACR ACRNA to the UOSS Control file, SYS$LIB$*UOSS$C.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.830.00 V0000665 CAT II AAP IAO File Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.2

Vulnerability The Automated Account Process (AAP) AIAO files are not secured in accordance with the standard.

Vulnerability Discussion The AAP IAO files contain the input userids and accounts for the AAP utility. If these files are not properly secured, they could be updated and unauthorized userids could be added to accounts on the system.
The SA will ensure the AAP IAO files are secured with an ACR to protect them from access by unauthorized personnel.

Checks

AAP IAO File

The reviewer will perform an @PRT,F JX$$<ALN>*USERID files and verify that they are protected with an ACR.

Fixes

AAP IAO Files

Secure the AAP IAO files in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.840.00 V0002677 CAT II AAP IAO File Access Q Shred Accounts

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.2

Vulnerability Unauthorized users have access to the AAP IAO files.

Vulnerability Discussion The AAP AIAO files are controlled by Access Control Records that are restricted to (ALN)JX1Q shred accounts. If unauthorized users are granted access to these (ALN)JX1Q shred accounts, they could update the AAP IAO files and give users access to accounts without proper authority or justification.
The SA will ensure only authorized IAOs have access to their respective AAP IAO files.

Checks

AAP IAO File Access

The reviewer will perform an @PRT,F JX$$<ALN>*USERID files to find the ACR attached to the file. The reviewer will then look at the Toolkit ACR Restrictions Report to see what accounts the ACRs are restricted to. The accounts should be <ALN>JX1Q shred accounts. Next the reviewer will look at the Toolkit Account Shred Report to see what userids have access to the <ALN>JX1Q shred accounts. The reviewer will verify that access is restricted to subadministrators.

Fixes

AAP IAO File Access

Ensure only authorized IAOs have access to their respective AAP ISSO file by means of an (ALN)JX1Q shred account.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.850.00 V0000666 CAT II ARP Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.1

Vulnerability Unauthorized users have access to the Automated Reset Process (ARP) program.

Vulnerability Discussion The ARP program is restricted to authorized TASOs and SAs under a Q shred account. If unauthorized users are given access to a Q shred account and can execute this program; userids and passwords can be reset or enabled without proper authority and user verification.
The SA will ensure only authorized TASOs and SAs have access to the respective Q shred accounts.

Checks

ARP Access

The will use the Toolkit Account Shred Report to see what <ALN/AIS/GANG>Q accounts are on the system. The reviewer will verify that only subadministrators have access to the <ALN>JX1Q accounts and only subadministrators/TASOs have access to the <ALN/AIS/GANG>Q accounts. The IAO or SA will have a list of authorized TASOs on file. Authorized SAs will already have Appointment Letters on file. If unauthorized users have access to these Q shred accounts this is a finding.

Fixes

ARP Access

Review all userids that are under a Q shred account to ensure only authorized users have access to the ARP program.
Remove all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.854.00 V0003961 CAT III Authorized TASO List

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.3.6.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.1.1

Vulnerability The IAO does not have a list of all authorized TASOs who have access to ARP.

Vulnerability Discussion If the IAO does not have a list of all authorized TASOs there is no way to validate that a specific user is an authorized TASO and needs to have access to the ARP.
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.

Checks

ARP Access List

The reviewer will interview the IAO and verify that there is a list of all TASOs and SAs that have access to the ARP utility.

Fixes

ARP Access List

The IAO will maintain a current list of all TASOs authorized to have access to ARP.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.856.00 V0003962 CAT II The file containing the DFAS ARP IAO Runstream

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.2.1.1

Vulnerability The file containing the DFAS ARP AIAO runstream is not secured in accordance with the Unisys STIG.

Vulnerability Discussion If unauthorized users can update the DFAS ARP AIAO runstream, they could grant unauthorized privileges to users. This can lead to the corruption of user data, the compromise of user data, or denial of access to the system.
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.

Checks

DFAS ARP Runstream

The reviewer will verify that the file containing the DFAS ARP runstream is protected by an ACR that restricts access to the appropiate Q shred account.

The DFAS ARP, if used, is called DESET and is located in SYS$LIB$*ALTLIB. The DESET IAO runstream that is executed by AMS via the DESET program is located in the 0JX0<ALN>*PUTLD file. The DESET runstream contains Field Organization site code information and password construction criteria so the file must be protected with an ACR that is restricted to the particular DFAS Field Organization IAO Q shred account. The reviewer will verify that the DESET runstream is located in the 0JX0<ALN>*PUTLD file. The reviewer can do this by performing an @PRT,T 0JX0<ALN>*PUTLD.DESET. If the runstream is found, the reviewer will perform an @PRT,F 0JX0<ALN>*PUTLD to see what ACR is attached to the file. The will then review the Toolkit ACR Restrictions Report to see what restrictions are on this ACR. The ACR will be unique for each DFAS Field Organization using DESET and will be restricted the DFAS Field Organization IAO Q shred account. The reviewer will then use the Toolkit Account Shred Report to see what user-IDs have access to the <ALN>JX1Q accounts. Only the DFAS Field Organization IAO will have access to the respective IAO Q shred account. If the PUTLD file contains the DESET runstream and is not protected an ACR, if the ACR is set up incorrectly, or if unauthorized users have access to the <ALN>JX1Q account, this is a finding.

Fixes

DFAS ARP Runstream

Secure the file containing the DFAS ARP IAO runstream in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.860.00 V0000576 CAT II Userid/password combinations Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.2

Vulnerability Userid/password combinations are not adequately secured from access by unauthorized personnel.

Vulnerability Discussion Having userid/password combinations in clear text on the system in unprotected files, Operating Instructions, or other unsecured documentation provides a means for unauthorized personnel to gain access to the system.
The IAO will ensure files containing the runstreams are used in the DDP-FJT SUBMIT runs or other files containing userid/password combinations are protected with an ACR, and the userid within the card reader simulated runstream have a run mode of Batch only.

Checks

Clear Text Passwords

The reviewer will use the Toolkit SRRFSM file and look for suspicious files. For example, search on items like DBM, FTP, USERS, SECURITY, SEC, RPC, TOOL, etc. Then reviewer can use @FLIST to display the files content and look through it for user-ID password combinations. Also, the reviewer will review Operator Instructions, cheat sheets on individual desks, configuration diagrams, etc. If clear text user-IDs/passwords are found written or in unprotected files, this is a finding.

Fixes

Clear Text Passwords

Protect files containing clear text passwords as described in the Unisys STIG and instruct personnel that clear text combinations of userids and passwords are treated For Official Use Only and properly secured.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.00 V0004029 CAT II There is not an ADMIN statement in the CMS1100 con

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.1.4

Vulnerability There is not an ADMIN statement in the CMS1100 configuration or it is not configured in accordance with the Unisys STIG.

Vulnerability Discussion There is no ADMIN statement in the CMS1100 configuration, or it is not configured correctly. The default option for the CMS1100 control access password is no password required. This can lead to a corruption of the CMS1100 configuration by the issuing of configuration modification commands by unauthorized users or the denial of service by the issuance of commands to terminate the communications software CMS1100. Additionally TELNET logging must be enabled by this statement and termination confirmation must be enabled to block accidental termination of the communications software.
The SA will ensure there is an ADMIN statement in the CMS 1100 Configuration.
The SA will ensure the second subfield of the SECURITY field does not have a value of NOT-REQUIRED.
The SA will ensure the second subfield of the LOG-TELNET-OPENS field is set to YES.
The SA will ensure the second subfield of the VERIFY-TERM-COMMANDS field is set to YES.

Checks

CMS 1100 ADMIN

The reviewer will verify that ADMIN statement in the CMS 1100 configuration file is exists and is of the following format. There will be an ADMIN statement in the configuration file and it should look like the following:

```
ADMIN SECURITY,PASSWORD,xxxxxxx  KEYIN-NAME,CMS  ;
      LOG-TELNET-OPENS,YES   VERIFY-TERM-COMMANDS,YES
```

On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.

NOTE: The second SECURITY subfield can be NO-ACCESS or PASSWORD. If PASSWORD, the actual password will follow DISA password construction rules and will be changed every 90 days. LOG-TELNET-OPENS will be set to YES and VERIFY-TERM-COMMMANDS will be set to YES.

Fixes

CMS 1100 ADMIN

Create or modify the ADMIN statement in the CMS1100 configuration in accordance with the Unisys STIG and implement the modified configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.01 V0004030 CAT III CMS1100 APPLICATION Statements PID-POOL

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.2

Vulnerability There are APPLICATION statements in the CMS1100 configuration with PID POOL fields.

Vulnerability Discussion When PID pools are configured, CMS1100 will assign a pool PID, Position Identifier, to a client whose end user id (terminal id) does not match a configured end user id on a PID configuration statement within CMS1100. This would make it difficult to trace the source of session that performs an unauthorized access to TIP.
The SA will ensure the PID-POOL Field is not used on the APPLICATION Statement.

Checks

CMS 1100 APPLICATION

The reviewer will verify that no APPLICATION statement in the CMS 1100 configuration file contains a PID-POOL field. On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.

Fixes

CMS 1100 APPLICATION

Remove all PID-POOL fields from APPLICATION statements within the CMS1100 configuration and implement the CMS1100 configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.02 V0004031 CAT III CMS1100 PID Statements with PID-POOL

8500.2 IA Control: DCBP-1 References:

Vulnerability There are PID statements in the CMS 1100 configuration with PID-POOL fields.

Vulnerability Discussion When PID pools are configured, CMS1100 will assign a pool PID, Position Identifier, to a client whose end user id (terminal id) does not match a configured end user id on a PID configuration statement within CMS1100. This would make it difficult to trace the source of session that performs an unauthorized access to TIP.
The SA will ensure the PID-POOL field of the PID statement is not used.

Checks

CMS 1100 PID

The reviewer will verify that no PID statement in the CMS 1100 configuration file contains a PID-POOL field. On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.

Fixes

CMS 1100 PID

Remove all PID-POOL fields from PID statements within the CMS1100 configuration and implement the CMS1100 configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.03 V0004032 CAT IV CMS1100 PROCESS,CSACSU with INTERNET-ADR

8500.2 IA Control: DCBP-1 References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.4.1

Vulnerability There is a PROCESS statement with a PROCESS,CSACSU field and an INTERNET-ADR field in the CMS 1100 configuration.

Vulnerability Discussion If there is a PROCESS statement within the CMS1100 configuration with a PROCESS,CSACSU field and an INTERNET-ADR field, anyone with a Unisys terminal emulator that knows the IP address of the Unisys system can open session to CMS1100 command process. If this user also knows the CMS1100 command password, they can corrupt the CMS1100 configuration with dynamic configuration statements or create a denial of service by initiating a shutdown of the communications software CMS1100.
The SA will ensure, if there is a “PROCESS,CSACSU” statement in the configuration, it does not have an INTERNET-ADR field.

Checks

CMS 1100 PROCESS,CSACSU

The reviewer will verify that if there is a PROCESS,CSACSU statement in the CMS 1100 configuration file it does not contain an INTERNET-ADR field. On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.

Fixes

CMS 1100 PROCESS,CSACSU

Remove the INTERNET-ADR field from any PROCESS statements containing the PROCESS,CSACSU field in the CMS1100 configuration and implement the modified configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.04 V0004033 CAT IV CMS 1100 TSAM example Password Used

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.4.2

Vulnerability There is a PROCESS statement for TSAM in the CMS 1100 configuration that uses a TSAM password in the PASSWORD field that is found in example configurations within Unisys documentation.

Vulnerability Discussion Use of example passwords can lead to use of the TSAM interface by an unauthorized user. This can cause a denial of service by stopping authorized users from connecting to the TSAM interface. Additionally CMS internal tables and buffers can be read leading to the compromising of data.
The SA will ensure no password from an example configuration is used on a CMS 1100 configuration statement.

Checks

CMS 1100 TSAM Passwords

The reviewer will verify that, if there is a PROCESS statement in the CMS 1100 configuration file with a TYPE field of TSAM, the PASSWORD field does not contain a password value from a configuration example. The PROCESS statements with a TYPE file of TSAM should look like the following:

```
PROCESS,CPFTP    TYPE,TSAM         PASSWORD,xxxxxx ;
PROCESS,DDP      TYPE,TSAM         PASSWORD,yyyyyy  ;
PROCESS,DEP1     TYPE,TSAM         PASSWORD,zzzzzz  ;
```

The actual passwords used in the PASSWORD subfield will not match any of those found in example configurations within Unisys documentation. If these example passwords are being used, this is a finding.
NOTE: These TSAM passwords must match the corresponding product TSAM password (for example, cpFTP) or the PROCESS will not come up properly. Care should be taken when changing these passwords to make sure it is done properly in both places. On SSO Montgomery supported sites, this file is found in SYS$LIB$*FEPLOAD.CONFIG.

Fixes

CMS 1100 TSAM Passwords

Change the offending TSAM passwords in the CMS1000 configuration to unique passwords following the password construction rules and implement the modified configuration. This must be done in synchronization with the other software component that uses the modified TASM process.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.05 V0004034 CAT III There is a RSI statement in the CMS 1100

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.5.2

Vulnerability There is a RSI statement in the CMS 1100 configuration that is not configured in accordance with the Unisys STIG.

Vulnerability Discussion If the RSI statement in the CMS1100 is not configured in accordance with the Unisys STIG, it will be difficult to trace the source of a violation of security.
The SA will ensure, if the RSI statement is used, it does not have a GENERIC field.
The SA will ensure, if the TIME-OUTS field of the RSI statement is used, the value of the second subfield is YES.

Checks

CMS 1100 RSI Statement

The reviewer will verify that if there is a RSI statement in the CMS 1100 configuration file it does not contain an GENERIC field. Additionally the RSI statement will have a TIME-OUTS field with the second subfield having the value of YES. On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.
EXAMPLE:

RSI TIME-OUTS,YES {other optional fields}

Fixes

CMS 1100 RSI Statement

Configure the RSI statement in the CMS 1100 configuration in accordance with the Unisys STIG and implement the modified configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.06 V0004035 CAT II SNMP-MGMT statement in the CMS 1100 configuration

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.1.6

Vulnerability There is a SNMP-MGMT statement in the CMS 1100 configuration.

Vulnerability Discussion CMS 1100 only supports SNMP version 1 and the SNMP-MGMT is the statement that turns on SNMP within CMS 1100. SNMP-MGMT version 1 is not allowed and is a Category II finding in the network STIG. Since SNMP version 1 is not allowed on the network, it must not be configured as on in CMS 1100 and is an equivalent finding.
The SA will ensure there is no SNMP-MGMT statement in the configuration.

Checks

CMS 1100 SNMP-MGNT

The reviewer will verify that there is no SNMP-MGNT statement in the CMS 1100 configuration file. On SSO Montgomery supported sites, this file is found in the element SYS$LIB$*FEPLOAD.CONFIG.

Fixes

CMS 1100 SNMP-MGMT

Remove all SNMP-MGMT statements from the CMS 1100 configuration and implement the modified configuration.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.07 V0004036 CAT III CMS 1100 Background Run Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.2.2

Vulnerability The userid used for the CMS 1100 background run is not configured in accordance with the Unisys STIG.

Vulnerability Discussion If the userid is not configured in accordance with the Unisys STIG, it can lead to unauthorized interactive access to the system using a userid having high privileges.
The SA will ensure the batch run userid for CMS 1100 background run is set up as described in this STIG.

Checks

CMS 1100 Background Userid

The reviewer will verify that the userid used for the CMS 1100 background batch run is correctly configured. The reviewer will check in SIMAN that the userid has only the following privileges.

SSADID
SSLOGER.
SSCONSOLE
SSSSCALLANY
SSRUNXOPT
SSTOKEN

Additionally, if the site has a DCP and/or there exist a PROCESS,RSBCSU STATUS,UP statement in its configuration, the following additional privileges are allowed.

SSSMOQUE
SSBPFC
SSBRWK
SSBYCL
SSBAFC
SSBKUP
SSBYPASSOWNR
SSBYCOMP

The userid will have only the following interfaces allowed.

MCODE$
PB$CON
TF$KEY
CONNECT$TIP
CMS$REG
MQF$
RSI$
RT$INT
RT$PID
TIP$SM
TIP$TALK
TIP$XMIT

If any privileges or interfaces other than those listed are allowed the userid this is a finding.
Finally the userid needs to create owned files so the “User to create only unowned files” flag will be cleared and only the only run mode allowed will be batch.

Fixes

CMS 1100 Userid

Configure the CMS 1100 background run userid in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.08 V0004037 CAT II The Account used for the CMS 1100 Background Run

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.3

Vulnerability The account used for the CMS 1100 background run is not configured in accordance with the Unisys STIG.

Vulnerability Discussion If the CMS 1100 background run account is not configured in accordance with the Unisys STIG, communications performance will deteriorate and access to required files will be denied.
The SA will ensure the CMS 1100 batch run account allows Real Time Level 2.
The SA will ensure the CMS 1100 batch run account is not the Privilege Account.
The SA will ensure the CMS 1100 batch run account is an ALN exempt account.

Checks

CMS 1100 Account

The reviewer will verify that the account that the CMS 1100 background batch run executes under is correctly configured.
The reviewer will use SIMAN to view the account and verify that is allowed a maximum realtime level of 2.
The reviewer will interview the SA and find out the privileged account, the account used for tape labeling, and verify that this is not the account used for the CMS 1100 background batch run.
The reviewer will, if this is an ALN system, verify that the account is an ALN exempt account.

Fixes

CMS 1100 Account

Configure the CMS 1100 background run account in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.09 V0004038 CAT III The CMS 1100 Subsystem Userid Configuration

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.4

Vulnerability The CMS 1100 Subsystem Userid is not configured in accordance with the Unisys STIG.

Vulnerability Discussion If the CMS 1100 Subsystem Userid is not configured in accordance with the Unisys STIG, CMS 1100 will not function properly and may fail leading to a denial of service.
The SA will ensure the CMS 1100 Subsystem Userid is configured as described in this STIG.

Checks

CMS 1100 Subsystem Userid

The reviewer will verify that the userid that owns the CMS 1100 subsystem file, SYS$LIB$*CMS1100 and/or CMS1100*TEST$LIB, does not have unneeded privileges. The reviewer will use SIMAN, the Display Userid function, to verify that the following settings are correct.

Run Mode	None will be selected.
System Control Designators	None will be selected!
Processor Privilege	Read Executive GRS
Access Privilege	Trusted
Sharing Level	Application
Clearance Level	Max 0 Min 0
Privileges	SSGAP
Interfaces	DUMP$SUBSYS

Fixes

CMS 1100 Subsystem Userid

Configure the CMS Subsystem Userid in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.870.10 V0004039 CAT II CMS1100 Dynamic Update Clean Up

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 11.1.5.2

Vulnerability Actions are not being taken in a timely manner to replace a Dynamic CMS 1100 configuration change with a static configuration.

Vulnerability Discussion If dynamic updates are not replaced with static configuration changes in a timely manner, it will become difficult to determine if the dynamic change was authorized because only the time and date of the last change is displayed. Additionally if there are a large number of dynamic changes made to CMS 1100 and the running configuration is lost, it will be hard if not impossible to recreate the running configuration from the last implemented and tested static configuration. This can lead to excessive outage caused by the difficulty of recovering the configuration or a denial of service to users of the facilities for which configurations where lost.

Checks

Unisys S103.870.10

The reviewer will interview the SA to verify that there exist a policy to either revert the configuration to the static configuration that existed prior to the emergency dynamic change or to update the static configuration to reflect the dynamic change and implement the new static configuration as soon as operationally expedient.

Fixes

Convert any Dynamic CMS 1100 c

Convert any Dynamic CMS 1100 configuration changes to static changes at the earliest convenient time.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.880.00 V0007511 CAT II Host Based Intrusion Detection

8500.2 IA Control: ECID-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability SSL or SSH is used there is an available host based intrusion detection (HID) system but it is not employed.

Vulnerability Discussion SSL or SSH that terminates in the host is used and there is an available host based intrusion detection (HID) system but it is not employed.

Checks

UNISYS S103.880.00

The reviewer will interview the IAO to verify if the site is using SSL or SSH which terminates within the Unisys host and if there is a host based intrusion detection system available for Unisys systems, that the host based intrusion detection system is in use. If there is not a host based intrusion detection system available for a Unisys host this is not a finding.

Fixes

Unisys S103.880.00

Acquire and deploy a Unisys host based intrusion detection system.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.880.10 V0007512 CAT II VPN Traffic and network IDS

8500.2 IA Control: EBBD-1, EBBD-2, EBBD-3

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability The VPN terminates in a manner that precludes the scanning by the Intrusion Detection System of traffic carried by the VPN.

Vulnerability Discussion If the VPN terminates such that its traffic is not visible to a network Intrusion Detection System there will be no intrusion detection scans made for this traffic defeating the ability to detect intrusion attempts before they can compromise a system or network.

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).

Checks

Unisys S103.880.10

The reviewer will interview the IAO to very that all VPN traffic is visible to the network Intrusion Detection System.

Fixes

Unisys S103.880.10

Modify the network structure so that all VPN traffic is visible to the network Intrusion Detection System.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.880.20 V0007513 CAT I FTP and Telnet from Outside the Enclave

8500.2 IA Control: EBRU-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability FTP or telnet from outside the enclave is being permitted into the enclave without required mitigating controls.

Vulnerability Discussion Unencrypted connections form outside the enclave into the enclave can lead the compromise of userids, passwords and sensitive data.

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).

Checks

Unisys S103.880.20

The reviewer will interview the IAO to verify that all FTP and telnet remote access to the enclave is in accordance with the Enclave and Unisys STIGs.

Fixes

Unisys S103.880.20

Modify the network and procedure so that all FTP and telnet remote access to the enclave is in accordance with the Unisys and Enclave STIGs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.880.30 V0007514 CAT II FTP and Telnet Passwords

8500.2 IA Control: IAIA-2, IAIA-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability Passwords of userids used for FTP and telnet by an individual are not configured to force changing every 90 days.

Vulnerability Discussion Passwords used in FTP and telnet are transmitted in clear text. This makes them vulnerable to compromise. Forcing the change of passwords every 90 days mitigates the problem by decreasing the size of the window of exposure for a compromised password.

The IAO will ensure all user FTP userid (UID) passwords have an expiration date and the password is changed every 90 days.

Checks

Unisys S103.880.30

The reviewer will check the Toolkit Password Expiration Report to verify that all userids have their maximum password expiration set to 90 days.

This only applies to individual userids not application to application passwords, which are covered in other checks.

Fixes

Max Pass Expire

All userid password expirations should be set to 90 days except those documented in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S103.880.40 V0007515 CAT I FTP or Telnet Privileged Userids

8500.2 IA Control: EBRP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.3

Vulnerability Privileged userids are used for FTP or telnet.

Vulnerability Discussion Since FTP and telnet require clear text passwords the userid/password can easily become compromised. To minimize the impact of a compromised userid, privileged userids will not be used for FTP or telnet sign in.

The IAO will ensure under no circumstances the FTP or telnet is used with a userid (UID)/password has administrative or root privileges.

Checks

Unisys S103.880.40

The reviewer will interview the IAO to verify that owners of privileged accounts are instructed not to use the privileged accounts for FTP or telnet.

Fixes

Unisys S104.880.40

Issue non-privileged userids for use with FTP or telnet to owners of privileged userids. Instruct the users to only use the privileged userids when the privileges granted are needed and never for FPT or telnet.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.010.00 V0000699 CAT II The IAO does not have userid information

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2

Vulnerability The IAO does not have accurate and readily available information to tie a userid to a specific individual or process.

Vulnerability Discussion There can be no positive user identification unless the IAO, AIAO, or TASOs maintain complete user information and have this information readily available for the IAO.
The IAO will ensure all SAARs or their equivalent forms are available if requested.

Checks

User documentation

The reviewer will randomly select userids and verify that the IAO has current documentation on the user who owns the userid. The reviewer can use the Toolkit Random Users Report and set the parameter so it randomly selects 25 userids.

Fixes

User Documentation

Implement a revalidation process for all userids that currently exist on the system. Ensure that all new userid access requests are maintained so that positive identification of a user to a given userid can be accomplished.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.020.00 V0000713 CAT I SIMAN Administrator userids have access to batch

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.10

Vulnerability SIMAN Administrator userids have access to batch mode.

Vulnerability Discussion Administrator userids that have batch access can be used by unauthorized personnel to start jobs that increase user privileges or negate security mechanisms.
The IAO will ensure the Master userid and userids with SIMAN Administrators privilege do not have access to batch mode.

Checks

Administrative Batch Access

The reviewer will verify that no userid that has the Administrator privilege has a Run Mode of Batch. The reviewer can use the Toolkit Administrators Report to verify that none of the SIMAN administrators have batch mode. Otherwise the reviewer will execute the following sequence.

```
@SIMAN,B
 Display Userid - !ALL breakpoint  USERID*ALL ;
 @eof
```

Then the reviewer will edit the file USERID*ALL, locate “is an ADMINISTRATOR”, identify the userid, and check for Batch on the “Allow Access to” line. The reviewer will perform this on all userids that have the “is an ADMINISTRATOR” line in their report section. If any administrator has Batch on their “Allow Access to” line, this is a finding.
Note for large sites there can be more than 10,000 userids in this report.

Fixes

Administrative Batch Access

Remove batch access from all SIMAN Administrator userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.030.00 V0000706 CAT II Security Userid Profile System

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8

Vulnerability There is no security profile system in place to ensure the least privilege concept is enforced.

Vulnerability Discussion Failure to implement a profile system makes it difficult for the IAO to enforce the least privilege concept. Excessive privileges create a greater vulnerability exposure than is operationally necessary.
The IAO will ensure there is a security profile system in place to ensure the least privilege concept is enforced.

Checks

Userid Profile System

The reviewer will interview the IAO to verify that there is a role based system in use for assigning privileges, interface access, etc. If the IAO cannot explain how this is done or preferably, show a documented procedure for performing this task, this is a finding.

Fixes

Userid Profile System

Implement a security profile system that ensures the least privilege concept is enforced. The DISA standard profile system is outlined in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.040.00 V0000717 CAT II Userids are not reflective of the profile system

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8

Vulnerability Userids are not reflective of the profile system and no documentation exists to justify the discrepancy between the profile and the actual access granted.

Vulnerability Discussion By not using the standard profiles and/or not documenting the privileges required, excessive privileges may be assigned without justification. Excessive privileges create a greater vulnerability exposure than is operationally necessary.
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.

Checks

Site Security Profile Use

The reviewer will verify that the process for profiling a user and assigning privileges, interface rights, and other security related userid features is followed for actual userids.

For sites using the DISA Security profiling system and the SRR Manager Toolkit supported by SSO Montgomery.
The will use the Toolkit Profile Summary Report.
Profile 1. The only authorized Profile 1 userids are SIMAN Administrators and SRR team members. There may be two Profile 1 userids for SSO Montgomery personnel if a security problem is being actively worked. NOTE: For HMP IX 7.0 and higher, the EXEC8 and INSTALLATION userids will be Profile 1, SIMAN Administrators userids with no run modes. These userids cannot be modified or deleted by any other userid, including the Security Officer’s userid.
Profile 2. There will be an adequate number, as determined by the IAM, of userids per system across all shifts. These should belong to Technical Support personnel. The runstream Profile/OPS will be used for the Standard System Batch userid. Also, each operator or SMC personnel will have a Profile 2 userid if they actually sign on to the system.
Profile 3. There will be one modified Profile 3 for each subadministrator. The rest will belong to site application support personnel. Also, xxJF00 (Scheduler), QUIKST, xxJSTM, and VTHSRV will be modified Profile 3 userids. There are special profile runstreams for these userids.
Profile 4. Will belong to site application support personnel and will be assigned to CDA personnel if software development is being accomplished on a dedicated development domain. Functional users (non-subadministrators) will not be assigned Profile 3 or 4 userids.
Profile 5/6/7. Profile 5/6/7 userids will be assigned to high-level functional users. A modified Profile 5 will be assigned to DPS, xxEZ00, and IPF (DDP). There are special profile runstreams for these userids. On ALN systems, the number of Profile 5/6/7userids should not exceed 16% unless deemed necessary by the IAM. On the DFAS-IN system, the number of Profile 5/6/7 userids should not exceed 20% unless deemed necessary by the IAM. On DNMC systems, the number of Profile 5/6/7 userids should not exceed 35% unless deemed necessary by the IAM. This item applies to Profiles 1 – 7 if subadministrators are used on the system. If there are no subadministrators on the system, this item pertains to Profiles 1 – 9. If guidelines are exceeded without adequate justification or if deviations, not listed above, form the profiles are not documented on the user’s SAAR, this is a finding.

For sites not using the DISA profiling system and the SRR Manager Toolkit.

Select a random group of userids and verify that they are configured as described in the site’s security profiling policy. Verify that any deviations from the policy are documented on the user’s SAAR. The random selection will include administrators, high-level users and normal users. If there are userids that deviate from the profile system that do not have the deviations documented on their SAAR, this is a finding.

Fixes

Security Profile Use

Ensure all users are assigned the least privilege necessary to perform their duties. Ensure documentation is maintained for the actual access granted that is not in accordance with the user profile.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.050.00 V0000715 CAT II A subadministrator is not following the profile

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8

Vulnerability A subadministrator is not following the profile guidelines when assigning userids.

Vulnerability Discussion By not using the standard profiles and/or not documenting the privileges required, excessive privileges may be assigned without justification. Excessive privileges create a greater vulnerability exposure than is operationally necessary.
IAOs and SAs will follow the profile guidelines when assigning userids.

Checks

Subadministrator Training

The reviewer will interviewer the owners of all of the userids found in S103.040.00 to have undocumented privileges, to verify that they have an adequate understanding of the sites profiling system.

Fixes

Subadministrator Training

Brief the sub-administrator on his/her roles and responsibilities and make sure the sub-administrator assigns users with the least privilege necessary to perform their duties. If the sub-administrator continues to fail to follow the profile guidelines when assigning userids, take appropriate administrative action and/or reassign the function to another person.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.060.00 V0000714 CAT II The Sub-Administrators Profile Match

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.11

Vulnerability The sub-administrators on the system do not match the profile as specified in the Unisys STIG.

Vulnerability Discussion Subadministrator userids can modify the level of privilege assigned to their users based upon the privileges possessed by the subadministrator. If the subadministrator possesses more privileges than required, these privileges may be granted to any owned userid. Excessive privileges create a greater vulnerability exposure than is operationally necessary.
For DISA sites, the SA will ensure a subadministrator’s configuration matches the profile specified in this STIG.

Checks

Subadministrator configuration

The reviewer will use the Toolkit Subadministrator Analysis Report to see how many subadministrators are out of compliance with the STIG. If keyin groups, Interfaces, and Privileges are out of compliance and the exceptions are not documented on the SAAR, this is a finding.

Fixes

Subadministrator Configuration

Ensure that the subadministrator userids are defined with the minimum privileges necessary.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.070.00 V0000636 CAT II Subadministrator Account Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.11

Vulnerability Subadministrators are not restricted as to which accounts they can assign to userids.

Vulnerability Discussion Failure to limit subadministrators to assigning certain accounts may cause them to assign unauthorized accounts to their users. Access to unauthorized accounts could allow a user to cross ALN boundaries, gain access to privileged system processors or ACRs, or create erroneous fee for service billing information.
The SA will ensure subadministrators are being restricted to the accounts they can assign to userids.

Checks

Subadmin Account Access

The reviewer will look at the Toolkit Users Allocating Accounts Report to verify that the subadministrator is restricted to the accounts that he/she can assign. All subadministrators that are listed on the Toolkit Administrators Report will be restricted. Otherwise the reviewer will execute the following sequence.

```
 @SIMAN,B
  Display Userid - !ALL breakpoint  USERID*ALL ;
  @eof
```

Then the reviewer will edit the file USERID*ALL, locate “subadministrator”, identify the userid, and check the userid is restricted to accounts. The reviewer will perform this on all userids that have the “subadministrator” in their report section. If any subadministrators not restricted to accounts, this is a finding.
Note for large sites there can be more than 10,000 userids in this report.

Fixes

Subadmin Account Access

Limit the accounts for each subadministrator to those appropriate for that site.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.080.00 V0000637 CAT II Subadministrator Account Existence

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.11

Vulnerability The list of accounts available to a subadministrator contains obsolete or invalid accounts.

Vulnerability Discussion If the list of accounts that a subadministrator can assign contains obsolete accounts, erroneous fee for service data could be generated, resulting in faulty billing information. If this list contains invalid or erroneous accounts, unauthorized users may be given access to another sites information or data.
The SA will ensure the list of accounts available to a subadministrator consist of valid accounts.

Checks

Subadministrator Account Exist

The reviewer will look at the Toolkit Users Allocating Accounts Report to see what accounts the subadministrator can assign. Then verify that the accounts are not obsolete or invalid. If there are an excessive number of invalid or obsolete accounts, this is a finding.

If the Toolkit is not used, reviewer will execute the following sequence.

```
@SIMAN,B
 Display Userid - !ALL breakpoint  USERID*ALL ;
 @eof
```

Then the reviewer will edit the file USERID*ALL, locate “subadministrator”, identify the userid, and check the userid is restricted accounts against a summary account report to verify that the accounts are valid and not obsolete. If there are an excessive number of invalid or obsolete accounts, this is a finding.

Fixes

Subadmin Account Review

The IAO should periodically review each subadministrators list of accounts to ensure only valid accounts are identified.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.090.00 V0000615 CAT II Subadministrator Project-ID Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.11

Vulnerability Subadministrators are not restricted as to which project-IDs they can assign to userids. (ALN Sites Only)

Vulnerability Discussion Failure to limit subadministrators to assigning certain project-IDs to their users may present aggregation of data threats in an ALN environment.
The SA will ensure subadministrators are restricted to the project-IDs they can assign to userids.

Checks

Subadminstrator Project-ID Acc

The reviewer will look at the Toolkit Users Allocating Project-ID Report to verify that the subadministrator is restricted to the project-IDs that they can assign. All subadministrators that are listed on the Toolkit Administrators Report will be restricted.
Otherwise the reviewer will execute the following sequence.

```
@SIMAN,B
 Display Userid - !ALL breakpoint  USERID*ALL ;
 @eof
```

Then the reviewer will edit the file USERID*ALL, locate “subadministrator”, identify the userid, and check the userid is restricted to project-IDs. The reviewer will perform this on all userids that have the “subadministrator” in their report section. If any subadministrators are not restricted to project-IDs, this is a finding.
Note for large sites there can be more than 10,000 userids in this report.

Fixes

Subadministrator Project-ID Ac

Limit the project-IDs for each subadministrator to those appropriate for that site.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.100.00 V0000616 CAT II Subadministrator Valid Project-IDs

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.11

Vulnerability The list of project-IDs available to a subadministrator contains obsolete or invalid project-IDs. (ALN Sites Only)

Vulnerability Discussion If the list of project-IDs that a subadministrator can assign contains obsolete or invalid project-IDs, erroneous fee for service data could be generated, resulting in faulty billing information. If the list contains erroneous project-IDs, unauthorized users could obtain access to another sites information or data, or obtain exempt status in an ALN environment.
The SA will ensure the list of project-IDs available to a subadministrator consist of valid project-IDs.

Checks

Subadministrator Valid Project

The reviewer will look at the Toolkit Users Allocating Project-IDs Report to see what project-IDs the subadministrator can assign. The reviewer will check to see if any project-IDs are obsolete or invalid. If there are an excessive number of invalid or obsolete project-IDs, this is a finding.

Fixes

Subadministrator Valid Project

Remove any invalid or obsolete project-IDs from the subadministrators project-ID assignment list..

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.110.00 V0000574 CAT III Userids used to start batch jobs Batch Only

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.2.3

Vulnerability The standard userids used to start batch jobs are not limited to batch only access.

Vulnerability Discussion The userids used to start batch jobs on the system are highly privileged and if access to Demand and TIP mode is not restricted, they could be used by unauthorized personnel to gain access to the system.
The SA will ensure standard userids used to start batch jobs on the system are limited to batch only access.

Checks

Standerd Batch Userid

The reviewer will sign on to the system in Display CONS mode and do a T,B D. The reviewer spot-check jobs like MCB, CMS, PDQ, PSERVR, TAS, DDN, PPC, DDPFJT, etc., using the RC keyin, to see if a standard userid is being used to start the run. The reviewer will then look at the Toolkit SRRALL to verify what attributes these userids have. These userids will only have Batch mode. If they have access to Demand or TIP, this is a finding.
IF the Toolkit is not used the reviewer will execute the following sequence:

```
@SIMAN,B
 Display Userid - !ALL breakpoint  USERID*ALL ;
 @eof
```

Then the reviewer will edit the file USERID*ALL, locate each userid found by the RC keyins and verify that it only has batch mode.
NOTE: MAPPER system batch userids can have access to TIP as well as Batch so the account field is displayed in the userid record.

Fixes

Standard Batch Userid

Remove the Demand and TIP access flags from these standard userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.120.00 V0000581 CAT I Unauthorized userids Activated response CONS

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.7.1.4

Vulnerability Unauthorized userids have activated response CONS mode.

Vulnerability Discussion Activated response CONS mode allows a user to intercept and enter certain message groups intended for the primary system console. This can result in erroneous replies to system messages or the unauthorized entry of operator keyins. These actions could affect system processing, availability of system resources, and/or result in denial of service to the users.
The SA will ensure userids do not have ACTIVE RESPONSE CONS mode.

Checks

Active Response CONS

The reviewer will look at the Toolkit Activated Response CONS Report to find out if any user has access to activated response CONS mode. This includes disabled user-IDs as well. If a user has activated response CONS, this is a finding.
IF the Toolkit is not used the reviewer will execute the following sequence.

```
 @SIMAN,B
  Display Userid - !ALL breakpoint  USERID*ALL ;
  @eof
```

Then the reviewer will edit the file USERID*ALL and locate “Response Message”. If “Response Message” is found, this is a finding.

Fixes

CONS Active Response

Ensure no userid has activated response CONS mode.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.124.00 V0004040 CAT I Unauthorized userids have response CONS mode.

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1

Vulnerability Unauthorized userids have response CONS mode.

Vulnerability Discussion Response CONS mode allows a user to intercept consol queries initiated by a CONS action taken by this user. This can lead to denial of service when the user responds to a system validation request caused by a command given by the user via CONS to the system that would be fatal to the system.
The SA will ensure RESPONSE CONS are limited to Profile 1 and 2 userids.

Checks

Response CONS

The reviewer look at the Toolkit CONS Report verify that no Profile 3 through Profile 9 user has access to response CONS mode.

Fixes

Response CONS

Remove responce CONS mode from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.130.00 V0000716 CAT II SIMAN Environment Not Properly Configured

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.3.2

Vulnerability The SIMAN environment is not properly configured on the system.

Vulnerability Discussion Failure to configure the SIMAN environment in accordance with the Unisys STIG may deactivate security mechanisms, which could affect the operation of the security environment. This can create vulnerabilities that may jeopardize the operating system environment and customer data.
The SA will ensure the SIMAN environment is properly configured on the system.

Checks

SIMAN Environment

The reviewer will look at the Toolkit SIMAN Environment Report to see if there are any discrepancies. The reviewer can also at the Toolkit SRRENV file to verify that the SIMAN environment is set up correctly.
If the toolkit is not used, the reviewer can enter SIMAN, follow the menu to the SIMAN Environment and display the SIMAN Environment verifying that the following settings are followed for all 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)

With the following additional settings in level HMP IX 8.1 and above.

Traditional Authentication Allowed (OFF)
Retain Clear Text Passwords (OFF)
Open Session Control (OFF)

Fixes

SIMAN Environment

Configure the SIMAN environment in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.140.00 V0000718 CAT II Executive Interfaces and Privilegleges Secured

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.4

Vulnerability Security related Executive Interfaces and Privileges are not secured on the system.

Vulnerability Discussion Executive Interfaces and Privileges provide the ability to secure operating system functions. Failure to secure certain Executive Interfaces and Privileges compromises system integrity.
The IAO will ensure security related Executive Interfaces are secured on the system.
The SA will ensure Interfaces are enforced or always enforced as stipulated in the Unysis STIG.

Checks

Enforced Privs and Interfaces

The reviewer will look at the Toolkit System Privs Un/Enforced Report to verify that no Interface or Privilege is listed. The reviewer can also look at the Toolkit SRRERP file to verify the settings of Interfaces and Privileges.
If any discrepancies appear on the report, this is a finding.

Fixes

Enforced Privs and Interfaces

Ensure all security related Executive Interfaces and Privileges are secured in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.150.00 V0000667 CAT I GEN Tag SECURITY_OPT_1_CTRL Requirements

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.4

Vulnerability The GEN tag SECURITY_OPT_1_CTRL is not set to the required value.

Vulnerability Discussion If the GEN tag SECURITY_OPT_1_CTL (SECOPT1) is not set properly, then the minimum requirements security cannot be met. Specifically, Identification and Authentication (IA) requirements cannot be met since IA down to the individual user may not be supported. In this situation, the security officers user-ID is the only user-ID afforded access to certain privileges. Without SECOPT1, the system cannot meet the Discretionary Access Control (DAC) requirement, because it does not allow the granularity of control to be specified (able to limit access to groups of users and also limit access to an individual user). These significant issues leave the system open to numerous security vulnerabilities.
The IAO will ensure Security Option 1 is configured in the Unisys operating system.
The IAO will ensure the GEN Tag SECURITY_OPT_1_CTRL is set to TRUE.

Checks

System Generation TAG

The reviewer will look at the Toolkit System Config Report to verify that this GENTAG is not listed. The reviewer can also look at the Toolkit SRRTAG file to verify the setting of this GENTAG

Fixes

SECURITY_OPT_1_CTRL

Ensure the GEN tag SECURITY_OPT_1_CTRL is set to the required value of TRUE by building a new operating system with Security Option (or Security Level) One Feature installed.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.160.00 V0000668 CAT I GEN tag EXERR_054_FOR_ALAT

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.4

Vulnerability The GEN tag EXERR_054_FOR_ALAT is not set to the required value.

Vulnerability Discussion If the GEN tag EXERR_054_FOR_ALAT is not set properly, critical system log data may be lost if the system audit trail becomes full or unavailable. The system log file keeps an accurate history of all system activity, including security relevant events.
The IAO will ensure the GEN Tag EXERR_054_FOR_ALAT is set to TRUE.

Checks

System Generation TAG

The reviewer will look at the Toolkit System Config Report to verify that this GENTAG is not listed. The reviewer can also look at the Toolkit SRRTAG file to verify the setting of this GENTAG

Fixes

EXERR_054_FOR_ALAT

Ensure the GEN tag EXERR_054_FOR_ALAT is set to the required value of TRUE

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.170.00 V0000638 CAT II Other security related GEN Tags

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 2.2.3.4

Vulnerability Other security related GEN Tags are not set to the required values.

Vulnerability Discussion If the security related GEN Tags are not set properly, security vulnerabilities may be introduced.
The IAO will ensure all other security related GEN Tags are set to the required values.

Checks

GENTAG Settings

The reviewer will look at the Toolkit System Config Report to verify that none of these GENTAG are listed. The IAO can also look at the Toolkit SRRTAG file to verify the setting of this GENTAG.
The Correct settings are:
Note Short tag is in parentheses (short tag).
Level 7.0 and above setting in square brackets [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

Fixes

GENTAG Settings

Ensure the security related GEN Tags are set to the required values. If deviations are required, they must be approved by the DISA DAA.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.180.00 V0000737 CAT III The account standard is not being followed

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2

Vulnerability The account standard is not being followed.

Vulnerability Discussion An account naming standard provides a means for the IAO to positively identify improperly assigned accounts or unauthorized userids under an account. Access to unauthorized accounts could allow a user to cross ALN boundaries, gain access to privileged system processors or ACRs, or create erroneous fee for service billing information.
For DISA sites, the IAO will ensure the account standard will be followed.

Checks

Account Name Standard

For ALN and CAMS CDB systems, the reviewer will look at the Toolkit Non-Standard Accounts Report to see how many accounts are not in compliance with the standard. The accounts for DFAS Field Organization Base Level users should be deleted from the report if they comply with the requirements of the Unisys STIG, Paragraph C.5.2. For DNMC and DFAS-IN systems, the reviewer will obtain a list of valid accounts from the IAO and compare this list against the Toolkit Non-Standard Accounts Report or account summary file. If there are invalid accounts, this is a finding.

Fixes

Account Naming Standard

Follow the account standard.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.190.00 V0000726 CAT II PRIVAC Account Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.4

Vulnerability Unauthorized users have access to the PRIVAC account.

Vulnerability Discussion The PRIVAC (privileged tape labeling) account allows users to label, unlabel, scratch, and manipulate any tape on the system. If unauthorized users have access to this account, tape information could be compromised, manipulated, or destroyed.
The SA will ensure non-site users do 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.

Checks

PRIVAC Account Access

The reviewer will look at the Toolkit PRIVAC Report. If non-site users have access to the PRIVAC account (for example, 0000TLABEL or UNLABELED), this is a finding. If a large number of site users (more than 10) have access to the PRIVAC account, this is a finding. The reviewer will spot-check the SAAR for those site users with access to the Privileged Tape Labeling Account to make sure this requirement is properly documented. The System Standard Batch Userid is authorized to have access to the PRIVAC account. This item applies to PRIVAC access in the account summary file and/or the userid record.
If the Toolkit is not used, the reviewer will execute the following.

```
@SIMAN,B
GEN ACC_SUM BRE = MY*ACC-SUM. ;
 @EOF
```

The reviewer will then edit the MY*ACC-SUM file locate the PRIVAC account and verify that all of the userids listed under the account have the access to PRIVAC documented on their SAAR.
NOTE: delete the MY*ACC-SUM file after this check is completed.

Fixes

PRIVAC Account Access

Remove unauthorized users from the PRIVAC account or obtain and document justification for the access.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.200.00 V0000724 CAT III Userid Naming Standard

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.9

Vulnerability A userid standard exists but is not being enforced.

Vulnerability Discussion Failing to adhere to a naming convention can make the job of tracing userid activity to an individual much more difficult.
For DISA sites, the IAO will enforce the userid standard established in the appropriate service specific appendix except for userids on the CAMS system.
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.

Checks

Userid Naming Standard

For ALN systems, the reviewer will look at the Toolkit Non-Standard Userids Report. If there are non-standard userids on the report, and this is not a CAMS CDB system, this is a finding.
For DNMC and DFAS-IN systems, the reviewer will obtain the latest userid standard and compare it against the Toolkit Non-Standard Userids Report. The userid standard should point out HQ Consolidated Supply Squadron userids and the CAMS CDB userid standard.

Fixes

Userid Naming Standard

The standard must be followed and non-conforming userids should be modified to conform to the standard.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.210.00 V0000725 CAT II Obsolete or Pre-installed, Userids

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.2

Vulnerability Obsolete, pre-installed, standard userids exist on the system (e.g., CMS, UNIVAC, SPERRY, etc.) and are not deactivated.

Vulnerability Discussion Obsolete system userids and default passwords are commonly known and can provide a means of unauthorized system access.
The IAO will ensure obsolete, pre-installed, standard userids do not exist on the system or are disabled.

Checks

Pre-insalled Userids

The reviewer look at the Toolkit Active or Profile Summary Reports for these user-IDs. If they are active on the system, this is a finding.
IF the Toolkit is not used the reviewer will execute the following.

```
@SIMAN,B
Display Userid = !ALL breakpoint = USERID*ALL ;
@eof
```

The reviewer will then edit the USERID*ALL file and verify that, if any of these userids exist, they are disabled with all run modes except Demand removed, all privileges and interfaces removed, and an @FIN in the ECL field.
The list of obsolete or pre-installed userids includes but is not limited to:
ASET
SPERRY
CMSRSI
CDTS
UNIVAC
ACFBAT
CMS
USAF
RETRIEVALS
VALCHG
SMXX6P
DCFS
Note: The USERID*ALL file is used by many checks but will be deleted at the completion of the SRR.

Fixes

Pre-installed userids

Deactivate pre-installed or obsolete userids from the system.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.220.00 V0000669 CAT III The DPS userid is not set up in accordance with th

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.3

Vulnerability The DPS userid is not set up in accordance with the standard.

Vulnerability Discussion The Display Processing System (DPS) userid is usually the default Master DPS userid when installing or configuring DPS software and must be used when initially establishing userid entries in the DPS password file. Since it is a default userid, it must be set up with minimum privileges so it cannot be used to bypass system security mechanisms if compromised.
The IAO will ensure the DPS userid is set up as a Profile 5 userid.

Checks

DPS Userid

The reviewer will look in the Toolkit SRRALL file for the DPS (or DPSSYS) userid and check it against the current JX$$0000*00.PROFILE/DPS to ensure it has the correct attributes. If it does not match the PROFILE/DPS, this is a finding.

Fixes

DPS Userid

Ensure the DPS userid is set up with the attributes specified by the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.230.00 V0000670 CAT III QUIKST Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.4

Vulnerability The QUIKST userid is not set up in accordance with the standard.

Vulnerability Discussion The QUIKST userid is used by the NJZMON processor to sign-on a demand RSI session. Once this demand RSI session is established, the operations staff can ST runstream names with abbreviated run-IDs. In addition, users can perform certain status keyins on the system without having access to dangerous keyin groups. If this userid is not set up correctly, system batch jobs would not start properly and users could not perform certain keyins necessary for the performance of their job.
The SA will ensure the QUIKST userid is set up as a Profile 3 userid with the STRTZOPT and IMMEDST privileges.

Checks

QUIKST Userid

The reviewer will look in the Toolkit SRRALL file for the QUIKST userid and verify it against the current JX$$0000*00.PROFILE/QUIKST to ensure it has the correct attributes. If it does not match the PROFILE/QUIKST, this is a finding.

Fixes

QUIKST Userid

The SA will re-profile the QUIKST userid using the latest PROFILE/QUIKST runstream. The PROFILE/QUIKST will make the QUIKST userid a modified Profile 3 with IMMEDST and STRTZOPT.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.240.00 V0000671 CAT III The IPFDDP, DDP, or IPF Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.4

Vulnerability The IPFDDP, DDP, or IPF userid is not set up in accordance with the standard.

Vulnerability Discussion The IPFDDP, DDP, or IPF userid is used by the Distributed Data Processor (DDP) to sign-on a demand RSI session. Once this demand RSI session is established, it is used by DDP to monitor the file job transfer environment and used by TCP/IP Application Services (TAS) to handle certain types of file transfers. If this userid is not set up correctly, file transfers would cease to process and delays in the transfer of critical data interfaces could occur.
The SA will ensure the IPFDDP, DDP, or IPF are be set up as a Profile 5 userid.

Checks

IPFDDP DDP or IPF userid

The reviewer will look in the Toolkit SRRALL file for the IPF userid, which could be IPF, IPFDDP, or DDP, and check it against the current JX$$0000*00.PROFILE/IPF to ensure it has the correct attributes. If it does not match the PROFILE/IPF, this is a finding.

Fixes

IPFDDP, DDP, or IPF Userid

The SA will re-profile the IPF userid using the PROFILE/IPF runstream. The PROFILE/IPF will make the IPF userid a modified Profile 5 with a system or user entered run card image.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.250.00 V0000672 CAT III Scheduler Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.4

Vulnerability The Scheduler userid is not set up in accordance with the standard.

Vulnerability Discussion The Scheduler userid is used to manage the automated processing of most batch runs. If this userid is not set up correctly, Scheduler can cease to process or process improperly. This could impact the timely processing of customer batch runs, resulting in denial of service to the user and delays in processing critical data.
The SA will ensure the Scheduler userid is set up as a Profile 3 userid with STRTZOPT and IMMEDST privileges.

Checks

Scheduler Userid

The reviewer will look in the Toolkit SRRALL file for the Scheduler userid and verify it against the current JX$$0000*00.PROFILE/SCHED to ensure it has the correct attributes. If it does not match the PROFILE/SCHED, this is a finding.

Fixes

Scheduler Userid

The SA will re-profile this userid using the latest PROFILE/SCHED runstream. The PROFILE/SCHED runstream will make the Scheduler userid a modified Profile 3 with IMMEDST and STRTZOPT.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.260.00 V0000673 CAT III VTHSRV Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.4

Vulnerability The VTHSRV userid is not set up in accordance with the standard. (VTH Sites Only)

Vulnerability Discussion The VTHSRV userid is used to manage numerous capabilities of the Virtual Tape software. If this userid is not set up correctly, the Virtual Tape software can cease to function properly and job requests for virtual tapes can be put into a hold status. This could impact the timely processing of customer batch runs, resulting in denial of service to the user and delays in processing critical data.
For DISA sites, the SA will ensure the VTHSRV userid is set up as a PROFILE/VTHSRV userid.

Checks

VTHSRV Userid

The reviewer will look in the Toolkit SRRALL file for the VTHSRV userid and verify it against the JX$$0000*00.PROFILE/VTHSRV to ensure it has the correct attributes. If it does not match the PROFILE/VTHSRV, this is a finding.

Fixes

VTHSRV Userid

The SA will re-profile this userid using the latest PROFILE/VTHSRV runstream. The PROFILE/VTHSRV runstream will make the VTHSRV userid a modified Profile 3 with FAS privileges.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.260.10 V0006451 CAT III EZLOAD Userid Profile

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.4

Vulnerability EZLOAD userids do not have the properties found in the PROFILE/EXLOAD setup element.

Vulnerability Discussion The EZLOAD userid is used to manage the software used to reload deleted or older versions of user files from backup tapes. If this userid is not set up correctly, the EZLOAD software can cease to function properly and requests for reloading files can fail. This could impact the timely processing of customer batch runs, resulting in denial of service to the user and delays in processing critical data.
For DISA sites, the SA will ensure the EZLOAD userid is set up as a PROFILE/EZLOAD userid.

Checks

EZLOAD Userid Profile

The reviewer will look in the Toolkit SRRALL file for the xxEZ00 userid(s) and verify it against the JX$$0000*00.PROFILE/EZLOAD to ensure it has the correct attributes. If it does not match the PROFILE/EZLOAD, this is a finding.

Fixes

EZLOAD Userid Profile

The SA will re-profile this userid using the latest PROFILE/VTHSRV runstream. The PROFILE/VTHSRV runstream will make the xxEZ00 userid a modified Profile 5 with the STRTZOPT privilege and access to the RNCNT1 keyin group.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.260.20 V0006454 CAT III Shared Library System Userid Profile

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.5

Vulnerability The Shared Library System userid does not have the properties found in the PROFILE/TAPE setup element.

Vulnerability Discussion The Shared Library System userid is used to manage the software used to synchronize the tape library database between two or more systems that are accessing the same tape library. If this userid is not set up correctly, the Shared Library Systems software can cease to function properly and the tape library databases will get out of sync. This could lead to data lose by overwriting of newly created tapes, the compromise of sensitive data by allowing a tape to be read by an unauthorized user or a denial of service caused by the shutting down of the tape library software.
For DISA sites, The SA will ensure the Shared Library System userid is set up as a PROFILE/TAPE userid.

Checks

SLS Userid Profile

The reviewer will look in the Toolkit SRRALL file for the xxJSTM userid and verify it against the JX$$0000*00.PROFILE/TAPE to ensure it has the correct attributes. If it does not match the PROFILE/TAPE, this is a finding.

Note: If this is an ALN site the userid will have the Bypass Ownership (BYOWNER) and Bypass ACR (BYACR) privileges.

Fixes

SLS Userid Profile

The SA will re-profile this userid using the latest PROFILE/TAPE runstream. The PROFILE/TAPE runstream will make the xxJSTM userid a modified Profile 3 with the BYOWNER and BYACR privileges.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.270.00 V0000674 CAT III DDP TXFR Userid

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.6

Vulnerability The DDP TXFR userid is not set up in accordance with the standard.

Vulnerability Discussion The DDP TXFR userid is used to transfer approved software releases from the HQ Standard Systems Group or SSO Montgomery to the sites. If this userid is not set up correctly, software releases may not be transferred properly, and the implementation of critical operating or application software fixes could be delayed.
The SA will ensure the DDP-FJT Tape Transfer userid is set up as a Profile 8 userid with only batch access and disabled.

Checks

DDP-FJT Tape File Transfer Use

The reviewer will look in the Toolkit SRRALL file for the SSC-SSQM or GAJT00 userids and verify them against the JX$$0000*00.PROFILE/TXFR to ensure they have the correct attributes. If they do not match the PROFILE/TXFR, this is a finding.

Fixes

DDP-FJT Tape File Transfer Use

The SA will re-profile these userids using the latest PROFILE/TXFR runstream. The PROFILE/TXFR runstream will make these userids a modified Profile 8 userid with batch only mode and disabled. NOTE: These userids are authorized access to an exempt account.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.274.00 V0004092 CAT III The UOSS userid is not set up correctly

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.7

Vulnerability The UOSS userid is not set up correctly.

Vulnerability Discussion If the UOSS userid is not set up correctly, UOSS may fail disabling the Unattended Operations features from the system.
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.

Checks

UOSS Userid

If UOSS is used, the reviewer will look in the Toolkit SRRALL file for the UOSS userid to verify that it is a Profile 2 userid with Response CONS; SYMCTL, RUNSTA, and RNCNT1 console keyin groups; and the ability to have the user enter a run image.

Fixes

UOSS Userid

The SA will re-profile these userids using the latest PROFILE-2 runstream. Then the SA will enter SIMAN and manually grant the UOSS userid Response Cons with access to the SYMCTL, RUNSTA, and RNCNT1 console keyin groups, and the ability to have the user enter a run image.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.280.00 V0000675 CAT III The Session Control Userids

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.9

Vulnerability The Session Control Userids are not set up in accordance with the standard.

Vulnerability Discussion The Session Control Userids are used by the operating system to manage and control certain features of TIP Session Control. If these userids are not set up correctly, certain capabilities within TIP Session Control may fail, resulting in denial of service to customers or delays in processing critical data. If these user-IDs are not protected as stipulated in the Unisys STIG, these userids may be subject to compromise and exploitation by unauthorized users.
The IAO will ensure Session Control userids do not have any run modes and are disabled.

Checks

Session Control Userids

The reviewer will look in the Toolkit SRRALL file for the Session Control userids, COM-SYSTEM-L, COM-SYSTEM-H, and TIPOUTPUT, and verify that these userids are disabled with no run modes.

Fixes

Session Control Userids

The IAO will enter SIMAN and manually update the Session Control userids so that they are disabled and have no run modes.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.290.00 V0000676 CAT II The Fixed Gate Subsystem userids are not set up in

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.9

Vulnerability The Fixed Gate Subsystem userids are not set up in accordance with the standard.

Vulnerability Discussion The Fixed Gate Subsystem userids own and control access to certain Executive Software files. If these userids are not set up correctly, certain software processors within the operating system will not function correctly, resulting in denial of service to customers or delays in processing critical data. If these userids are not protected as stipulated in the Unisys STIG, these userids may be subject to compromise and exploitation by unauthorized users.
The IAO will ensure all Fixed Gate Subsystem userids, except where noted, do not have any run modes and are disabled.

Checks

Fixed Gate Subsystem Userids

The reviewer will look in the Toolkit SRRALL file for the Fixed Gate Subsystem userids and verify that these userids are disabled with no run modes. NOTE: -DDP-PPC-, -UDS0x- (for active application groups only), -CIFS-ADMIN-, and -MQS2200- are authorized to have batch mode.

Fixes

Fixed Gate Subsystem Userids

Ensure the Fixed Gate Subsystem userids are set up with the attributes specified by the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.300.00 V0000677 CAT I The EXEC Userids

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.5.9

Vulnerability The EXEC userids are not set up in accordance with the standard.

Vulnerability Discussion The EXEC userids have access to all Executive Interfaces and Privileges, and are used by the operating system for unique internal processing requirements. If TSS$FILE security records are created for these userids, they expose these special system userids to potential compromise and exploitation by unauthorized users. For HMP IX 7.0 and above these userids have security records, have no run modes, they cannot be modified by any userid and they cannot be used except by the operating system.
The IAO will ensure in system levels below HMP IX 7.0 the EXEC userids (EXEC8 and INSTALLATION) do not have TSS$FILE records, only SACRD$

Checks

System Userids

The reviewer, on system prior to HMP IX 7.0, will check the Toolkit Active and Disabled Reports to verify that these userids are not listed. If they are found on the reports, this is a finding. For HMP IX 7.0 and higher operating systems, these userids will exist. However they cannot be modified or deleted by any other userid, including the Security Officer’s userid, therefore check is not applicable.

Fixes

System Userids

The process required for removal of these userids is complex. If the site is supported by SSO Montgomery contact SSO Montgomery for assistance. If SSO Montgomery does not support the site, contact Unisys for assistance.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.310.00 V0000618 CAT II Unauthorized users have an ALN-exempt project-ID

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.13.11.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.2

Vulnerability Unauthorized users have an ALN-exempt project-ID in their userid record. (ALN Sites Only)

Vulnerability Discussion Users who are ALN exempt can access or destroy data from site workloads they are not authorized access to. Also, ALN exempt users present a serious aggregation of data threat.
The SA will ensure non-exempt users do not have an exempt project-ID in their userid record.

Checks

ALN-Exempt Project-ID

The reviewer will look at the Toolkit Exempt Account/Project-ID Report to verify that non-site users do not have an ALN-exempt project-ID in their userid record. If any non-site users are identified, then there will be documentation cross-coordinated with every functional area for every ALN on that particular system. If properly coordinated documentation is not available, this is a finding.

Fixes

ALN-Exempt Project-ID

Remove all ALN-exempt project-IDs from unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.320.00 V0000619 CAT II Unauthorized users have an ALN-exempt account

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.1

Vulnerability Unauthorized users have an ALN-exempt account in their userid record. (ALN Sites Only)

Vulnerability Discussion Users who are ALN exempt can access or destroy data from site workloads they are not authorized access to. Also, ALN exempt users present a serious aggregation of data threat.
The SA will ensure non-exempt users, except where documented, do not have an exempt account in their userid record.

Checks

ALN Exempt Accounts

The reviewer will look at the Toolkit Exempt Account/Project-ID Report to see if any non-site users have an ALN exempt account in their userid record. If any non-site users are identified, then the access should be documented and cross-coordinated with functional area for every ALN on that particular system. If the proper documentation does not exist this is a finding.

Fixes

ALN Exempt Accounts

Remove all ALN-exempt accounts from unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.330.00 V0000582 CAT II Users are not Restricted to Project-IDs

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.2

Vulnerability Unauthorized users are not restricted to specific project-IDs (ALN Only).

Vulnerability Discussion Users who are not restricted to their list of project-IDs can use unauthorized qualifiers, including exempt qualifiers, when starting batch jobs. This capability gives a user the potential to alter databases or files not belonging to that user.
The SA will ensure non-exempt users, except where documented, are restricted to a specific list of project-Ids.

Checks

ALN Project-ID restricted

The reviewer will look at the Toolkit Project-ID Unrestricted Report to verify that non-site users are restricted to specific project-IDs. If any non-site users are identified, proper documentations will exist. The documentation will be cross-coordinated with every functional area for every ALN on that particular system since an end user could @START a batch job with an exempt project-ID on the START statement. If proper documentation does not exist this is a finding.

Fixes

ALN Project-ID Restricted

Modify userid security records so users are restricted to their list of project-IDs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.340.00 V0000617 CAT II Users are allowed to enter their own project-id

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.11.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.3.2

Vulnerability Unauthorized users are allowed to enter their own project-ID at signon time. (ALN Sites Only)

Vulnerability Discussion Users who can enter their project-IDs can bypass ALN boundaries thereby having the potential to alter another sites workload data.
The SA will ensure non-exempt users, except where documented, are not allowed to enter their project-ID at sign-on time.

Checks

ALN Project-ID at Sign On.

The reviewer will look at the Toolkit Account/Project-ID Entry Report to verify that non-site users are not allowed to enter a project-ID at sign on time. If any non-site users are identified, proper documentation will exist. This documentation will be cross-coordinated with every functional area for every ALN on that particular system. If proper documentation does not exist this is a finding.

Fixes

ALN Project-ID at Sign On

Modify userid security records to restrict unauthorized users from entering their project-ID.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.350.00 V0000720 CAT III Users Five Account Access

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.1

Vulnerability Users who require access to less than five accounts have the ability to enter an account at signon time.

Vulnerability Discussion Users that can enter an account may circumvent ALN security mechanisms, gain access to privileged system processors or ACRs, and create erroneous fee for service information.
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.

Checks

Less than 5 Accounts

The reviewer will look at the Toolkit Account/Project-ID Entry Report to verify that no users are allowed to enter an account at sign on time. If any users are identified, check the Userid Account/Project-ID Report to see what accounts are in the userid record. Also, check the account summary file to find out what accounts this userid has access to. SSO Montgomery has provided two SQL queries to assist with the reviewer with this checklist item. The first query is called AcctUseEntACT. This query will list all non-site code userids that are active and have the User Entered Account flag set. It will also list all the accounts in the userid record. The second query is called UserEnterAcctSum. This query uses the userids identified in the AcctUseEntACT query as input and identifies what accounts in the Account Summary file (Unisys_Platform_Accounts table) these userids have access to. It also displays the accounts that are located in the userid record. On ALN systems, if a userid has access to ALN exempt accounts, this is a finding. If a userid only has access to five or less non-exempt accounts, this is a finding unless this access is properly documented.. On DNMC, DFAS-IN, and CAMS CDB systems, documentation will exist for any user that can enter an account.

Fixes

Less than 5 accounts

Ensure that the ability to enter an account at signon is disabled for unauthorized users requiring access to five or less accounts.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.354.00 V0004094 CAT III Users who require more than five accounts

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.2.1

Vulnerability Users who require access to more than five accounts are not correctly documented.

Vulnerability Discussion Users who require access to more than 5 accounts must be allowed to enter an account during signon. If these users are not correctly documented, they cannot be readily distinguished from users that have no need to enter an account during signon. This can lead to unauthorized users who can enter an account circumventing ALN security mechanisms, gaining access to privileged system processors or ACRs, and creating erroneous fee for service information.
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.

Checks

More than 5 accounts.

The reviewer will look at the Toolkit Account/Project-ID Entry Report to verify that users with access to more than 5 accounts have proper documentation. If any users are identified, check the Userid Account/Project-ID Report to see what accounts are in the userid record. Also, check the account summary file to find out what accounts this userid has access to. SSO Montgomery has provided two SQL queries to assist with the reviewer with this checklist item. The first query is called AcctUseEntACT. This query will list all non-site code userids that are active and have the User Entered Account flag set. It will also list all the accounts in the userid record. The second query is called UserEnterAcctSum. This query uses the userids identified in the AcctUseEntACT query as input and identifies what accounts in the Account Summary file (Unisys_Platform_Accounts table) these userids have access to. It also displays the accounts that are located in the userid record. On ALN systems, if a userid has access to ALN exempt accounts, this is a finding. If a userid has access to more than five accounts, this is a finding unless this access is properly documented. On DNMC, DFAS-IN, and CAMS CDB systems, documentation will exist for any user that can enter an account.

Fixes

More than 5 accounts

Document all users that require access to more than five accounts in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.360.00 V0000624 CAT II CONS levels beyond Profile

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.2

Vulnerability There are users who have access to CONS levels beyond that which are defined in their security profile and there is no documentation to justify the access.

Vulnerability Discussion Some of the CONS levels, in conjunction with CONS keyin groups, could adversely affect system processing, availability of system resources, result in denial of service, or have a detrimental impact on system performance.
The SA will ensure users, except where documented, do not have access to CONS levels beyond specified in their security profile.

Checks

Excessive CONS Level

The reviewer will check the Toolkit CONS Capability Report. If there are active user-IDs that have a CONS level outside their assigned profile, this is a finding unless properly documented on the SAAR. NOTE: A reasonable number of site Profile 2 user-IDs can have RESPONSE CONS. If there are Profile 8 user-IDs with DISPLAY CONS, the IAO should spot-check these user-IDs to verify that this requirement is properly justified and documented on the individual's SAAR.

Fixes

Excessive CONS level

Ensure all users are assigned the least CONS level necessary to perform their duties. Ensure all documentation is maintained for actual user access granted that is not in accordance with the user profile. Any user who does not have a documented need for CONS level above that granted their profile will have the excessive CONS level replaced with the correct level.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.370.00 V0000719 CAT II CONS Keyin Groups

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.7.2.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.6

Vulnerability There are users who have access to security related CONS keyin groups that are beyond that which are defined in their security profile and there is no documentation to justify the access.

Vulnerability Discussion Some of the CONS keyin groups, in conjunction with CONS levels, could adversely affect system processing, availability of system resources, result in denial of service, or have a detrimental impact on system performance.
The SA will ensure users, except where documented, do not have access to CONS keyin groups beyond those specified in their security profile.

Checks

CONS Keyin Groups

The reviewer will check the Toolkit Danger CONS/Keyins Report to verify access to CONS keyin groups outside the userid's profile is documented.
On ALN systems.
If there are active user-IDs that have dangerous CONS keyin groups outside their assigned profile, the reviewer will verify that they are correctly documented.. If there are any non-site user-IDs with the TIPGRP, RNCNT1, RNCNT2, MSTCNT, DEBUGS, or DEVCNT keyin group, the reviewer will verify that they are correctly documented. If there are any non-site users with FULL or higher CONS mode and the SYMCTL keyin group, this is a finding. If there are non-site users with LIMITED or lower CONS mode and the SYMCTL keyin group, the reviewer will verify that they are correctly documented.

On DNMC and DFAS-IN systems and all non-ALN systems.
The reviewer will spot Profile 7 and 8 userids that have the SYMCTL or RNCNT1 keyin group verify this requirement is properly documented on the individual's SAAR. A reasonable number will be allowed provided they have the correct level of CONS for the profile assigned to the userid. The reviewer will verify that any userid that has Full or Display CONS and the SYMCTL, RNCNT1, or TIPGRP keyin group is documented.

On the Toolkit Report, the reviewer will delete Profile 7 and 8 userids with the correct level of CONS and the SYMCTL or RNCNT1 keyin group. Additionally the reviewer will delete properly documented userids that have Full or Display CONS and the SYMCTL, RNCNT1, or TIPGRP keyin group. After this is done, if any userid are left this is a finding.

Fixes

CONS Keyin Groups

Ensure all users are assigned the least CONS keyin groups necessary to perform their duties. Ensure all documentation is maintained for actual user access granted that is not in accordance with the user profile. Remove any CONS keyin groups from users who's documentation does not require the group.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.380.00 V0000577 CAT II Terminal Timeout

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.4, Computing Services Security Handbook

Vulnerability Userids have the terminal time out set greater than the standard allows.

Vulnerability Discussion Without time out mechanisms, active sessions may be compromised through access to the unattended physical device.
The SA will ensure userids, except where documented, have their terminal time out set in to fifteen minutes.

Checks

Terminal Timeout

The reviewer will verify that the terminal timeout does not exceed fifteen (15) minutes or the system wide value that has been designated by the IAM. In the case of the IAM designated timeout, the value will not exceed 60 minutes.
The reviewer will cross out or delete any exception userids from the Toolkit Timeout (Demand and No Demand) Reports. If there are active userids that are still out of compliance, this is a finding. The following exceptions will be allowed.
CAMS TIP Profile 9 userids, 780 minutes if CAMS internal timeout is set to 15 minutes.
CAMS DBM Demand userid, 780 minutes.
SSBS System Code GV Output Only TIP Profile 9 userids, 540 minutes.
MASS System code GW TIP Profile 9 userids, 540 minutes.
SBSS RPS Function 057 terminal Demand userid, 0 minutes/timeout disabled.
SBSS RPS other terminal Demand, userids 540 minutes.
SATS batch/TIP userid, 480 minutes.
CBAS TIP Profile 9 userids, 240 minutes.

Fixes

Terminal Timeout

Review all userids to ensure no userid has a terminal time out threshold above the guidelines documented in the Unisys STIG.
Maintain documentation as specified in the Unisys STIG for all required exceptions.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.390.00 V0000578 CAT II Userids can Disable Terminal Timeout

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.4

Vulnerability Userids have the ability to disable their terminal time out.

Vulnerability Discussion Without time out mechanisms, active sessions may be compromised through access to the unattended physical device.
The SA will ensure userids, except where documented, do not have the ability to disable their terminal time out.

Checks

Timeout Disabled

The reviewer will check the Toolkit Timeout (Demand and No Demand) Reports to verify that only userids that are authorized have their terminal time out disabled. The authorized userids specified in the Unisys STIG are currently:
QUIKST used by the QUICKSTART background run.
IPF, IPFDDP, or DDP used by the DDP-FJT background run.
Scheduler used by the Scheduler background runs.
VTHSRV used by the Virtual Tape Handler background run.
xxEZ00 used by EZLOAD background run.
xxJSTM used by SLS.
Other userids used for the above functions.
If there are other userids that have their terminal time out disabled, this is a finding.

Fixes

Timeout Disabled

Ensure no userid, other than those documented in the Unisys STIG, can disable their terminal time out.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.400.00 V0000721 CAT II Userids maximum password expiration

8500.2 IA Control: DCBP-1

References: Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense-in-Depth: Information Assuran C.A.7, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.3.4

Vulnerability Userids have the maximum password expiration set greater than the standard allows.

Vulnerability Discussion Unless passwords are changed on a regular interval, a compromised password may be exploited threatening system and data integrity.
The SA will ensure all users, except documented exceptions, have a maximum password expiration of 90 days.

Checks

Max Pass expire

The reviewer will check the Toolkit Password Expiration Report to verify that all userids have their maximum password expiration set to 90 days.
Exceptions to this requirement are:
Demand RSI userids and other system userids, as identified in the Unisys STIG, are authorized 365 days. Currently these userids are:
QUIKST
IPF, IPFDDP, or DDP
Scheduler,
VTHSRV
xxEZ00
xxJSTM
FTP only userids are authorized 365 days.
If active userids are set not correctly, this is a finding.

Fixes

Max Pass Expire

All userid password expirations should be set to 90 days except those documented in the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.410.00 V0000552 CAT II Userids minimum password expiration.

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.6.3.4

Vulnerability Userids have a minimum password expiration set less than the standard allows.

Vulnerability Discussion Having a minimum password set less than the standard allows encourages users to change their new password back to their old password and bypass established security countermeasures that require new password changes on a regular interval.
The SA will ensure all users, except documented exceptions, have a minimum password expiration of one day.

Checks

Min Pass Expire

The reviewer will check the Toolkit Password Expiration Report. Subadministrators userids that are documented as being passed between SA for multi-shift coverage are allowed to have the value of zero in this field. All other userids will have a value of one or greater in this field.

Fixes

Min Pass Expire

All userid's minimum password expirations should be set to a minimum value of one (1) day.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.420.00 V0000722 CAT II Userids Clearance Levels

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.2

Vulnerability Userids have access to clearance levels beyond that specified by their profile and no justification exists.

Vulnerability Discussion By not using the standard profiles and/or not documenting the clearance levels required, higher clearance levels may be assigned without justification. Unauthorized access to a higher clearance level could allow a user access to files that are assigned a specific clearance level for security reasons.
The SA will ensure users, except where documented, do not have access to clearance levels beyond those specified in their security profile.

Checks

Userid Clearance Level

The reviewer will check the Toolkit Clearance Levels Report to verify that no userid is granted a clearance level range outside of that specified in the profile assigned the userid. Subadministrators will show up on this report as a false positive since they are modified Profile 3 userids. The reviewer will verify that subadministrators are set to a clearance level of 0 – 0 and not 0 – 11 or 0 – 63. Once this is verified, the reviewer can cross out or delete these userids from the report. If any active userid has a clearance level beyond that specified for their profile, this is a finding.

Fixes

Userid Clearance Level

Ensure all users are assigned the least clearance level necessary to perform their duties. Clearance levels should be established to fall within the range as specified in the Unisys STIG. Where the actual clearance level granted differs from the profile range, the IAO should maintain documentation to justify the difference.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.430.00 V0000735 CAT II Security Bypass Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.4

Vulnerability Unauthorized users have security bypass privileges in their userid record.

Vulnerability Discussion The bypass privileges allow users to circumvent Unisys Discretionary Access Controls. These privileges are not generally required by an end user and present a significant threat.
The SA will ensure users do not have access to security bypass privileges beyond those specified in their security profile.

Checks

Security Bypass Privileges

The reviewer will check the Toolkit Bypass Report to verify that no userid is granted a security bypass privilege that is not in the profile assigned the userid unless it it's a documented exception.. If active user-IDs have security bypass privileges beyond that specified for their profile and the userid is not listed in the Unisys STIG as being granted this exception, this is a finding.

Fixes

Security Bypass Privileges

Remove bypass privileges from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.440.00 V0000738 CAT I MODPS$ Interface

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 6.3, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 8.9.3

Vulnerability Unauthorized personnel have access to the MODPS$ Executive Interface.

Vulnerability Discussion The MODPS$ Executive Interface provides a means for users to activate certain security relevant privileges. This interface is also used to secure certain system processors are secure from unauthorized use.
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.

Checks

MODPS$ Interface

The reviewer will check the Toolkit MODPS$ Report to verify that unauthorized users are not granted access to the MODPS$ interface.. If any active userid has the MODPS$ Executive Interface outside of their assigned profile and this access is not documented on the user’s SAAR, this is a finding.

Fixes

MODPS$ Interface

Remove access to the MODPS$ Executive Interface from unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.450.00 V0000678 CAT II SSWRSUBDAC Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.4

Vulnerability Unauthorized users have access to the SSWRSUBDAC privilege.

Vulnerability Discussion The SSWRSUBDAC privilege is used to restrict access to the CSUPDT processor to authorized users. If access to the CSUPDT processor is granted to unauthorized users, it can be used to obtain or modify sensitive information concerning the File Transfer user-ID and distributed data processing configuration. Improper or malicious modifications could result in the termination of file transfers or misrouting of files to unauthorized personnel.
The SA will ensure users do not have access to the SSWRSUBDAC privilege unless it is authorized for their security profile.

Checks

SSWRSUBDAC Privilege

The reviewer will check the Toolkit SSWRSUBDAC Report to verify that unauthorized users are not granted access to the SSWRSUBDAC. If any active userid has the SSWRSUBDAC privilege outside of their assigned profile without the access being documented on the user’s SAAR, this is a finding.

Fixes

SSWRSUBDAC Privilege

Ensure only authorized userids have the SSWRSUBDAC privilege.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.460.00 V0000679 CAT II STRTZOPT Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.4

Vulnerability Unauthorized users have access to the STRTZOPT privilege.

Vulnerability Discussion The STRTZOPT privilege allows a user with Full or higher CONS and the RNCNT1 keyin group to ST a job with a userid other than his/her own. If the STRTZOPT privilege is assigned to unauthorized users, they can gain access to the privileged security attributes of another userid, and possibly exploit or cause grave damage to system and application files.
The SA will ensure users do not have access to STRTZOPT privilege unless they are authorized for their security profile.

Checks

STRTZOP Privilege

The reviewer will check the Toolkit STRTZOPT Report to verify that no unauthorized user is granted access to the STRTZOP privilege. If any active userid has the STRTZOPT privilege outside of their assigned profile and this access is not granted on the user’s SAAR, this is a finding.

NOTE: QUIKST, xxEZ00, and the Scheduler user-ID are authorized to have this privilege.

Fixes

STRTZOP Privilege

Remove the STRTZOPT privilege from any unauthorized userid.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.470.00 V0000680 CAT II IMMEDST Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.4

Vulnerability Unauthorized users have access to the IMMEDST privilege.

Vulnerability Discussion The IMMEDST privilege allows a user to use the X option on a @START or ST command, which causes a batch run to start immediately, regardless of system holds or Batch limit. If the IMMEDST privilege is assigned to unauthorized users, they could override system holds and batch utilization controls and degrade system performance. This could delay the completion of authorized jobs, resulting in denial of service.
The SA will ensure users do not have access to IMMEDST privilege unless it is authorized for their security profile.

Checks

IMMEDST Privilege:

The reviewer will check the Toolkit IMMEDST Report to verify that unauthorized users are not granted access to the IMMEDST privilege. If any active userid has the IMMEDST privilege outside of their assigned profile and this access is not documented on the user’s SAAR, this is a finding.

NOTE: QUIKST and the Scheduler userid are authorized to have this privilege.

Fixes

IMMEDST Privilege

Remove the IMMEDST privilege from all unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.480.00 V0000681 CAT II COMPALTR or SSTIPBLD Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE N/A

Vulnerability Unauthorized users have access to the COMPALTR or the SSTIPBLD (for HMP IX 7.0 and above) privilege.

Vulnerability Discussion The COMPALTR privilege is used to restrict access to the TIP validation table utility (VTBUTL) processor to authorized users. On systems in HMP IX 7.0 and above, SSTIPBLD are used to restrict this access. If access to the VTBUTL processor is granted to unauthorized users, it can be used to modify sensitive information concerning TIP transactions and their attributes. Improper or malicious modifications could cause erroneous TIP transactions to be started, which can compromise data integrity and/or degrade the efficiency of TIP transaction processing on the domain.
The SA will ensure users do not have access to COMPALTR and SSTIPBLD privileges unless they are authorized for their security profile.

Checks

COMPALTR & SSTIPBLD Privilege

The reviewer will check the Toolkit COMPALTR Report to verify that unauthorized users do not have access to the COMPALTR and/or SSTIPBLD privileges.
For sites running the SSO Montgomery modified versions of the TIP Utilities prior to level HMP IX 7.0.
If any active userid has the COMPALTR privilege outside of their assigned profile and this access is not documented on the user's SAAR, this is a finding.

NOTE: Select Profile 2 userids are authorized to have the COMPALTR privilege.

All sites with HMP IX 7.0 or higher.
The SSTIPBLD privilege is available with HMP IX 7.0 and higher operating systems. The reviewer will run the SSO Montgomery provided SQL query FIND-PRV-ALL to locate those users with the SSTIPBLD privilege. The reviewer will update this query to select ~ZH.

NOTE: Select Profile 2 userids are authorized to have this SSTIPBLD privilege.
If any active userids has either of these privileges outside of their assigned profile and this access is not documented on the user's SAAR, this is a finding.

Note: On SSO supported systems, SSTIPBLD privilege is enforced when the HMP IX 8.0 and higher operating system is loaded

Fixes

COMPALTR & SSTIPBLD Privilege

Remove COMPALTR or SSTIPBLD privileges from unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.490.00 V0000734 CAT II SSMMGRBYPASS Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5

Vulnerability Unauthorized users have access to the SSMMGRBYPASS privilege.

Vulnerability Discussion The SSMMGRBYPASS privilege allows users to bypass STAR tape access restrictions. If assigned to unauthorized personnel, this weakens the tape object security mechanisms put in place by site and application personnel.
The SA will ensure users do not have access to the SSMMGRBYPASS privilege unless it is authorized for their security profile.

Checks

SSMMGRBYPASS Privilege

The reviewer will check the Toolkit Media Manager Userids Report to verify that unauthorized users are not granted access to the SSMMGRBYPASS privilege. If any active userid has the SSMMGRBYPASS privilege outside their security profile and this access is not documented on the user’s SAAR, this is a finding.

Fixes

SSMMGRBYPASS Privilege

Remove the SSMMGRBYPASS privilege from unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.500.00 V0000579 CAT II SSMMGRILES3 Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the SSMMGRILES3 privilege.

Vulnerability Discussion Unauthorized access to the SSMMGRILES3 privilege would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to the standalone SSMMGRILES3 privilege unless it is authorized for their security profile.

Checks

SSMMGRILES3 Privilege Standalo

The reviewer will check the Toolkit Media Manager User-IDs Report. Subadministrators will show up on the Toolkit Media Manager User-IDs report with an asterisk under invalid distribution. The subadministrators show up on the report because they are modified Profile 3 userids. However, subadministrators will only have the SSMMGRILES1 privilege and not the SSMMGRILES3 privilege. Once this is verified, then the reviewer can cross out or delete the subadministrator userids from the report. If there are any remaining userids with the standalone SSMMGRILES3 privilege and this access is not documented on the user’s SAAR, this is a finding.

Fixes

SSMMGRILES3 Privilege Standalo

Remove the standalone SSMMGRILES3 privilege from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.510.00 V0000580 CAT II SSMMGRILES2 Privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the SSMMGRILES2 privilege.

Vulnerability Discussion Unauthorized access to the SSMMGRILES2 privilege would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to the standalone SSMMGRILES2 privilege.

Checks

SSMMGRILES2 Privilege Standalo

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized userids have access to the SSMMGRILES2 privilege. If active users have standalone access to SSMMGRILES2 privilege beyond that specified for their profile and this access is not documented in the user’s SAAR, this is a finding.

Fixes

SSMMGRILES2 Privilege Standalo

Remove the SSMMGRILES2 privilege from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.520.00 V0000682 CAT II Combined SSMMGRILES1 and SSMMGRILES2 Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the combined SSMMGRILES1 and SSMMGRILES2 privileges.

Vulnerability Discussion Unauthorized access to the combined SSMMGRILES1 and SSMMGRILES2 privileges would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES2 privileges unless this combination is authorized for their security profile.

Checks

SSMMGRILES1 and SSMMGRILES2 C

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized users have access to both SSMMGRILES1 and SSMMGRILES2 privileges. If any active users have both these privileges beyond that specified for their profile and the access is not documented on the user’s SAAR, this is a finding.

Fixes

SSMMGRILES1 and SSMMGRILES2 C

Remove the combined SSMMGRILES1 and SSMMGRILES2 privileges from all unauthorized users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.530.00 V0000683 CAT II Combined SSMMGRILES1 and SSMMGRILES3 Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the combined SSMMGRILES1 and SSMMGRILES3 privileges.

Vulnerability Discussion Unauthorized access to the combined SSMMGRILES1 and SSMMGRILES3 privileges would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to both SSMMGRILES1 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.

Checks

SSMMGRILES1 and SSMMGRILES3 Co

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized users have access to both SSMMGRILES1 and SSMMGRILES3 privileges. If any active users have both these privileges beyond that specified for their profile and the access is not documented on the user’s SAAR, this is a finding.

Fixes

SSMMGRILES1 and SSMMGRILES3 Co

Remove the combined SSMMGRILES1 and SSMMGRILES3 privileges from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.540.00 V0000684 CAT II Combined SSMMGRILES2 and SSMMGRILES3 Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the combined SSMMGRILES2 and SSMMGRILES3 privileges.

Vulnerability Discussion Unauthorized access to the combined SSMMGRILES2 and SSMMGRILES3 privileges would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to both SSMMGRILES2 and SSMMGRILES3 privileges unless this combination is authorized for their security profile.

Checks

Combined SSMMGRILES2 and SSMMG

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized users have access to both SSMMGRILES2 and SSMMGRILES3 privileges. If any active users have both these privileges beyond that specified for their profile and the access is not documented on the user’s SAAR, this is a finding.

Fixes

Combined SSMMGRILES2 and SSMMG

Remove the combined SSMMGRILES2 and SSMMGRILES3 privileges from any unauthorized userid.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.550.00 V0000685 CAT II Combined SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the combined SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges.

Vulnerability Discussion Unauthorized access to the combined SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges would allow users to modify tape records beyond their intended span of control.
The SA will ensure users do not have access to SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges unless this combination is authorized for their security profile.

Checks

SSMMGRILES1, SSMMGRILES2 and S

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized users have access to the SSMMGRILES1, SSMMGRILES2 and SSMMGRILES3 privileges. If any active users have all of these privileges beyond that specified for their profile and the access is not documented on the user’s SAAR, this is a finding.

Fixes

SSMMGRILES1, SSMMGRILES2 and S

Remove the combined SSMMGRILES1, SSMMGRILES2, and SSMMGRILES3 privileges from all unauthorized userids..

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.560.00 V0000686 CAT I All three SSMMGRILESx and SSMMGRBYPASS Privileges

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.8.5, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 7.2.3

Vulnerability Unauthorized users have access to the combined SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRBYPASS privileges.

Vulnerability Discussion Unauthorized access to the combined SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRBYPASS privileges would allow users to modify tape records beyond their intended span of control and/or bypass the security mechanisms of the STAR software.
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.

Checks

All SSMMGRILES Privileges

The reviewer will check the Toolkit Media Manager User-IDs Report to verify that no unauthorized users have access to the SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRILESBYPASS privileges. If any active users have all of these privileges beyond that specified for their profile and the access is not documented on the user’s SAAR, this is a finding.

Fixes

All SSMMGRILES Privileges

Remove the combined SSMMGRILES1, SSMMGRILES2, SSMMGRILES3, and SSMMGRBYPASS privileges from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.570.00 V0000687 CAT II Deactivating Userids that have Never Signed On

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.4

Vulnerability The IAO is not deactivating userids that have never signed on.

Vulnerability Discussion Dormant userids present a means of unauthorized system access. A userid that has never signed on presents a unique vulnerability because the initial password is still assigned to the userid. If proper password construction rules are not followed, this initial password may be easily guessed.
The IAO will identify userids are installed but never signed on to the system and implement appropriate corrective actions.

Checks

Never Sign on Userids

The reviewer will check the Toolkit Dormant User-IDs (Never On) Report to verify that there are no userids that have never signed on to the system. If active users do not sign on in more than three days from creation or reactivation, this is a finding.

Fixes

Never Sign On Userids

Review all dormant userids and deactivate those userids that have never signed on. Educate subadministrators on the risks associated with staging userids and emphasize the need to activate and assign userids only when needed.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.580.00 V0000688 CAT II The IAO is not deactivating dormant userids

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.4

Vulnerability The IAO is not deactivating dormant userids.

Vulnerability Discussion If dormant userids (inactive for more than 35 days or 65 days for SBSS and CAMS users) remain enabled, there is a risk of unauthorized users or users who are no longer authorized to gain access to the system.
The IAO will identify userids are dormant and implement the appropriate corrective actions.
The IAO will deactivate a userid when notified and the user will no longer require access.

Checks

Dormant Userid

The reviewer will check the Toolkit Dormant (On Before) Report to verify that all dormant userids are deactivated. If the domain is supporting CAMS or SBSS, the reviewer will cross out or delete these userids from the Report if the days of inactivity are 65 days or less. If active userids are identified as being dormant, this is a finding.

Fixes

Dormant Userid

Review the Dormant Report regularly and deactivate any dormant userids..

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.600.00 V0000742 CAT II Access to Print Viewing Utilities

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 12.7

Vulnerability There is unrestricted access to print viewing utilities allowing any demand user to access all print files on the system.

Vulnerability Discussion If users have unrestricted access to print viewing utilities, they could gain unauthorized access to another sites print files and reroute, delete, and/or manipulate these files.
The SA will ensure accesses to print viewing utilities are restricted in accordance with this STIG requirement.

Checks

Print Utility Access

For DISA sites.
On ALN and CAMS CDB systems, the reviewer check for the presence of the @SMQ processor in an unprotected file. If this processor is found in an unprotected file, this is a finding. If this processor cannot be found, the reviewer will check the Toolkit TERMRUN$ Report to verify that the only authorized userids can access the TERMRUN$ interface. If the userids on this report do not have the access to TERMRUN$ documented on the user’s SAAR this is a finding.
For DNMC and DFAS-IN systems.
The reviewer will find out how these processors are restricted (for example, located in a protected file, requires MODPS$, etc.). Then the reviewer will verify that the restriction is enforced and that userids allowed access to the processors have this access documented on the user’s SAAR. Finally, the reviewer will check the Toolkit TERMRUN$ Report as described for ALN sites. If the print processors are not secured, there are unauthorized users with access to the processors, or there are unauthorized users with TERMRUN$ access, this is a finding.

Fixes

Print Viewing Utilities

Restrict access to print viewing processors in accordance with the Unisys STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.610.00 V0000639 CAT II SSAGNAME privilege

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 6.2.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 6.2.2

Vulnerability Unauthorized users have access to the SSAGNAME privilege.

Vulnerability Discussion The SSAGNAME privilege is needed to update the EZLOAD userid database and could be used to give unauthorized users the ability to reload or rename unsecured files on the system. This could lead to the placement of erroneous or obsolete files on the system resulting in a loss of data integrity or denial of service to the customer.
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.

Checks

DISA Sites SSAGNAME

For DISA sites:
The reviewer will check the Toolkit SSAGNAME Report to verify that unauthorized userids do not have access to the SSAGNAME privilege.. If any userids other the Master userid, SIMAN Administrators, and System Standard Batch userids have access to the SSAGNAME privilege appear on this Report, this is a finding.

Fixes

DISA Site SSAGNAME

Ensure only authorized users have the SSAGNAME privilege.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.614.00 V0004095 CAT II Userids exist that do not have a security record

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Userids exist that do not have a security record.

Vulnerability Discussion Userids that do not have a security record receive the system default security attributes of the system which may contain privileges the user is not authorized to have. The SA will ensure all userids have a security record.

Checks

Userid Security Record

The reviewer will check the Toolkit SACRD Report to verify that all userids have a security record. If there are any userids on the report, this is a finding.

Fixes

Userid Security Record

Give all userids a security record and assign the minimum privileges and interface access that the user needs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.616.00 V0004096 CAT II Userid Record Access of Private

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Unauthorized userids do not have record access Private.

Vulnerability Discussion Userids that do not have record access Private set are restricted to Subsystem Userids that control software subsystems and should not be set for normal userids.
The SA will ensure all userids have a record access of Private set.

Checks

Userid Record Access

The reviewer will verify that all non subsystem userids have “Record Access” set to private in the Userid Access section. SSO Montgomery has released this set of queries for checking the record access of a userid to make sure it is set to Private. These queries are called RecAccess-ACT, RecAccess-ALL, and RecAccess-DIS. ACT will identify all active userids, ALL will identify all userids, and DIS will identify only disabled userids. The reviewer will need to change the host-ID in the query for each host checked. If userids, other than fixed gate subsystem userids, appear on these queries, is a finding.

Fixes

Userid Record Access

Set Record Access Private for all non Subsystem Userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.616.01 V0006439 CAT II DISA User to Create Unowned Files

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Unauthorized users do not have the "user to Create Only Unowned Files' flag set for their userid.

Vulnerability Discussion The applications written for the DISA sites depend on files being private by account or private by project not private by userid. If this value is not set sensitive information may become compromised. Additionally, this complicates file recovery if the creating userid is removed from the system which can lead to loss of access to data.
For DISA sites, the SA will ensure all userids has “User to Create Only Unowned Files” set.

Checks

DISA Unisys Unowned Files

The reviewer will verify that all unauthorized userids have the “User to Create Only Unowned Files” flag set. SSO Montgomery has developed a set of queries for checking whether the userid can create only unowned files. These queries are called UnOwned-ACT, UnOwned-ALL, and Unowned-DIS. ACT will identify all active userids, ALL will identify all userids, and DIS will identify only disabled userids. The reviewer will need to change the host-ID in the query for each host checked. If userids appear on these queries and this privilege is not documented on the user’s SAAR, this is a finding.
Note that the userid that CMS 1100 executes under is allowed to own files.

Fixes

DISA Unisys Unowned files

Set the ôUser to Create Only Unowned Filesö flag for all unauthorized userids. Locate all files owned by any unauthorized userid and make the files unowned.
NOTE: The IAO should not alter any fixed gate subsystems userids if they appear on these queries. Also, the IAO should be very careful of modifying system type userids. If there are any questions, the IAO should contact SSO Montgomery for assistance.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.616.02 V0006440 CAT II User to Create Only Unowned Files

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Unauthorized users can create unowned files.

Vulnerability Discussion It is not easy and sometimes not possible to verify which user created a file if the userid that created the file can create unowned files.
The SA will ensure all userids, except documented exceptions do not have “User to Create Only Unowned Files” set.

Checks

Unisys Unowned Files

The reviewer will verify that no unauthorized userid has the “User to create Only Unowned Files” flag set.
The reviewer will execute the following sequence in a demand session.

```
    @SIMAN,B
     Display Userid = !ALL breakpoint = USERID*ALL ;
     @eof
```

The reviewer will then edit the file USERID*ALL.
Then locate “Unowned Files”. The reviewer will verify that any userid other than a subsystem userid has this privilege documented on the user’s SAAR. If there are any undocumented and therefore unauthorized userids with the “User to Create Only Unowed Files” flag set this is a finding.

Fixes

Unisys Unowned Files

Remove the ôUser to Create Only Unowned Filesö flag from all unauthorized userids. Locate any unowned files created by these userids and modify them to be owned by the userid. This will be difficult if not impossible. Locate any unowned files on the system and if their ownership cannot be determined and it cannot be determined that they must remain unowned, modify the files making them owned by the userid used to run the FAS backup and restore runs.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.618.00 V0004097 CAT II Read Executive GRS

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Unauthorized userids exist that do not have Can only Read Executive GRS set.

Vulnerability Discussion Any value other than Read Executive GRS set in an unauthorized userid record will allow user privileges that can lead to system corruption and denial of system access.
The SA will ensure all functional userids have “Can only read Executive GRS” set in the SUBSYSTM screen.

Checks

Read Executive GRS

The reviewer will verify that functional users only have the Read Executive GRS set in the Subsystem Access section of their security record. SSO Montgomery has released one set of queries so the reviewer can verify this checklist item. These queries will check for userid records that do not have the Read Executive GRS flag set. These queries are called ReadGRS-ACT, ReadGRS-ALL, and ReadGRS-DIS. ACT will identify all active userids, ALL will identify all userids, and DIS will identify only disabled userids. The reviewer will need to change the host-ID in the query for each host the IAO wants to check. The only userids that should have the Can Write Executive GRS flag set are the subsystem userids, System Standard Batch Userid and high-level Technical Support personnel. If userids show up on these queries that do not have this access documented on the user’s SAAR, this is a finding.

Fixes

Read Executive GRS

Remove any Processor Privileges other than Read Executive GRS from unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.620.00 V0000553 CAT II Userid Maximum Days of Inactivity

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.6

Vulnerability Userids have the maximum days of inactivity set greater than the standard allows.

Vulnerability Discussion If a userid exceeds the maximum days of inactivity standard, there is a greater chance for the userid and password to be compromised by unauthorized personnel.
The SA will ensure no userid, except documented exceptions, has “maximum days of inactivity” set to a value greater than 35.

Checks

Maximum days of Inactivity

The reviewer will check the Toolkit Non-Standard Max-Activity Report to verify that unauthorized users do not have their “maximum Days of Inactivity set to more than 35 days.
For systems supporting CAMS or SBSS, the reviewer cross out or delete all CAMS and SBSS userids if they have the days of inactivity parameter set to 65 days or less.

For the Demand RSI, SLS, and other system userids as specified in the Unisys STIG can have this parameter set to 365 days and the reviewer will cross out or delete them from the Report. Currently, these userids are QUIKST, IPF, Scheduler, VTHSRV, xxEZ00, and xxJSTM. If active userids are set to more than 35 days, this is a finding.

Fixes

Maximum days of inactivity

All userids (except the Security Officers userid, SIMAN Administrators, CAMS userids, SBSS userids, and select Demand RSI userids) should be set up with a maximum of 35 days inactivity. CAMS and SBSS userids are authorized a 65 days of inactivity setting. Select Demand RSI userids can be set to 365 days of inactivity. The Security Officer and SIMAN Administrator userids can be set to zero days of inactivity.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.630.00 V0000690 CAT II Maximum Days of Inactivity Siman Disable Userid

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.6

Vulnerability Unauthorized userids have the maximum days of inactivity SIMAN Disable User-ID feature deactivated.

Vulnerability Discussion If a userid has the maximum days of inactivity SIMAN Disable Userid feature deactivated, there is a greater chance for the userid and password to be compromised by unauthorized personnel.

Checks

Max Inactivity Disable Userid

The reviewer check the Toolkit Non-Standard Max-Activity Report to verify that unauthorized userids do not have the SIMAN Userid Disable feature disabled by having their maximum days of inactivity set to zero. If any userids, other than the Security Officer’s userid and SIMAN Administrators userids, are set to zero, this is a finding.

Fixes

Max Inactivity Disable Userid

All userids (except the Security Officers userid, SIMAN Administrators, CAMS and SBSS userids, and select Demand RSI userids) should be set up with a maximum of 35 days inactivity. All CAMS and SBSS userids are authorized a 65 days of inactivity setting. Select Demand RSI userids, as documented in the Unisys STIG, can be set to 365 days of inactivity. The Security Officer and SIMAN Administrator userids can be set to zero days of inactivity.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.640.00 V0000689 CAT II Userids have the maximum invalid password attempts

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.6

Vulnerability Userids have the maximum invalid password attempts set greater than the standard.

Vulnerability Discussion If a userid exceeds the maximum number of invalid password attempts, there is a greater chance for the userid and password to be compromised by unauthorized personnel.
The SA will ensure all userids, except documented exceptions, and has a setting of three in the maximum invalid password attempts field.

Checks

Invalid Password Attempts

The reviewer will check the Toolkit Non-Standard Password Attempts Report to verify that no unauthorized user has an invalid value for the maximum invalid password attempts. If active userids except for the documented exceptions has the invalid password attempts parameter is set to any value greater than three, this is a finding.
Documented exceptions include.
The Security Officer’s userid.
SIMAN Administrators
QUIKST
IPF
Scheduler
VTHSRV
xxEZ00
xxJSTM

Fixes

Invalid Password Attempts

All userids (except the Security Officers userid, SIMAN Administrators, and select Demand RSI userids) should be set up with a maximum of three invalid password attempts. The Security Officers userid, SIMAN Administrators, and select Demand RSI userids, as documented in the Unisys STIG, may be set to zero invalid password attempts.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.650.00 V0000691 CAT II SIMAN Disable User-ID Invalid Password Attempts

8500.2 IA Control: IAAC-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.3.2, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.6

Vulnerability Unauthorized userids have the maximum invalid password attempts SIMAN Disable Userid feature deactivated.

Vulnerability Discussion If a userid has the maximum invalid password attempts SIMAN Disable Userid feature deactivated, there is a greater chance for the userid and password to be compromised by unauthorized personnel.
The SA will ensure no userid, except documented exceptions, has the SIMAN Disable Userid feature disabled by having “invalid password attempts” set to zero.

Checks

Invalid Pass Attempt SIMAN

The reviewer check the Toolkit Non-Standard Password Attempts Report to verify that no unauthorized userid has the SIMAN Userid Disable feature disabled by having the invalid password attempts parameter set to zero. If any userids, other authorized userids, are set to zero, this is a finding.
The authorized userids are:
System userids identified in the Unisys STIG:
The Security Officer’s userid
SIMAN Administrators
The Demand RSI userids identified in the Unisys STIG:
QUIKST
IPF
Scheduler
VTHSRV
xxEZ00
xxJSTM.

Fixes

Invalid Pass Attempt SIMAN

All userids (except the Security Officers userid, SIMAN Administrators, and select Demand RSI userids) should be set up with a maximum of three invalid password attempts. The Security Officers userid, SIMAN Administrators, and select Demand RSI userids, as documented in the Unisys STIG, may be set to zero, this is a finding.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.650.10 V0006438 CAT II Password Notices May be Ignored

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.3.11.1

Vulnerability Unauthorized users have the "password notices may be ignored" value set to a value other than zero.

Vulnerability Discussion This value controls the maximum number of consecutive successful log-ons where the operating system gives a password expiration notice, in which the user does not change passwords. When this number is reached, the operating system disables the userid. Since this is a count and not the number of days, the user could have a password in use for many more days than the maximum allowed before the userid is disabled.
The SA will ensure all userid, except documented exceptions, have “ password notices may be ignored” set to zero.

Checks

Unisys Max Pass Ignore

The reviewer will verify that no userid has the “password Notices may be ignored" value set to a value other than zero .
The reviewer will execute the following sequence in a demand session.

```
@SIMAN,B
 Display Userid = !ALL breakpoint = USERID*ALL ;
 @eof
```

The reviewer will then edit the file USERID*ALL.
Then locate “Maximum 1 password-expired notices” thru “Maximum 63 password-expired notices”. If any of these locates gets a hit, this is a finding.

Fixes

Unisys Max Pass Ignore

Set the ôpassword Notices may be ignoredö value to zero for all userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.654.00 V0004098 CAT II Users Not Properly Validated Before Userid Enabled

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.3.2

Vulnerability Users are not properly validated before their userids are enabled.

Vulnerability Discussion Failure to properly validate a user before enabling a disabled userid can lead to the compromise of the userid and password allowing an unauthorized user access to sensitive data.
The SA will ensure users identity is verified before their userids are enabled.

Checks

User identity Verification

The reviewer will interview the TASOs, SAs, and/or IAOs to verify that there is a process in place to verify the users identity prior to enabling a disabled userid. For example, the individual could provide the last six numbers of their SSN to the TASO, SA, or IAO for verification against the individual’s SAAR.

Fixes

User Identity Validation

Develop a written procedure for validating a user's identity prior to enabling a disabled userid, distribute the policy to all individuals that have the ability to enable userids and instruct them to use the policy.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.660.00 V0000621 CAT II Userids have an @SIMAN in userid

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1

Vulnerability Userids have an @SIMAN in their userid control image.

Vulnerability Discussion If a userid with an @SIMAN in the control image is compromised, this control image will immediately place an unauthorized user into the system security processor (SIMAN). If the compromised userid is identified in SIMAN as a subadministrator, an unauthorized user could add, modify, or delete userids that were created by this subadministrator.
The SA will ensure userids do not have an @SIMAN in their control image.

Checks

SIMAN Control Image

The reviewer will check the Toolkit @SIMAN Control Image Report to verify that no userid is identified on this report as having @SIMAN in their Control Image.

Fixes

SIMAN Control Image

Remove @SIMAN from the Control Image field for all userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.670.00 V0000622 CAT II Unauthorized Ability to Enter Run Image

8500.2 IA Control: ECLP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1

Vulnerability Unauthorized userids have the ability to enter their own run image.

Vulnerability Discussion Many sites have set up their Automated Message System (AMS) to intercept messages from certain run-ids and depending on the run-id, AMS will perform certain keyins on the operator's console. At other sites, operators will accomplish certain keyins if a request is made by a particular run-id (for example, an individual in Technical Support). If unauthorized users are allowed to enter their own run image, they can spoof these special run-ids and cause keyins to be performed at inappropriate times. These actions may threaten the data integrity of an application or result in a denial of service to supported customers.
For DISA sites, the SA will ensure only authorized select site Profile 2 userids have the ability to enter their own run image.

Checks

Enter Run Image

The reviewer will check the Toolkit User Entered Run Image Report to verify that no unauthorized userid has the ability to enter the run image at sign on. If any userids, other than the IPF userid or UOSS userid (if used), appear in this report as having the ability to enter their own run image and this requirement is not documented on the user’s SAAR, this is a finding.

Fixes

Enter Run Image

Remove the ability to enter their own run image from all unauthorized userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.680.00 V0000623 CAT II Unauthorized Alternate Run-ID

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1

Vulnerability Unauthorized userids have an alternate run-ID in their userid record.

Vulnerability Discussion Many sites have set up their Automated Message System (AMS) to intercept messages from certain run-ids and depending on the run-id, AMS will perform certain keyins on the operator's console. At other sites, operators will accomplish certain keyins if a request is made by a particular run-id (for example, an individual in Technical Support). If a subadministrator sets up a userid with one of these special run-ids as an alternate run-id, the special run-id can be spoofed and unauthorized keyins could be performed at inappropriate times. These actions may threaten the data integrity of an application or result in a denial of service to supported customers.
For DISA sites, the SA will ensure only authorized userids have an alternate run-ID.

Checks

Alternate Run-ID

The reviewer will check the Toolkit Alternate Run-ID Report to verify that no unauthorized userids have alternate run-IDs.. Only userids on a DNMC system are authorized to have alternate run-IDs. If this is not a DNMC system and there are userids in the report, this is a finding.

Fixes

Alternate Run-ID

Review all userids to ensure no unauthorized userids have an alternate run-ID in their userid record. The only exceptions are the userids belonging to the DNMC applications. These userids have a 3 character site prefix with the last 5 or 6 characters making them unique. The use of alternate run-IDs is the only way to make these run-ids unique in the DNMC report distribution system and are automatically generated by INFOQUEST.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.690.00 V0000692 CAT III Authorized alternate run-IDs improper syntax

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1

Vulnerability Authorized alternate run-IDs do not match the last five or six characters of the userid. (DNMC Sites Only)

Vulnerability Discussion Unless alternate run-IDs match the last five or six characters of the userid, there is a risk of inadvertently distributing reports with sensitive data to unauthorized personnel.
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.

Checks

Alternate Run-ID Syntax

For DNMC systems only. The reviewer will check the Toolkit Alternate Run-ID Report and identify any alternate run-ID that does not match the last five or six characters of the userid. If any are found, this is a finding.

Fixes

Alternate Run-ID Syntax

Ensure all alternate run-IDs match the last five or six characters of the userid.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.700.00 V0000693 CAT II Authorized alternate run-IDs are duplicated

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.1.1, UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1.4.5.1

Vulnerability Authorized alternate run-IDs are duplicated (DNMC Sites Only)

Vulnerability Discussion Unless unique alternate run-IDs are used, there is a greater risk of inadvertently distributing reports with sensitive data to unauthorized personnel.
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.

Checks

Duplicate Alternate Run-IDs

For DNMC systems only. The reviewer will check the Toolkit Alternate Run-ID Report and identify any alternate run-ID that is duplicated. If any are found, this is a finding.

Fixes

Duplicate Alternate Run-IDs

Review all alternate run-IDs and ensure none of these run-IDs are duplicated.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.710.00 V0000707 CAT II Group or shared userids exist on the system

8500.2 IA Control: IAIA-1, IAIA-2

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 3.1

Vulnerability Group or shared userids exist on the system.

Vulnerability Discussion Sharing of userids negates the ability of the IAO to positively identify userid actions to the responsible user.
The IAO will ensure group and shared userids are not used on the system.

Checks

Shared Userids

The reviewer will check the Toolkit Shared User-IDs Report for indications of shared userids. If there is any occurrence of the same userid signed on to unlike terminal-IDs and the user’s run-ID is incremented, then this is a potential problem. The reviewer will find out if there is any documentation on the situation. The only known exception should be the userid that is used to sign on to the Supply RPS 057 main terminal and the RPS room should maintain a log transferring responsibility of this userid at each shift turnover. NOTE: This RPS 057 userid should not have access to database or other dangerous utilities.
If shared userids exist, this is a finding.

Fixes

Shared Userids

Ensure each userid is used by only one person and that all users are instructed not to share their userids.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.720.00 V0000557 CAT II Security tapes are not physically secured

8500.2 IA Control: DCPB-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 4.1.1.2

Vulnerability Security tapes are not physically secured.

Vulnerability Discussion If security tapes are not physically secured, unauthorized users can request them and corrupt the data on the tape or gain access to information in the system security environment.
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.
The IAO will ensure the AUTOLIB flag in STAR is removed on tapes used to create the Security Merge SECTAPE.
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.

Checks

Security Tape Storage

The reviewer will check the Toolkit Silo Security Files Report. If there are any tapes listed, this is a finding.

Security Tape Storage Intervie

The reviewer will interview to verify that the security tapes are stored in the computer room.

Fixes

Security Tape Storage

Security tapes created by the SV process will be physically secured (not kept in tape silos) and kept separate from other tapes.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

S104.720.01 V0006505 CAT II SEC,SAVE tapes in a Tape Silo

8500.2 IA Control: DCBP-1

References: UNISYS SECURITY TECHNICAL IMPLEMENTATION GUIDE 4.1.1.2

Vulnerability The IAO has no documentation of the mitigating controls in place for security tapes created using the SEC,SAVE keyin and being stored in a tape silo.

Vulnerability Discussion If the security database backup tapes are stored in a tape silo, additional security needs to be in place to stop unauthorized users from accessing the tapes. This can be done by tape library settings or AMS routines. Allowing the tapes to be stored in the tape silo allows the site to remove hardware that is only being used for security tape backups and restores.
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.

Checks

Unisys SEC Tapes in Silo

The reviewer will interview the IAO to verify that there are sufficient mitigating controls implemented to protect security tapes created by the SEC,SAVE command from being accessed by unauthorized users.

Fixes

Unisys SEC Tapes in Silo

Develop and implement adequate mitigating controls to protect security tapes created by the SEC,SAVE command and stored in a tape silo from unauthorized access or manually eject the tapes immediately after creation.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes: