CIS IBM i V7R5M0 Benchmark

v1.1.0 - 09-19-2023

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

Table of Contents

Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This standard provides the baseline security requirements for IBM i systems.
An owner must be designated for IBM i electronic information assets including the programs and the data labeled as Confidential or Highly Restricted as defined by the company's data classification. The owner must designate an administrator who is responsible for the secure configuration and maintenance. Privileges to modify the functionality and services supported by the IBM i must be restricted to the administrator and approved by the IBM i owner.
Roles and responsibilities on the IBM i must be clearly defined and documented, and address system, application and data security and operational responsibilities. Roles must include resource owners who are responsible for ensuring that appropriate security controls are defined, implemented and maintained and are ultimately accountable for security, access and performance on their designated resource.
Development and production roles and responsibilities must be kept separate to ensure an appropriate segregation of duties. Security administration and/or audit roles and responsibilities should be defined to provide validation of activities performed by the administrators and other privileged users.

Intended Audience

These standards apply to all applications, databases and connections to the IBM i.

Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Corporate/Enterprise Environment (general use)

  Items in this profile intend to:

```
-be practical and prudent;

-provide a clear security benefit; and

-not negatively inhibit the utility of the technology beyond acceptable
means.
```

- **Level 2**

  High Security/Sensitive Data Environment (limited functionality)

  Items in this profile may have the following characteristic(s):

```
-are intended for environments or use cases where security is paramount

-acts as defense in depth measure

-may negatively inhibit the utility or performance of the technology.
```

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Author
Bruce Bading

Contributor
Thomas Barlen
Robert Andrews
Terry Ford
Robin Tatam
Dan Riehl
Tim Mullenbach
Steve Will
Bálint Varga-Perke

Editor
Edward Byrd

Recommendations

1 Access Control

The following paragraphs define the controls and parameters for access control to the IBM i and its resources.

Critical, sensitive, confidential and/or highly restricted objects must be *EXCLUDEd from the *PUBLIC and private authorities, group authorities and/or authorization lists must be used to secure these objects. The minimum authority required to perform specific functions must be granted and excessive authorities must be removed.

Periodic reviews of critical, sensitive, confidential and/or highly restricted objects objects must be performed to ensure that proper access control is maintained.

https://www.ibm.com/docs/en/i/7.5?topic=concepts-resource-security

2 Adopted Authority

You should use adopted authorities with care to prevent possible security risks. Allowing a program to run using adopted authority is an intentional release of control. You permit the user to have authority to objects, and possibly special authority, which the user will not normally have. Adopted authority provides an important tool for meeting diverse authority requirements, but it should be used with care:

https://www.ibm.com/docs/en/i/7.5?topic=authority-adopted-risks-recommendations

- Adopt the minimum authority required to meet the application requirements using the Principle of Least Privilege (PoLP). Adopting the authority of an application owner is preferable to adopting the authority of QSECOFR or a user with any special authorities, especially *ALLOBJ.
- Carefully monitor the function provided by programs that adopt authority. Make sure that the programs do not provide a means for the user to access objects outside the control of the program, such as command line entry capability.
- Make sure that programs that adopt authority and call other programs perform library qualified calls. Do not use the library list (*LIBL) on the call.
- Control which users are permitted to call programs that adopt authority. Use menu interfaces and library security to prevent these programs from being called without sufficient control.
- Administrative and third-party libraries such as Profile and System Administration, High Availability and Change Management libraries that contain programs that adopt powerful special authorities shall be controlled with *PUBLIC *EXCLUDE access and grant only authorized user/groups access whose job roles require such access.

3 User Profiles

User Profiles provide identity authentication into your system. Designing them well can help you protect your system and customize it for your users. Each user profile is a *USRPRF object in system library QSYS, that contains a password, several security related parameters and a list of the objects the user owns.

Resource security is an important aspect of your system security and defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects. User profiles are a specific type of resource that exists as a *USRPRF object type in the system library QSYS and in many ways is similar to the UNIX/Linux etc/passwd or Active Directory SAM files. *USRPRF resource objects should be secured and should grant only the *USRPRF resource authority to itself, the owner should be QSECOFR and the *PUBLIC should have an authority of *EXCLUDE.

Following are important aspects of IBM i user profiles that you should consider to properly secure your systems.

• Every user profile should be unique (no shared accounts).

• Every user should have a unique and non-trivial password of sufficient strength and complexity.

• Each individual user profile should have authorities and privileges commensurate with their specific job role.

• There are a total of eight administrative special authorities and each administrator should have the minimum special authority commensurate with their job role.

• Application users and groups should have no Special Authorities (*NONE) and be granted proper authority to resources (objects and file) commensurate with their job role.

• All *USRPRF objects should be authorized only to the *USRPRF owner and the user profile itself and the *PUBLIC authority should be *EXCLUDE and no private authorities should be granted to any *USRPRF objects.

https://www.ibm.com/docs/en/i/7.5?topic=reference-user-profiles
https://www.ibm.com/docs/en/i/7.5?topic=fields-special-authority
https://www.ibm.com/docs/en/i/7.5?topic=reference-resource-security

*3.1 (L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority) (Automated)*

Profile Applicability:

- Level 1

Description:

Resource security is an important aspect of your system security and defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects. User profiles are a specific type of resource that exists as a *USRPRF object type in the system library QSYS and in many ways is similar to the UNIX/Linux etc/passwd or Active Directory SAM files. *USRPRF resource objects should be secured and should grant only the *USRPRF resource authority to itself, the owner should be QSECOFR and the *PUBLIC should have an authority of *EXCLUDE.

Granting resource authorities to *USRPRF objects in system library QSYS creates a vulnerability that allows an ad-hoc swap with the *USRPRF resource without requiring a password or credentials by those authorized and will inherit privileges and authorities that may elevate the scope of the original user's access resulting in an exploitable vulnerability.

*PUBLIC authority to all user profiles should be *EXCLUDE, and where necessary, application profile swaps should be programmatically performed securely using the IBM i swap APIs similar to how UNIX setUID and setGID bits function. By design as shipped, the IBM i provides only the following three *USRPRF objects with a *PUBLIC authority greater than *EXCLUDE to allow printing and database functions:

QDBSHR QDBSHRDO QTMPLPD

Rationale:

Granting *PUBLIC authority of *USE or greater to any *USRPRF object allows an attacker to swap with these profiles and use their privileges and authorizations without their passwords or credentials outside of designed application access requirements from a system command line and from remote facilities like remote command, ODBC, etc. *PUBLIC refers to all authenticated users.

A user defined authority (USER DEF) including a minimum of Read authority allows others to display *ALL attributes of a profile including object ownership and authorities. Granting the *PUBLIC authority to any profile other than QDBSHR, QDBSHRDO and QTMPLPD is a security risk and may lead to privilege escalation whereby a user may increase the scope and scale of their access permissions that impacts the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Note that the three IBM profiles that grant the public and authority that is not exclude (QDBSHR QDBSHRDO QTMPLPD) have less than *USE so cannot be swapped to. Also, QDBSHR and QDBSHRDO are prevented from being swapped to by internal checks (can't do a Get Profile Handle). Authorities to these three profiles should never be changed.

Impact:

Functions involving profile swaps may be impacted.

Audit:

• On a command line, type STRSQL and press Enter
• Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT ALL
SYS_ONAME, OBJTYPE, USER_NAME, OBJ_AUTH
FROM QSYS2/OBJ_PRIV T01
WHERE OBJTYPE = '*USRPRF'
AND SYS_ONAME NOT IN ('QDBSHR', 'QDBSHRDO', 'QTMPLPD')
AND USER_NAME = '*PUBLIC'
AND OBJ_AUTH <> '*EXCLUDE'
```

• Verify that the display returns no *PUBLIC authorized objects.

Remediation:

To establish the recommended configuration, change any *USRPRF objects identified in the audit to the default shipped and creation value *EXCLUDE to secure all user profiles from malicious use.

GRTOBJAUT OBJ(<*xxxxxx*>) OBJTYPE(*USRPRF) USER(*PUBLIC) AUT(*EXCLUDE) REPLACE(*YES)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/crtusrprf.htm
2. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
3. https://www.ibm.com/docs/en/i/7.5?topic=reference-resource-security
4. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/apis/QWTSETP.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

*3.2 (L1) User Profile (*USRPRF) Access Controls (Private authority) (Automated)*

Profile Applicability:

- Level 1

Description:

Resource security is an important aspect of your system security and defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects. User profiles are a specific type of resource that exists as a *USRPRF object type in the system library QSYS and in many ways is similar to the UNIX/Linux etc/passwd or Active Directory SAM files. *USRPRF resource objects should be secured and should grant only the *USRPRF resource authority to itself, the owner should be QSECOFR, the *PUBLIC should have an authority of *EXCLUDE and no other private should exist. The one exception is that group profiles shall grant a User Defined (USER DEF) authority to all group members and no other private authorities shall exist other than the group members.

Granting resource authorities to *USRPRF objects in system library QSYS creates a vulnerability that allows an ad-hoc swap with the *USRPRF resource without requiring a password or credentials by those authorized and will inherit privileges and authorities that may elevate the scope of the original user's access resulting in an exploitable vulnerability.

No private authorities should exist, and where necessary, application profile swaps should be programmatically performed securely using the IBM i swap APIs similar to how UNIX setUID and setGID bits function.

All Private authorities to all user profiles other than the owner’s and the profile itself should be removed.

Rationale:

Granting a private authority of *USE or greater to any *USRPRF object allows an attacker to swap with these profiles and use their privileges and authorizations without their passwords or credentials outside of designed application access requirements from a system command line and from remote facilities like remote command, ODBC, etc.

A user defined authority (USER DEF) including a minimum of Read authority allows others to display *ALL attributes of a profile including object ownership and authorities. Granting a private authority to any profile is a security risk and may lead to privilege escalation whereby a user may increase the scope and scale of their access permissions that impacts the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

Functions involving profile swaps may be impacted.

Audit:

• On a command line, type STRSQL and press Enter
• Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT SYS_ONAME, OBJTYPE, USER_NAME, OBJ_AUTH
FROM QSYS2/OBJ_PRIV LEFT OUTER JOIN QSYS2/GROUPLIST
ON SYS_ONAME = GROUPNAME
WHERE OBJTYPE = '*USRPRF'
AND SYS_ONAME <> USER_NAME
AND USER_NAME <> OWNER
AND USER_NAME <> '*PUBLIC'
AND USERNAME IS NULL
AND SYS_ONAME CONCAT USER_NAME NOT IN
('QGATEQSNADS', 'QMQMQMQMADM', 'QMSFQTCP',
'QSPLJOBQSPL', 'QTCPQMSF', 'QTMHHTTPQCLUSTER')
```

• Verify that the display returns no privately authorized objects.
• SYSTEM_OBJECT_NAME is the *USRPRF object that is privately authorized to the USER_NAME profile.

The one exception is that group profiles shall grant a User Defined (USER DEF) authority to all group members and no other private authorities shall exist other than the group members.

Ensure that the group members do not have more authority than was given by the system – USER DEF = *OBJOPR, *OBJMGT, *READ, *ADD, *UPD, and *DLT. Do not give the members of the group *EXECUTE so the members of the group do not have *USE authority to the group profile which would allow all members to swap to the group profile. The following SQL should be run to ensure that no group members have more authority than was given by the system.

• On a command line, type STRSQL and press Enter
• Copy or type the following SQL statement to the terminal and press Enter.

SELECT

SYS_ONAME, OBJTYPE, USER_NAME, OBJ_AUTH,

OBJEXIST, OBJALTER, OBJREF

FROM QSYS2/OBJ_PRIV LEFT OUTER JOIN

QSYS2/GROUPLIST

ON SYS_ONAME = GROUPNAME

WHERE OBJTYPE = '*USRPRF'

AND SYS_ONAME <> USER_NAME

AND USER_NAME <> OWNER

AND USER_NAME <> '*PUBLIC'

AND USER_NAME = USERNAME

AND OBJEXIST CONCAT OBJALTER CONCAT OBJREF <> 'NONONO'

Remediation:

To establish the recommended configuration, change any *USRPRF (SYSTEM_OBJECT NAME) objects identified in the audit to the default shipped and creation value *EXCLUDE to secure all user profiles from malicious use.
RVKOBJAUT OBJ(<*xxxxxx*>) OBJTYPE(*USRPRF) USER(<*xxxxxx*>) AUT(*ALL)
• Note: Replace xxxxxx for OBJ(<*xxxxxx*>) with the SYSTEM_OBJECT_NAME from the audit
• Replace xxxxxx for USER(<*xxxxxx*>) with the USER_NAME from the audit

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/crtusrprf.htm
2. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
3. https://www.ibm.com/docs/en/i/7.5?topic=reference-resource-security
4. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/apis/QWTSETP.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

*3.3 (L1) User Profile (*USRPRF) Object Ownership (Automated)*

Profile Applicability:

- Level 1

Description:

Resource security is an important aspect of your system security and defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects. User profiles are a specific type of resource that exists as a *USRPRF object type in the system library QSYS and in many ways is similar to the UNIX/Linux etc/passwd or Active Directory SAM files. *USRPRF resource objects should be secured and should grant only the *USRPRF resource authority to itself, the owner should be QSECOFR and the *PUBLIC should have an authority of *EXCLUDE.

Granting resource authorities to *USRPRF objects in system library QSYS creates a vulnerability that allows an ad-hoc swap with the *USRPRF resource without requiring a password or credentials by those authorized and will inherit privileges and authorities that may elevate the scope of the original user's access resulting in an exploitable vulnerability.

QSECOFR should be the owner of all profiles and new profile ownership can be automated through an exit program registered to the QIBM_QSY_CRT_PROFILE exit point. This follows the same security design of UNIX/Linux where the etc/passwd file is owned by root and the Active Directory SAM file is owned by the system profile.

All IBM Supplied Profiles shall be owned by QSYS with the following exceptions:

• QFAXMSF shall be owned by QAUTPROF

• QRDARS400xx shall be owned by QRDARS400

• QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI

Non-IBM (user created) profiles shall be owned by QSECOFR.

Rationale:

Granting group or private ownership to any *USRPRF object allows an attacker to swap with these profiles and use their privileges and authorizations without their passwords or credentials outside of designed application access requirements from a system command line and from remote facilities like remote command, ODBC, etc. Group or private ownership of any *USRPRF resource in library QSYS is a security risk and may lead to privilege escalation whereby a user may increase the scope and scale of their access permissions that impacts the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

A secure password reset/change program can swap securely with the owner QSECOFR to provide and validate all password/parameter settings and limit access [in accordance with / under] the Principle of Least Privilege (PoLP)..

Impact:

Functions involving profile swaps may be impacted.

Audit:

• On a command line, type STRSQL and press Enter
• Copy or type the following SQL statement to the terminal and press Enter.
SELECT ALL SYS_ONAME, OBJTYPE, OWNER FROM QSYS2/OBJ_PRIV
WHERE OBJTYPE = '*USRPRF' AND USER_NAME = '*PUBLIC'
AND OWNER NOT IN ('QSECOFR', 'QSYS')
• Verify that the display returns no ownership anomalies with the following valid exceptions.

- QFAXMSF shall be owned by QAUTPROF
- QRDARS400<*x*> shall be owned by QRDARS400
- QTIVOLI, QTIVROOT and QTIVUSER shall be owned by QTIVOLI

Remediation:

To establish the recommended configuration, change the owner of all non-IBM supplied *USRPRF objects to QSECOFR:
CHGOBJOWN OBJ() OBJTYPE(*USRPRF) NEWOWN(QSECOFR)
CUROWNAUT(*REVOKE)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
2. https://www.ibm.com/docs/en/i/7.5?topic=reference-resource-security
3. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/apis/QWTSETP.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

3.4 (L1) Administrative Special Authorities (Automated)

Profile Applicability:

- Level 1

Description:

Special authority is used to specify the types of actions a user can perform on system resources. A system administrator can be given one or more special authorities directly or through a group. System administrators should be granted administrative special authorities commensurate with their job roles.

Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes dividing mission or business functions and support functions among different individuals or roles, conducting system support functions with different individuals, and ensuring that security personnel who administer access control functions do not also administer audit functions. Because separation of duty violations can span systems and application domains, organizations consider the entirety of systems and system components when developing policy on separation of duties.

Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned organizational tasks.

Rationale:

Special authorities should be granted to administrators based on the Special authority (SPCAUT) parameter in the user profile. Based on the Principle of Least Privilege (PoLP), administrative privileges (special authorities) should be controlled, limited and monitored and non-administrative users should have no administrative special authority (SPCAUT = *NONE).

Granting any of the eight administrative special authorities must be done in consideration with the Principle of Least Privilege (PoLP) as defined by the NIST and regulatory compliance requirements.

Granting special authorities greater than the Principle of Least Privilege (PoLP) can allow privilege escalation, which is the process by which a user with limited access to IT systems can increase the scope and scale of their access permissions to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

Administrator functions performed with administrator special authorities may be impacted.

Audit:

PRTUSRPRF SELECT(*SPCAUT) SPCAUT(*ALL)
Type WRKSPLF and locate your spool file with the name QPSECUSR and User Data PRTUSRPRF. View the spool file output to ensure that all administrators listed with Special Authorities have the least privileges commensurate with their administrative job roles. Note that administrative Special Authorities are cumulative from User Profile and Group Profiles.
IBM supplied user profiles will appear in the report and should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

Remediation:

To establish the recommended configuration, lower all administrators to the special authorities commensurate with their job roles.
CHGUSRPRF USRPRF(<*xxxxxx*>) SPCAUT(<*xxxxxx*>)
Change all non-administrative *USER class users and groups to SPCAUT = *NONE:
CHGUSRPRF USRPRF(<*xxxxxx*>) SPCAUT(*NONE)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=fields-special-authority
2. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
3. https://www.ibm.com/docs/en/i/7.5?topic=fields-user-class
4. https://csrc.nist.gov/glossary/term/least_privilege

Additional Information:

The User class (USRCLS) parameter in the DSPUSRPRF, CRTUSRPRF and CHGUSRPRF commands does not define the privileges or special authorities available to the user. It is only used as a template in the CRTUSRPRF and CHGUSRPRF commands when *USRCLS is specified for the Special authority (SPCAUT) parameter in conjunction with a corresponding User class (USRCLS). Additionally, If no special authorities are specified when a user profile is created, the user class and the security level (QSECURITY) system value are used to determine the special authorities for the user. See the knowledge center links for more information on the User class (USRCLS) parameter.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

3.5 (L1) User Profile Action Auditing (Automated)

Profile Applicability:

- Level 1

Description:

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights:

• Act as part of the operating system or access system and other sensitive objects

• Back up objects, files and directories

• Restore objects, files and directories

• Take ownership of files or other objects

• Create, change and delete user profiles

• Change priority or end and control system and other user's jobs and spooled files.

• Start System Service Tools, debug programs and perform or alter service functions

• Trace communications and jobs

• Change, view and control system and resource auditing

• Change how the system and communications are configured

Actions of administrative special authorities allow auditors to monitor actions taken by administrators.

Rationale:

Auditing these events may be useful when investigating a security incident.

The CHGUSRAUD (Change User Audit) command allows a user with audit (*AUDIT) special authority to set up or change auditing for a user. The system value QAUDCTL controls turning auditing on and off. The auditing attributes of a user profile can be displayed with the Display User Profile (DSPUSRPRF) command.

Impact:

If no audit settings are configured, or if audit settings are too lax in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Audit:

PRTUSRPRF SELECT(*SPCAUT) SPCAUT(*ALL)
Type WRKSPLF to locate your spool file with the name QPSECUSR and User Data PRTUSRPRF. View spool file output and use the DSPUSRPRF command to ensure that all administrators with special authorities have an action auditing value of *CMD. Note that administrative Special Authorities are cumulative from User Profile and Group Profiles.
IBM supplied user profiles with the exception of QSECOFR should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

1. Type DSPUSRPRF For each of the users in the report and examine the action auditing value to ensure that *CMD action auditing is specified.
2. DSPUSRPRF USRPRF(<*xxxxxx*>) TYPE(*BASIC)

Remediation:

To establish the recommended configuration, change the action auditing value of all administrative special authority users to include *CMD action auditing:
CHGUSRAUD USRPRF(<*xxxxxx*>) AUDLVL(*CMD)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=fields-special-authority
2. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
3. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/chgusraud.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

3.6 (L1) Default Passwords (Automated)

Profile Applicability:

- Level 1

Description:

A profile has a default password when the profile's password matches the user profile name. A change was made in 7.5 so that the default for the password on CRTUSRPRF is *NONE. When you create new user profiles, consider assigning a unique, non-trivial password instead of using a default password. Additionally, shared accounts or a common account shared by many different individuals provides an attack vector because actions taken by these shared profiles cannot be attributed to a unique account as described in NIST Special Publication 800-53.

Rationale:

Default passwords provide an opportunity for someone to enter your system anonymously. Default passwords are easy to guess. Additionally, accounts with default passwords are often used for shared (non-unique) accounts. Tell the new user the password confidentially, such as in a “Welcome to the System” letter that outlines your security policies. Require the user to change the password the first time that the user signs on by setting the user profile to **PWDEXP(*YES)**.

Impact:

Shared passwords may be impacted.

Audit:

• On a command line, type STRSQL and press Enter
• Enter the following SQL statement and press Enter.

```
SELECT ALL
USER_NAME, STATUS, DFTPWD, PWDEXP
FROM QSYS2/USER_INFO T01
WHERE DFTPWD = 'YES'
```

Remediation:

To establish the recommended configuration, change the password of all user profiles with default passwords to a non-trivial password and set the password to expire.
CHGUSRPRF USRPRF(<*xxxxxx*>) PASSWORD(<*xxxxxx*>) PWDEXP(*YES)
Additionally, the command ANZDFTPWD ACTION (*DISABLE) should be added to a job schedule entry to periodically scan for and *DISABLE any profiles with *DEFAULT passwords, and system value QPWDRULES should contain the parameters *ALLCRTCHG and *LMTPRFNAME to prevent the creation of profiles with *DEFAULT passwords.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/anzdftpwd.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.7 Manage Default Accounts on Enterprise Assets and Software Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.	●	●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.2 Change Default Passwords Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers			

3.7 (L1) Inactive Profiles (Automated)

Profile Applicability:

- Level 1

Description:

Remove/disable inactive user profiles within 90 days.

Rationale:

Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access sensitive data.

Audit:

• On a command line, type STRSQL and press Enter
• Enter the following SQL statement and press Enter.
SELECT

USER_NAME, STATUS, LASTUSED, TIMESTAMP

FROM QSYS2/USER_INFO T01

WHERE STATUS = '*ENABLED'

AND LASTUSED <= 'yyyy-mm-dd'

AND TIMESTAMP <= 'yyyy-mm-dd'

OR STATUS = '*ENABLED'

AND TIMESTAMP <= 'yyyy-mm-dd'

AND LASTUSED IS NULL
Note: In the above SQL, enter the calendar date equal to 90 days prior to the audit or that of your inactive profile policy as the LASTUED date in the format yyyy-mm-dd. The date needs to be entered in 'yyyy-mm-dd' format enclosed in single ' marks as in the following example:
LASTUSED <= '2020-01-01'
TIMESTAMP < = '2020-01-01'
Note: Also enter the calendar date equal to a creation date equal to 90 days prior to the audit as the TIMESTAMP date in the format yyyy-mm-dd to ensure that recently created but not used profiles are not included in the analysis.
IBM supplied user profiles will appear in the report and should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

Remediation:

To establish the recommended configuration, remove/disable all inactive profiles displayed.
CHGUSRPRF USRPRF(<*xxxxxx*>) STATUS(*DISABLED)
Optional (recommended) on a regular basis such as 30-90 days after inactive profiles have been *DISABLED, they should be archived and removed.
DLTUSRPRF USRPRF(<*xxxxxx*>)
Note that when removing user profiles, there needs to be consideration of changing ownership of the objects they own.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
2. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/anzprfact.htm
3. https://www.ibm.com/docs/en/i/7.5?topic=information-disabling-user-profiles-automatically

Additional Information:

The ANZPRFACT command will determine if profiles have been inactive for a specified number of days. If a profile has been inactive for the specified number of days it will be disabled. The ANZPRFACT command can be added to a job scheduler to automatically disable inactive profiles.

Note: ANZPRFACT does not immediately detect inactive profiles. It adds a job schedule entry that runs every day at 1am to determine if you have profiles that have been inactive the specified number of days.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●
v7	16.9 Disable Dormant Accounts Automatically disable dormant accounts after a set period of inactivity.	●	●	●

3.8 (L1) User Profile With Non-Expiring Passwords (Automated)

Profile Applicability:

- Level 1

Description:

User Profiles with non-expiring passwords are never required to change their password.

Rationale:

Non-expiring passwords are security risks because if no automated solution is in place, users are never prompted to change their passwords. Non-expiring passwords present a security risk as they may either be shared (non-unique) accounts or their passwords may be easy to obtain through observation of login keystrokes over an indefinite period of time.

Impact:

Shared accounts may be impacted.

Audit:

• On a command line, type STRSQL and press Enter
• Enter the following SQL statement and press Enter.

```
SELECT ALL
USER_NAME, STATUS, PWDEXPITV, LASTUSED
FROM QSYS2/USER_INFO T01
WHERE PWDEXPITV = -1
AND NOPWD ='NO'
```

Service accounts may be excluded from the audit and remediation. A service account is a user account that is created explicitly to provide a security context for automated system and application services running on the system. Service accounts should be configured with a non-trivial, complex password that is used in an automated service process and never used interactively. Service accounts should be documented and their Password expiration interval may be set to *NOMAX. A process should then be documented and executed to periodically change their passwords manually.

Remediation:

To establish the recommended configuration, change all interactive user profile password expiration intervals to *SYSVAL and ensure that your system value for QPWDEXPITV is set to 90 days or less or a value commensurate with your policy:
CHGUSRPRF USRPRF(<*xxxxxx*>) PWDEXPITV(*SYSVAL)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

3.9 (L1) User Profiles With Command Line Access (Automated)

Profile Applicability:

- Level 1

Description:

User Profiles with command line access can run commands they are authorized to from a command line.

Rationale:

Application user profiles should be limited to menus and restricted from directly running system commands from a command line. Only administrators with Special Authorities limited to the Principle of Least Privilege may be allowed to run commands from a command line.

Impact:

Users will be prevented from running command from a command line.

Audit:

• On a command line, type STRSQL and press Enter
• Enter the following SQL statement and press Enter.
SELECT ALL
USER_NAME, STATUS, LMTCPB, SPCAUT
FROM QSYS2/USER_INFO T01
WHERE LMTCPB <> '*YES'
IBM supplied user profiles will appear in the report and should be excluded from the audit. A list of IBM supplied user profiles can be obtained from the references below.

Remediation:

To establish the recommended configuration, change all non-administrative application users to command line capability to *YES:
CHGUSRPRF USRPRF(<*xxxxxx*>) LMTCPB(*YES)

Additional Information:

Certain IBM supplied commands such as DSPJOB, DSPJOBLOG, DSPMSG, SIGNOFF, SNDMSG and WRKMSG allow limited users. Additionally, any command can be changed and many 3rd party commands if a command's ALWLMTUSR parameter = *YES. Many remote functions such as the IBM i remote command server, ODBC, etc. do not honor user profile limit capabilities (LMTCPB) and allow remote users to run commands remotely regardless of the ALWLMTUSR parameter. There are many ways to run a command without command line access - remote command, sql, ftp, ssh...

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.8 Collect Command-Line Audit Logs Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.		●	●
v7	8.8 Enable Command-line Audit Logging Enable command-line audit logging for command shells, such as Microsoft Powershell and Bash.		●	●

3.10 (L1) IBM Supplied User Profiles (Automated)

Profile Applicability:

- Level 1

Description:

This section contains information about the IBM-Supplied user profiles that are shipped with the system and Licensed Program Products. These profiles are used as object owners for various system functions. Some system functions also run under specific IBM-supplied user profiles.

Rationale:

You must change the password for the QSECOFR profile after you install your system. This password is the same for every IBM i system and poses a security exposure until it is changed. However, Do not change any other values for IBM-supplied user profiles. Changing these profiles can cause system functions to fail. Additionally, IBM Supplied Profiles should not be used as group profiles with few exceptions. It is better to create your own group profiles with the proper authorities and special authorities using the Principle of Least Privilege (PoLP) as defined by the NIST and regulatory compliance requirements.

All IBM-supplied user profiles except for QSECOFR are shipped with a password of *NONE and are not intended for sign-on. These profiles are used by the IBM i operating system. Therefore, signing on with these profiles or using the profiles to own user (non-IBM supplied) objects is not recommended.

Impact:

Functions using the authorities and parameters of any profile you change may fail. You may want to contact IBM or your business partner for guidance prior to making any changes.

Audit:

Changes to IBM Supplied Profiles

- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

```
SELECT AUTHORIZATION_NAME, NO_PASSWORD_INDICATOR, STATUS,

USER_CLASS_NAME, INITIAL_PROGRAM_NAME,
LIMIT_CAPABILITIES, SPECIAL_AUTHORITIES
FROM QSYS2/USER_INFO WHERE AUTHORIZATION_NAME LIKE 'Q%' AND
NO_PASSWORD_INDICATOR = 'NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND
STATUS = '*DISABLED' OR AUTHORIZATION_NAME LIKE 'Q%' AND
USER_CLASS_NAME <> '*USER' OR AUTHORIZATION_NAME LIKE 'Q%' AND
INITIAL_PROGRAM_NAME <> '*NONE' OR AUTHORIZATION_NAME LIKE 'Q%' AND
LIMIT_CAPABILITIES <> '*NO' OR AUTHORIZATION_NAME LIKE 'Q%' AND
SPECIAL_AUTHORITIES <> '*NONE'
```

- Review the results of the screen output. This indicates that one or more of the following parameters of the profiles in the list does not match the default values that are used for all IBM-supplied user profiles.
- NO_PASSWORD_INDICATOR (PASSWORD) = YES (Default)
- STATUS (STATUS) = *ENABLED (Default)
- USER_CLASS_NAME (USRCLS) = *USER (Default)
- INITIAL_PROGRAM_NAME (INLPGM) = *NONE (Default)
- LIMIT_CAPABILITIES (LMTCPB) = *NO (Default)
- SPECIAL_AUTHORITIES (SPCAUT) = *NONE (Default)
- Compare the results of the screen output to information about IBM-supplied profiles, their purpose, and values for any IBM-supplied profiles that are different from the defaults from the shipped defaults from the following link.

https://www.ibm.com/docs/en/i/7.5?topic=reference-supplied-user-profiles

IBM Supplied Group Profiles

- To check if IBM Supplied Profiles are being used as Group Profiles
- On a command line, type STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

SELECT T01.GROUPNAME, T01.USERNAME FROM QSYS2/GROUPLIST T01
INNER JOIN

QSYS2/USER_INFO T02 ON T01.GROUPNAME = T02.USER_NAME WHERE

T02.USER_NAME LIKE 'Q%'
AND T02.USER_NAME NOT IN ('QBRMS', 'QMQMADM', 'QONDADM',
'QRDARS400', 'QRDARSADM', 'QWQADMIN')

- Review the results of the screen output. The following are valid exclusions from the audit.
- QBRMS
- QMQMADM
- QONDADM
- QRDARS400
- QRDARSADM
- QWQADMIN

Remediation:

- Change any IBM-Supplied user profile found in the audit that are different from the defaults or values different from the list in the referenced table

https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
CHGUSRPRF USRPRF(<*xxxxxx*>) <*parameter*>(<*xxxxxx*>)

- Change any User Profile that is a group member of an IBM-Supplied user profile found in the audit to remove the IBM-Supplied user profile from its Group (GRPPRF) and/or Supplemental Group (SUPGRPPRF) paramaters.

CHGUSRPRF USRPRF(<*xxxxxx*>) GRPPRF(<*xxxxxx*>) SUPGRPPRF(<*xxxxxx*>)
Note: Many of the IBM supplied user profiles cannot be specified on CHGUSRPRF. If there are IBM supplied user profiles that don't match the documented default values, they can be reset using the Reset Profile Attributes (QSYRESPA) API.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=reference-supplied-user-profiles
2. https://www.ibm.com/docs/en/i/7.5?topic=profiles-default-values-user
3. https://www.ibm.com/docs/en/i/7.5?topic=sup-supplied-user-profiles
4. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/apis/qsyrespa.htm

Additional Information:

Note: The table includes only some, but not all user profiles for licensed program products; therefore, the list may not be inclusive of all IBM supplied profiles. Contact IBM or an IBM i Business Partner if you have questions or need guidance. Note however that you should also contact an IBM i Security Subject Matter Expert for guidance.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

3.11 (L1) Group Profiles With Passwords (Automated)

Profile Applicability:

- Level 1

Description:

Group profiles should not have a password as they are usually not associated with a unique account.

Rationale:

Unique accounts provide accountability to the actions they perform. Group members should all be unique, but allowing the group profile to which they belong to sign on with a password provides no unique accountability to the actions that shared profiles with a password present.

Audit:

• On a command line, type STRSQL and press Enter
• Copy or type the following SQL statement to the terminal and press Enter.
SELECT All

T01.GROUPNAME, T02.NOPWD

FROM QSYS2/GROUPLIST T01 INNER JOIN

QSYS2/USER_INFO T02

ON T01.GROUPNAME = T02.USER_NAME

WHERE T02.NOPWD = 'NO'
• Verify that the display returns no group profiles with a password (NOPWD = NO).

Remediation:

CHGUSRPRF USRPRF(<*xxxxxx*>) PASSWORD(*NONE)
Where USRPRF(<*xxxxxx*>) in the above example is the group profile/s from the above audit.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			

4 System Configuration

The recommendations that follow detail the IBM i configuration settings.

4.1 Security System Values

The following recommendations represent the comprehensive standard system settings for the i system.

4.1.1 Level 1

Corporate/Enterprise Environment (general use)

4.1.1.1 (L1) Allow Restoration of Security-Sensitive Objects (Automated)

Profile Applicability:

- Level 1

Description:

Determines if the system will allow authorized users to restore system-state objects or programs that adopt authority to the system.

System administrators must use this privileged access to restore objects frequently as a part of their routine IBM-supplied PTF O/S maintenance as well as related to back-up and recover processes for applications. The restore privileges will be limited to System administrator and security personnel based on special authorities.

Rationale:

Because some programs may cause serious problems, this system value provides a method to protect your system.

Impact:

It is important to set the QALWOBJRST value to *ALL before performing some system activities, such as:

- Installing a new release of the IBM® i licensed program
- Installing new licensed programs
- Recovering your system

These activities may fail if the QALWOBJRST value is not *ALL. To ensure system security, return the QALWOBJRST value to your normal setting after completing the system activity.

If you regularly restore programs and applications to your system and accept the risk, you might need to set the QALWOBJRST system value to *ALWPGMADP. Restoration of programs that adopt authority may pose a security risk to your system and must be evaluated carefully prior to restoring to your system.

Audit:

DSPSYSVAL SYSVAL(QALWOBJRST)

Remediation:

To establish the recommended configuration, set the following system value to *ALWPTF:
QALWOBJRST
CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('*ALWPTF')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-allow-restoring-security-sensitive-objects-qalwobjrst

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

4.1.1.2 (L1) Set Attention Program (Automated)

Profile Applicability:

- Level 1

Description:

Determines what program is executed when the user presses the attention-key. (Note:*ASSIST is interpreted by the system to use the QSYS/QEZMAIN program, which is displayed if you view the setting using the PRTSYSSECA command.)

Rationale:

You can specify the program to call when you press the Attention key.

Audit:

DSPSYSVAL SYSVAL(QATNPGM)

Remediation:

To establish the recommended configuration, set the following system value to *NONE:
QATNPGM
CHGSYSVAL SYSVAL(QATNPGM) VALUE('*NONE')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=overview-system-user-defaults-system-values-attention-program

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.3 (L1) Set Auditing Control (Automated)

Profile Applicability:

- Level 1

Description:

Serves as the on/off switch for security auditing. *AUDLVL activates event auditing at the system or user level. *OBJAUD activates object auditing. *NOQTEMP prevents extraneous auditing entries for objects in library QTEMP.

Rationale:

Auditing can be defined as an inspection or examination of a process or system to determine the quality of it, and is also used to ensure compliance to requirements.

Audit:

DSPSYSVAL SYSVAL(QAUDCTL)

Remediation:

To establish the recommended configuration, set the following system value to *NOQTEMP, *OBJAUD, *AUDLVL:
QAUDCTL
CHGSYSVAL SYSVAL(QAUDCTL) VALUE('*NOQTEMP *OBJAUD *AUDLVL')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-control-qaudctl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

4.1.1.4 (L1) Set Auditing End Action (Automated)

Profile Applicability:

- Level 1

Description:

Determines the action the system should take if it is unable to continue auditing (e.g. the audit record is full).

Rationale:

System continues to operate but sends a message to the system operator and to the QSYS/QSYSMSG if the message.

Audit:

DSPSYSVAL SYSVAL(QAUDENDACN)

Remediation:

To establish the recommended configuration, set the following system value to *NOTIFY:
QAUDENDACN
CHGSYSVAL SYSVAL(QAUDENDACN) VALUE('*NOTIFY')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-end-action-qaudendacn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

4.1.1.5 (L1) Set Auditing Force Level (Automated)

Profile Applicability:

- Level 1

Description:

Determines how many auditing journal entries records are cached in memory before they are physically written to disk from memory.

Rationale:

This will provide the best auditing performance and lets the system determine the appropriate setting based on performance history.

Audit:

DSPSYSVAL SYSVAL(QAUDFRCLVL)

Remediation:

To establish the recommended configuration, set the following system value to *SYS:
QAUDFRCLVL
CHGSYSVAL SYSVAL(QAUDFRCLVL) VALUE('*SYS')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-force-level-qaudfrclvl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

4.1.1.6 (L1) Set Auditing Level (Automated)

Profile Applicability:

- Level 1

Description:

Determines the level of auditing on the system. At a minimum the following settings must be set;

- *AUTFAIL – Authority failures.
- *CREATE – Objects are created
- *DELETE – Objects are deleted
- *OBJMGT – Object management tasks.
- *PGMFAIL - Program failures, i.e. a blocked instruction, validation value failure, domain violation
- *SAVRST – Save and restore operations,
- *SECURITY - Security events.
- *SERVICE – Use of service tools,
- *SYSMGT – System management tasks

Rationale:

This will make it easier to view the security audit journal as it determines which security-related events are logged.

Audit:

DSPSYSVAL SYSVAL(QAUDLVL)

Remediation:

To establish the recommended configuration, set the following system value to *AUTFAIL, *CREATE, *DELETE, *OBJMGT, *PGMFAIL, *SAVRST, *SECURITY, *SERVICE, *SYSMGT:
QAUDLVL
CHGSYSVAL SYSVAL(QAUDLVL) VALUE('*AUTFAIL *CREATE *DELETE *OBJMGT *PGMFAIL *SAVRST *SECURITY *SERVICE *SYSMGT')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-level-qaudlvl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.1.7 (L1) Set Security Auditing Level Extensions (Automated)

Profile Applicability:

- Level 1

Description:

Allows additional space to specify more than sixteen audit values.

You can specify more than one value for the QAUDLVL2 system value, unless you specify *NONE. For the QAUDLVL2 system value to take effect, the QAUDCTL system value must include *AUDLVL and the QAUDLVL system value must include *AUDLVL2.

Rationale:

The Auditing Level Extension (QAUDLVL2) system value is required when more than sixteen auditing values are needed.

Audit:

DSPSYSVAL SYSVAL(QAUDLVL2)

Remediation:

CHGSYSVAL SYSVAL(QAUDLVL2) VALUE(*NONE)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-level-extension-qaudlvl2

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.1.1.8 (L1) Set Automatic Device Configuration (Automated)

Profile Applicability:

- Level 1

Description:

Specifies whether locally attached devices are configured automatically.

Rationale:

Automatic configuration changes the device description to match the keyboard attached. You may not want to use automatic configuration if you are using manual configuration to set up a device with a different keyboard type than the hardware reports.

Impact:

Do NOT automatically configure locally attached devices except when configuring new local controllers or devices.

Audit:

DSPSYSVAL SYSVAL(QAUTOCFG)

Remediation:

To establish the recommended configuration, set the following system value to "0" (OFF):
QAUTOCFG
CHGSYSVAL SYSVAL(QAUTOCFG) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-automatic-device-configuration-qautocfg

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.9 (L1) Set Automatic Remote Controller Configuration (Automated)

Profile Applicability:

- Level 1

Description:

Determines whether automatic remote workstation controller configuration is enabled.

Rationale:

Impact:

Do NOT automatically configure remote workstation controllers.

Audit:

DSPSYSVAL SYSVAL(QAUTORMT)

Remediation:

To establish the recommended configuration, set the following system value to "0" (OFF):
QAUTORMT
CHGSYSVAL SYSVAL(QAUTORMT) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=overview-devices-system-values-remote-controllers-devices

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.10 (L1) Set Automatic Virtual Device Creation (Automated)

Profile Applicability:

- Level 1

Description:

Determines whether automatic device creation is allowed and if so, how many devices can be configured automatically. Specify a value 1 through 32500 for this system value and is both sufficient to support the needs of the business and not too large to represent a denial of service exposure since it represents a finite limit. Setting the value to *NOMAX is a security risk as an infinite number of virtual devices may lead to a denial of service if disk capacity is reached.

Rationale:

The value should be sufficient enough that enough devices are allocated to support the business.

Audit:

DSPSYSVAL SYSVAL(QAUTOVRT)

Remediation:

To establish the recommended configuration, set the following system value to 32500 or less to specify an adequate number of devices to support the business:
QAUTOVRT
CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(<*XXXXXX*>)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-automatic-configuration-virtual-devices-qautovrt

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.11 (L1) Set Create Authority (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the default public authority.

Rationale:

This lets the public view newly created objects, but not change them. This will ensure the integrity of the newly created objects. You can override the QCRTAUT system value at a library level to specify data classifications within specific application libraries.

Impact:

Several IBM-supplied libraries, including QSYS, have a CRTAUT value of *SYSVAL. If you change the QCRTAUT system value to something other than *CHANGE, you might encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than *CHANGE, make sure that all device descriptions and their associated message queues have a PUBLIC authority of *CHANGE. One way to accomplish this is to change the CRTAUT value for library QSYS to *CHANGE from *SYSVAL.

Audit:

DSPSYSVAL SYSVAL(QCRTAUT)

Remediation:

To establish the recommended configuration, set the following system value to *USE:
QCRTAUT
CHGSYSVAL SYSVAL(QCRTAUT) VALUE('*USE')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-authority-new-objects-qcrtaut

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

4.1.1.12 (L1) Set Disconnect-Job Interval (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the interval in minutes that a job can be disconnected before the system ends the job.

Rationale:

A disconnected job uses up system resources, as well as retaining any locks on objects and should be ended eventually to avoid this.

Audit:

DSPSYSVAL SYSVAL(QDSCJOBITV)

Remediation:

To establish the recommended configuration, set the following system value to "30" (Times out disconnected jobs after 30 minutes):
QDSCJOBITV
CHGSYSVAL SYSVAL(QDSCJOBITV) VALUE('30')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-disconnected-job-time-out-interval-qdscjobitv

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.13 (L1) Set Display User Sign-on Information (Automated)

Profile Applicability:

- Level 1

Description:

Specifies whether the sign-on information display appears when a user signs on. Promotes logon monitoring.

Rationale:

This is recommended so that users can monitor attempted use of their profiles.

Audit:

DSPSYSVAL SYSVAL(QDSPSGNINF)

Remediation:

To establish the recommended configuration, set the following system value to "1" (ON):
QDSPSGNINF
CHGSYSVAL SYSVAL(QDSPSGNINF) VALUE('1')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-display-sign-information-qdspsgninf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.1.1.14 (L1) Set Force Conversion On Restore (Automated)

Profile Applicability:

- Level 1

Description:

Determines under what conditions objects will be forced to convert when they are being restored to the system. When an object is translated it is recompiled using a trusted translator guaranteed not to circumvent the integrity of the system. (See also QALWOBJRST & QVFYOBJRST, 2.1.1.1 and 2.1.1.49)

Rationale:

This setting attempts to strike a balance between ensuring system integrity and incurring the overhead of recompiling programs that do not appear to have been altered.

Audit:

DSPSYSVAL SYSVAL(QFRCCVNRST)

Remediation:

To establish the recommended configuration, set the following system value to "3":
QFRCCVNRST
CHGSYSVAL SYSVAL(QFRCCVNRST) VALUE('3')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=generation-qfrccvnrst-system-value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			
v7	8 Malware Defenses Malware Defenses			

4.1.1.15 (L1) Set Inactivity Time-out Interval (Automated)

Profile Applicability:

- Level 1

Description:

Determines the interval in minutes that a workstation can be inactive before the system sends a message to a message queue or ends the job. All users must use a password protected screen saver that locks the PC after 15 minutes of inactivity to comply with Payment Card Industry Data Security Standards.

Rationale:

The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed on. An inactive workstation might allow an unauthorized person access to the system.

Audit:

DSPSYSVAL SYSVAL(QINACTITV)

Remediation:

To establish the recommended configuration, set the following system value to "30" (The system times out inactive jobs after 30 minutes of inactivity):
QINACTITV
CHGSYSVAL SYSVAL(QINACTITV) VALUE('30')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-inactive-job-time-out-interval-qinactitv

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4.1.1.16 (L1) Set Inactivity Message Queue (Automated)

Profile Applicability:

- Level 1

Description:

Specifies either the action to be taken when the inactivity time-out interval is reached or the name of the message queue that will receive messages about the workstation. The current system standard ends the job after the inactivity time-out interval is reached.

Rationale:

Controlling inactive jobs provides security so that users do not leave signed on displays inactive.

Audit:

DSPSYSVAL SYSVAL(QINACTMSGQ)

Remediation:

To establish the recommended configuration, set the following system value to *DSCJOB:
QINACTMSGQ
CHGSYSVAL SYSVAL(QINACTMSGQ) VALUE('*DSCJOB')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-inactive-job-time-out-message-queue-qinactmsgq

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4.1.1.17 (L1) Set Limit Device Sessions (Automated)

Profile Applicability:

- Level 1

Description:

Specifies if users can have concurrent device sessions.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QLMTDEVSSN)

Remediation:

To establish the recommended configuration, set the following system value to any value between 1 and 9:
QLMTDEVSSN
CHGSYSVAL SYSVAL(QLMTDEVSSN) VALUE(<*x*>)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-limit-device-sessions-qlmtdevssn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.18 (L1) Set Limit Security Officer Access to Workstations (Automated)

Profile Applicability:

- Level 1

Description:

Limits users with *ALLOBJ or *SERVICE special authority to authorized devices.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QLMTSECOFR)

Remediation:

To establish the recommended configuration, set the following system value to "0":
QLMTSECOFR
CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-limit-security-officer-qlmtsecofr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

4.1.1.19 (L1) Set Maximum Sign-on Action (Automated)

Profile Applicability:

- Level 1

Description:

Determines the action the system takes when a user reaches the maximum number of sign-on attempts.

Disables the user profile when the maximum sign-on limit is reached.

Rationale:

This disables the user profile when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same or different devices. This helps to prevent access to unauthorized users.

Audit:

DSPSYSVAL SYSVAL(QMAXSGNACN)

Remediation:

To establish the recommended configuration, set the following system value to "2":
QMAXSGNACN
CHGSYSVAL SYSVAL(QMAXSGNACN) VALUE('2')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-action-when-sign-attempts-reached-qmaxsgnacn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.20 (L1) Set Maximum Sign-on Attempts (Automated)

Profile Applicability:

- Level 1

Description:

Determines the maximum number of invalid sign-on attempts a user is allowed.

Rationale:

This setting helps to prevent unauthorized access into user profiles by giving the user a limited number of login attempts before disabling the user profile

Audit:

DSPSYSVAL SYSVAL(QMAXSIGN)

Remediation:

To establish the recommended configuration, set the following system value to "5":
QMAXSIGN
CHGSYSVAL SYSVAL(QMAXSIGN) VALUE('5')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-maximum-sign-attempts-qmaxsign

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.21 (L1) Set Block Password Change (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the time period during which a password is blocked from being changed following the prior successful password change operation. This system value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

DSPSYSVAL SYSVAL(QPWDCHGBLK)

Remediation:

To establish the recommended configuration, set the following system value to "24":
QPWDCHGBLK
CHGSYSVAL SYSVAL(QPWDCHGBLK) VALUE('24')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-block-password-change-qpwdchgblk

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.22 (L1) Set Password Expiration Interval (Automated)

Profile Applicability:

- Level 1

Description:

Determines the maximum number of days a password is valid from 1 to 366 or *NOMAX. Note that special application profiles that must logon should have PWDEXPITV set to *NOMAX on the user profile whereas standard user profiles should be set to *SYSVAL.

Rationale:

This helps to prevent access to unauthorized persons by forcing a password change after a set amount of days.

Audit:

DSPSYSVAL SYSVAL(QPWDEXPITV)

Remediation:

To establish the recommended configuration, set the following system value to "90":
QPWDEXPITV
CHGSYSVAL SYSVAL(QPWDEXPITV) VALUE('90')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-expiration-interval-qpwdexpitv

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.23 (L1) Set Password Expiration Warning (Automated)

Profile Applicability:

- Level 1

Description:

Controls the number of days prior to a password expiring to begin displaying password expiration warning messages on the Sign-on Information display.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QPWDEXPWRN)

Remediation:

To establish the recommended configuration, set the following system value to "7":
QPWDEXPWRN
CHGSYSVAL SYSVAL(QPWDEXPWRN) VALUE('7')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-expiration-warning-qpwdexpwrn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.1.1.24 (L1) Set Password Level (Automated)

Profile Applicability:

- Level 1

Description:

Determines the length of password that is supported as well as weak and deprecated NTLM passwords for Windows 95/98/ME clients will be removed from the system. User passwords with a length of 1-10 characters are supported and excludes the use of decryptable password hashes (NTLM) for older 16 bit clients.

Note that NTLM or Lan Manager authentication uses a method of hashing a user's password into 14 (7+7) characters and the hash is calculated into the two halves separately making it easily decryptable. NTLM was replaced by NTLMv2 in the late 1990s and has since been deprecated.

Rationale:

This provides additional security by having options to only support passwords that meets specified length and security requirements.

Audit:

DSPSYSVAL SYSVAL(QPWDLVL)

Remediation:

To establish the recommended configuration, set the following system value to "1":
QPWDLVL
CHGSYSVAL SYSVAL(QPWDLVL) VALUE(1)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-level-qpwdlvl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.1.1.25 (L1) Set Required Difference in Passwords (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. To maintain the effectiveness of this policy setting, use the Block Password Change (QPWDCHGBLK) setting to prevent users from repeatedly changing their password.

The recommended state for this setting is: 24 or more password(s).

Rationale:

TThe longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

Audit:

DSPSYSVAL SYSVAL(QPWDRQDDIF). Ensure that QPWDRQDDIF is set to a value of 2=Cannot be the same as last 24.

Remediation:

To establish the recommended configuration, set the following system value to "2":
QPWDRQDDIF
CHGSYSVAL SYSVAL(QPWDRQDDIF) VALUE('2')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-required-difference-in-qpwdrqddif

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.26 (L1) Set Password Rules (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the rules used to check whether a password is formed correctly.

Rationale:

This provides additional security by having a system in place to verify if a password meets the specified rules set.

Audit:

DSPSYSVAL SYSVAL(QPWDRULES)

Remediation:

• CALL QCMD
• CHGSYSVAL SYSVAL(QPWDRULES) VALUE('*ALLCRTCHG *DGTLMTAJC *DGTLMTFST *DGTLMTLST *DGTMIN1 *LMTPRFNAME *MAXLEN10 *MINLEN8 *REQANY3 *SPCCHRLMTAJC *SPCCHRLMTFST *SPCCHRLMTLST')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-rules-qpwdrules

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.1.27 (L1) Retain Server Security (Automated)

Profile Applicability:

- Level 1

Description:

The Retain Server Security Data (QRETSVRSEC) system value is no longer used. The QRETSVRSEC system value no longer needs to be set to '1' to retain the security data needed by a server for authentication. This includes the Server Authentication Entry interfaces and the Validation List (*VLDL) interfaces.

Rationale:

Audit:

Remediation:

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-retain-server-security-qretsvrsec

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.28 (L1) Set Remote IPL (Automated)

Profile Applicability:

- Level 1

Description:

Determines if an operator is allowed to IPL the machine remotely.

Rationale:

Disabling this provides additional security by not allowing power-on and restart to be done remotely.

Audit:

DSPSYSVAL SYSVAL(QRMTIPL)

Remediation:

To establish the recommended configuration, set the following system value to "0":
QRMTIPL
CHGSYSVAL SYSVAL(QRMTIPL) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-remote-power-restart-qrmtipl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.29 (L1) Set Remote Sign-on Value (Automated)

Profile Applicability:

- Level 1

Description:

Determine whether and how automatic sign-on from a remote system is allowed.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QRMTSIGN)

Remediation:

To establish the recommended configuration, set the following system value to *VERIFY:
QRMTSIGN
CHGSYSVAL SYSVAL(QRMTSIGN) VALUE('*VERIFY')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-remote-sign-control-qrmtsign

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.1.1.30 (L1) Set Remote Service Attribute (Automated)

Profile Applicability:

- Level 1

Description:

Determines if the remote system service ability is enabled.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QRMTSRVATR)

Remediation:

To establish the recommended configuration, set the following system value to "0":
QRMTSRVATR
CHGSYSVAL SYSVAL(QRMTSRVATR) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-remote-service-attribute-qrmtsrvatr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.31 (L1) Scan File System (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the integrated file system in which objects will be scanned when exit programs are registered with any of the integrated file system scan-related exit points.

Rationale:

This provides an additional layer of security because this option can be used to scan for a virus.

Audit:

DSPSYSVAL SYSVAL(QSCANFS)

Remediation:

To establish the recommended configuration, set the following system value to *ROOTOPNUD:
QSCANFS
CHGSYSVAL SYSVAL(QSCANFS) VALUE('*ROOTOPNUD')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-scan-file-systems-qscanfs

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8 Malware Defenses Malware Defenses			

4.1.1.32 (L1) Set Scan File System Control (Automated)

Profile Applicability:

- Level 1

Description:

Controls the integrated file system scanning on the system when exit programs are registered with any of the integrated file system scan-related exit points.

Rationale:

This ensures that any failure from the scan exit programs prevent the associated operations, as well as not give the exit program additional access levels

Audit:

DSPSYSVAL SYSVAL(QSCANFSCTL)

Remediation:

To establish the recommended configuration, set the following system value to *ERRFAIL and *NOWRTUPG:
QSCANFSCTL
CHGSYSVAL SYSVAL(QSCANFSCTL) VALUE('*ERRFAIL *NOWRTUPG')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-scan-file-systems-control-qscanfsctl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	8 Malware Defenses Malware Defenses			

4.1.1.33 (L1) Set System Security Level (Automated)

Profile Applicability:

- Level 1

Description:

Determines the level of security features supported. Level 40 is the recommend level of security for non-DoD production systems. In addition to password authentication and privileged access controls, level 40 can effectively safeguard data, programs, and other production objects and prevent unintentional data loss or modification. Level 50 can add considerable overhead depending on how the application is written and would need to be tested for performance impact before being implemented.

Rationale:

Security level 40 prevents potential integrity or security risks from programs that can circumvent security in special cases.

Audit:

DSPSYSVAL SYSVAL(QSECURITY)

Remediation:

To establish the recommended configuration, set the following system value to "40":
QSECURITY
CHGSYSVAL SYSVAL(QSECURITY) VALUE('40')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=reference-using-system-security-qsecurity-system-value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.34 (L1) Set Shared Memory Control (Automated)

Profile Applicability:

- Level 1

Description:

Controls whether or not users are allowed to use shared memory APIs or mapped memory objects that have write capability to modify shared memory. While enabling this system value introduces the possibility of an integrity issue if not used correctly, the probability is low given our systems other security controls. Specifically, restricting the ability to create, restore, or use shared memory APIs.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QSHRMEMCTL)

Remediation:

To establish the recommended configuration, set the following value to "1":
QSHRMEMCTL
CHGSYSVAL SYSVAL(QSHRMEMCTL) VALUE('1')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-share-memory-control-qshrmemctl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.1.35 (L1) Secure Sockets Layer Cipher Specification List (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the list of cipher suites that are supported by System. The values are read-only unless the QSSLCSLCTL (cipher control) system value is set to *USRDFN.

Rationale:

Configuring your IBM i server to allow the use of weak protocols and weak cipher suites will result in your IBM i server potentially being at risk of a network security breach. Adding an older cipher suite to the default list results in opening up all applications that use the default list to known security vulnerabilities.

Audit:

DSPSYSVAL QSSLCSL

Remediation:

Specify the following cipher suites that are supported by System:
• CALL QCMD
• CHGSYSVAL SYSVAL(QSSLCSL) VALUE('*AES_128_GCM_SHA256
*AES_256_GCM_SHA384 *CHACHA20_POLY1305_SHA256
*ECDHE_ECDSA_AES_128_GCM_SHA256
*ECDHE_ECDSA_AES_256_GCM_SHA384 *ECDHE_RSA_AES_128_GCM_SHA256
*ECDHE_RSA_AES_256_GCM_SHA384
*ECDHE_ECDSA_CHACHA20_POLY1305_SHA256
*ECDHE_RSA_CHACHA20_POLY1305_SHA256')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=srsv-transport-layer-security-tls-cipher-specification-list-qsslcsl
2. https://www.ibm.com/support/pages/configuring-your-ibm-i-system-secure-sockets-layer-ssltransport-layer-security-tls-protocols-and-cipher-suites

Additional Information:

Setting System Value QSSLCSLCTL to *OPSYS will automatically maintain the Remediation Procedure in System Value QSSLCSL. Therefore if System Value QSSLCSLCTL is set to *OPSYS, there is no need to remediate this section. It is highly recommended that QSSLCSLCTL be set to *OPSYS to maintain the QSSLCSL values as read-only.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.1.1.36 (L1) Secure Sockets Layer Cipher Control (Automated)

Profile Applicability:

- Level 1

Description:

Specifies whether or not the QSSLCSL (cipher specification list) system value is controlled by the system or by the user.

Rationale:

Configuring your IBM i server to allow the use of weak protocols and weak cipher suites will result in your IBM i server potentially being at risk of a network security breach. Adding an older cipher suite to the default list results in opening up all applications that use the default list to known security vulnerabilities.

Audit:

DSPSYSVAL SYSVAL(QSSLCSLCTL)

Remediation:

To establish the recommended configuration, set the following system value to *OPSYS:
QSSLCSLCTL
CHGSYSVAL SYSVAL(QSSLCSLCTL) VALUE('*OPSYS')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-transport-layer-security-tls-cipher-control-qsslcslctl
2. https://www.ibm.com/support/pages/configuring-your-ibm-i-system-secure-sockets-layer-ssltransport-layer-security-tls-protocols-and-cipher-suites

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.1.1.37 (L1) Secure Socket Layer Security protocols (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the SSL protocol versions supported by System SSL.

Rationale:

Configuring your IBM i server to allow the use of weak protocols and weak cipher suites will result in your IBM i server potentially being at risk of a network security breach. Adding an older cipher suite to the default list results in opening up all applications that use the default list to known security vulnerabilities.

Audit:

DSPSYSVAL SYSVAL(QSSLPCL)

Remediation:

To establish the recommended configuration, set the following system value to *OPSYS:
QSSLPCL
CHGSYSVAL QSSLPCL VALUE('*OPSYS')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-transport-layer-security-tls-protocols-qsslpcl
2. https://www.ibm.com/support/pages/configuring-your-ibm-i-system-secure-sockets-layer-ssltransport-layer-security-tls-protocols-and-cipher-suites

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.1.1.38 (L1) System Library List (Automated)

Profile Applicability:

- Level 1

Description:

The system library list (QSYSLIBL) system value is used as the first part of the library list associated with a job.

The libraries in the system part of the library list of a job are searched before any other libraries in the library list of a job. The list can contain as many as 15 names. You cannot delete or rename a library specified as part of the system library list, because libraries in this library list are locked.

You can change the system library list (QSYSLIBL). If you change QSYSLIBL, the change takes place immediately for new jobs entering the system. The change does not affect running jobs, unless the application in the job accesses the system library list directly.

Rationale:

The security of the System Library List is a vital part of your overall system security. All libraries in the System Library List should provide *PUBLIC *USE authority. Any authority greater than *USE to any library in the System Library List can allow the introduction of trojans and malicious code into your system that will be searched before any other libraries in the library list of a job.

Audit:

DSPSYSVAL SYSVAL(QSYSLIBL)

- Make note of all Libraries in the System part of the library list
- DSPOBJAUT OBJ(<*xxxxxx*>) OBJTYPE(*LIB) For each library in the list
- Ensure that each library in the list grants *PUBLIC *USE Object Authority and that any additional Users with an authority greater than *USE are properly authorized by the business to introduce changes into the library.

Remediation:

To establish the recommended configuration, set the *PUBLIC authority to *USE to all libraries in the System part of the library list QSYSLIBL that grant an authority greater than *USE:
GRTOBJAUT OBJ(<*xxxxxx*>) OBJTYPE(*LIB) USER(*PUBLIC) AUT(*USE) REPLACE(*YES)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-system-library-list-qsyslibl-system-value
2. https://www.ibm.com/docs/en/i/7.5?topic=lists-jobs-library-list

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

4.1.1.39 (L1) Set Use Adopted Authority (Automated)

Profile Applicability:

- Level 1

Description:

Controls those users allowed to create or change programs that use adopted authority from other programs that call it. If an authorization list is specified, *PUBLIC(EXCLUDE) should be used. Specific access granted for those users that are allowed to create or change programs that adopt authority should be limited to system administrator personnel and change control personnel responsible for disaster recovery and program change control respectively.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QUSEADPAUT)

Remediation:

To establish the recommended configuration, enter a name for the authorization list for the following system value:
QUSEADPAUT
• CRTAUTL AUTL(QUSEADPAUT) AUT(*EXCLUDE)
• CHGOBJOWN OBJ(QUSEADPAUT) OBJTYPE(*AUTL) NEWOWN(QSYS)
• CHGSYSVAL SYSVAL(QUSEADPAUT) VALUE(QUSEADPAUT)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=commands-use-adopted-authority-quseadpaut

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

4.1.1.40 (L1) Verify Object On Restore (Automated)

Profile Applicability:

- Level 1

Description:

Determines when signatures will be verified and if the object will be restored without a valid signature. (See also QALWOBJRST & QFRCCVNRST, 2.1.1.1 and 2.1.1.16) Use this value for normal operations, when you expect some of the objects you restore to be unsigned, but you want to ensure that all signed objects have signatures that are valid. Commands and programs you have created or purchased before digital signatures were available will be unsigned. This value allows those commands and programs to be restored. This is the default value.

Rationale:

You can prevent anyone from restoring an object, unless that object has a correct digital signature from a trusted software provider.

Impact:

When your system is shipped, the QVFYOBJRST system value is set to 3. If you change the value of QVFYOBJRST, it is important to set the QVFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

Audit:

DSPSYSVAL SYSVAL(QVFYOBJRST)

Remediation:

To establish the recommended configuration, set the following system value to "3":
QVFYOBJRST
CHGSYSVAL SYSVAL(QVFYOBJRST) VALUE('3')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=objects-qvfyobjrst-system-value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

4.1.2 Level 2

High Security/Sensitive Data Environment (limited functionality)

4.1.2.1 (L2) Allow Restoration of Security-Sensitive Objects (Automated)

Profile Applicability:

- Level 2

Description:

Does not allow objects with security-sensitive attributes to be restored.

Rationale:

Because some programs may cause serious problems, this system value provides a method to protect your system.

Impact:

It is important to set the QALWOBJRST value to *ALL before performing some system activities, such as:

- Installing a new release of the IBM® i licensed program
- Installing new licensed programs
- Recovering your system

These activities may fail if the QALWOBJRST value is not *ALL. To ensure system security, return the QALWOBJRST value to your normal setting after completing the system activity.

Audit:

DSPSYSVAL SYSVAL(QALWOBJRST)

Remediation:

To establish the recommended configuration, set the following system value to *NONE:
QALWOBJRST
CHGSYSVAL SYSVAL(QALWOBJRST) VALUE('*NONE')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-allow-restoring-security-sensitive-objects-qalwobjrst

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

4.1.2.2 (L2) Allow User Domain Objects in These Libraries (Automated)

Profile Applicability:

- Level 2

Description:

This specifies the names of the libraries that can contain the *USRSPC (user space), *USRIDX (user index), and *USRQ (user queue) type objects. In our environment many vendor applications are making use of USRxx objects in numerous and changing libraries. This increases the complexity of restricting this system value to specific libraries without creating a threat to legitimate operations.

In addition, the value of *ALL is generally acceptable for any system that does not need to comply with DoD C2 level security specifications. In addition, the probability of damaging events is low if object authority and application behavior is controlled appropriately. This is the shipped value.

Rationale:

Some systems have application software that relies on object types *USRSPC, *USRIDX, or *USRQ. For those systems, the list of libraries for the QALWUSRDMN system value should include the libraries that are used by the application software.

Impact:

Systems with high security requirements require the restriction of user *USRSPC, *USRIDX, *USRQ objects. The system cannot audit the movement of information to and from user domain objects. The restriction does not apply to user domain objects of type program (*PGM), server program (*SRVPGM), and SQL packages (*SQLPKG).

Audit:

DSPSYSVAL SYSVAL(QALWUSRDMN)

Remediation:

To establish the recommended configuration, set the following system value to QTEMP:
QALWUSRDMN
CHGSYSVAL SYSVAL(QALWUSRDMN) VALUE('QTEMP')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-allow-user-domain-objects-qalwusrdmn

Additional Information:

If your system has a high security requirement, you should allow user domain objects only in the QTEMP library

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

4.1.2.3 (L2) Set Auditing Control (Automated)

Profile Applicability:

- Level 2

Description:

Serves as the on/off switch for security auditing. *AUDLVL activates event auditing at the system or user level. *OBJAUD activates object auditing. *NOQTEMP prevents extraneous auditing entries for objects in library QTEMP.

Rationale:

Auditing can be defined as an inspection or examination of a process or system to determine the quality of it, and is also used to ensure compliance to requirements.

Activates event and object auditing including QTEMP

Audit:

DSPSYSVAL SYSVAL(QAUDCTL)

Remediation:

To establish the recommended configuration, set the following system value to *OBJAUD, *AUDLVL :
QAUDCTL
CHGSYSVAL SYSVAL(QAUDCTL) VALUE('*OBJAUD *AUDLVL')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-control-qaudctl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

4.1.2.4 (L2) Set Auditing End Action (Automated)

Profile Applicability:

- Level 2

Description:

Determines the action the system should take if it is unable to continue auditing (e.g. the audit record is full).

Rationale:

If the system is unable to write audit journal entries and the QAUDENDACN system value is *PWRDWNSYS, your system ends abnormally. This might cause a lengthy initial program load (IPL) when your system is powered on again.

Audit:

DSPSYSVAL SYSVAL(QAUDENDACN)

Remediation:

To establish the recommended configuration, set the following system value to *PWRDWNSYS:
QAUDENDACN
CHGSYSVAL SYSVAL(QAUDENDACN) VALUE('*PWRDWNSYS')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-end-action-qaudendacn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

4.1.2.5 (L2) Set Auditing Force Level (Automated)

Profile Applicability:

- Level 2

Description:

Determines how many auditing journal entries records are cached in memory before they are physically written to disk from memory.

Rationale:

This will provide the best auditing performance.

Impact:

if your installation requires that no audit entries be lost when your system ends abnormally, you must specify 1. Specifying 1 might impair performance.

Audit:

DSPSYSVAL SYSVAL(QAUDFRCLVL)

Remediation:

To establish the recommended configuration, set the following system value to "1":
QAUDFRCLVL
CHGSYSVAL SYSVAL(QAUDFRCLVL) VALUE(1)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-force-level-qaudfrclvl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

4.1.2.6 (L2) Set Automatic Virtual Device Creation (Automated)

Profile Applicability:

- Level 2

Description:

Determines whether automatic device creation is allowed and if so, how many devices can be configured automatically. 32500 is the maximum numerical value that can be set for this system value and is both sufficient to support the needs of the business and not too large to represent a denial of service exposure since it represents a finite limit.

Rationale:

Prevents new virtual devices from being created.

Impact:

Users are able to break into your system more easily using pass-through or telnet if you allow the system to automatically configure virtual devices. A user that is attempting to break in has a limited number of attempts at each virtual device without automatic configuration.

Audit:

DSPSYSVAL SYSVAL(QAUTOVRT)

Remediation:

To establish the recommended configuration, set the following system value to "0":
QAUTOVRT
CHGSYSVAL SYSVAL(QAUTOVRT) VALUE(0)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-automatic-configuration-virtual-devices-qautovrt

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.7 (L2) Set Create Authority (Automated)

Profile Applicability:

- Level 2

Description:

Specifies the default public authority.

Sets *EXCLUDE as the default public authority for new objects created in libraries that do not have a CRTAUT value specified.

Rationale:

This excludes the public from newly created objects. This will ensure the integrity of the newly created objects. You can override the QCRTAUT system value at a library level to specify data classifications within specific application libraries.

Impact:

Several IBM-supplied libraries, including QSYS, have a CRTAUT value of *SYSVAL. If you change the QCRTAUT system value to something other than *CHANGE, you might encounter problems with signing on at new or automatically created devices. To avoid these problems when you change QCRTAUT to something other than *CHANGE, make sure that all device descriptions and their associated message queues have a PUBLIC authority of *CHANGE. One way to accomplish this is to change the CRTAUT value for library QSYS to *CHANGE from *SYSVAL.

Audit:

DSPSYSVAL SYSVAL(QCRTAUT)

Remediation:

To establish the recommended configuration, set the following system value to *EXCLUDE:
QCRTAUT
CHGSYSVAL SYSVAL(QCRTAUT) VALUE('*EXCLUDE')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-authority-new-objects-qcrtaut

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

4.1.2.8 (L2) Set Create Object Audit Level (Automated)

Profile Applicability:

- Level 2

Description:

Determines the default object auditing level for new objects.

An audit record is written for any security relevant action that affects the read or change of all newly created objects.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QCRTOBJAUD)

Remediation:

To establish the recommended configuration, set the following system value to *ALL:
QCRTOBJAUD
CHGSYSVAL SYSVAL(QCRTOBJAUD) VALUE('*ALL')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=auditing-new-objects-qcrtobjaud

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.14 Log Sensitive Data Access Log sensitive data access, including modification and disposal.			●
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	14.9 Enforce Detail Logging for Access or Changes to Sensitive Data Enforce detailed audit logging for access to sensitive data or changes to sensitive data (utilizing tools such as File Integrity Monitoring or Security Information and Event Monitoring).			●

4.1.2.9 (L2) Set Disconnect-Job Interval (Automated)

Profile Applicability:

- Level 2

Description:

Specifies the interval in minutes that a job can be disconnected before the system ends the job.

Rationale:

A disconnected job uses up system resources, as well as retaining any locks on objects and should be ended eventually to avoid this.

Audit:

DSPSYSVAL SYSVAL(QDSCJOBITV)

Remediation:

To establish the recommended configuration, set the following system value to "15" (Times out disconnected jobs after 15 minutes):
QDSCJOBITV
CHGSYSVAL SYSVAL(QDSCJOBITV) VALUE('15')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-disconnected-job-time-out-interval-qdscjobitv

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.10 (L2) Set Force Conversion On Restore (Automated)

Profile Applicability:

- Level 2

Description:

Determines under what conditions objects will be forced to convert when they are being restored to the system. When an object is translated it is recompiled using a trusted translator guaranteed not to circumvent the integrity of the system. (See also QALWOBJRST & QVFYOBJRST, 2.1.2.1 and 2.1.2.31)

All objects will be converted.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QFRCCVNRST)

Remediation:

To establish the recommended configuration, set the following system value to "7":
QFRCCVNRST
CHGSYSVAL SYSVAL(QFRCCVNRST) VALUE('7')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=generation-qfrccvnrst-system-value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			
v7	8 Malware Defenses Malware Defenses			

4.1.2.11 (L2) Set Inactivity Time-out Interval (Automated)

Profile Applicability:

- Level 2

Description:

Determines the interval in minutes that a workstation can be inactive before the system sends a message to a message queue or ends the job. All users must use a password protected screen saver that locks the PC after 15 minutes of inactivity to comply with Payment Card Industry Data Security Standards.

Rationale:

The QINACTITV and QINACTMSGQ system values provide security by preventing users from leaving inactive workstations signed on. An inactive workstation might allow an unauthorized person access to the system.

Audit:

DSPSYSVAL SYSVAL(QINACTITV)

Remediation:

To establish the recommended configuration, set the following system value to "15" (The system times out inactive jobs after 15 minutes of inactivity):
QINACTITV
CHGSYSVAL SYSVAL(QINACTITV) VALUE('15')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-inactive-job-time-out-interval-qinactitv

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4.1.2.12 (L2) Set Inactivity Message Queue (Automated)

Profile Applicability:

- Level 2

Description:

Specifies either the action to be taken when the inactivity time-out interval is reached or the name of the message queue that will receive messages about the workstation. The current system standard ends the job after the inactivity time-out interval is reached.

Rationale:

Controlling inactive jobs provides security so that users do not leave signed on displays inactive.

Audit:

DSPSYSVAL SYSVAL(QINACTMSGQ)

Remediation:

To establish the recommended configuration, set the following system value to *ENDJOB:
QINACTMSGQ
CHGSYSVAL SYSVAL(QINACTMSGQ) VALUE('*ENDJOB')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-inactive-job-time-out-message-queue-qinactmsgq

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4.1.2.13 (L2) Set Limit Device Sessions (Automated)

Profile Applicability:

- Level 2

Description:

Specifies if users can have concurrent device sessions.

Rationale:

This is recommended because limiting users to a single device reduces the likelihood of sharing passwords and leaving devices unattended.

Audit:

DSPSYSVAL SYSVAL(QLMTDEVSSN)

Remediation:

To establish the recommended configuration, set the following system value to '1':
QLMTDEVSSN
CHGSYSVAL SYSVAL(QLMTDEVSSN) VALUE('1')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-limit-device-sessions-qlmtdevssn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.14 (L2) Set Limit Security Officer Access to Workstations (Automated)

Profile Applicability:

- Level 2

Description:

Limits users with *ALLOBJ or *SERVICE special authority to authorized devices.

Rationale:

This system value controls whether users with *ALLOBJ or *SERVICE special authorities need explicit authority to specific work stations.

Impact:

If the value of QLMTSECOFR is set to a value of 1, a user with *ALLOBJ or *SERVICE special authority can sign on at a workstation only if that user is specifically authorized (that is, given *CHANGE authority) to the workstation or if user profile QSECOFR is authorized (given *CHANGE authority) to the workstation. This authority cannot come from public authority.

Audit:

DSPSYSVAL SYSVAL(QLMTSECOFR)

Remediation:

To establish the recommended configuration, set the following system value to "1":
QLMTSECOFR
CHGSYSVAL SYSVAL(QLMTSECOFR) VALUE('1')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-limit-security-officer-qlmtsecofr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work Establish and maintain dedicated computing resources, either physically or logically separated, for all administrative tasks or tasks requiring administrative access. The computing resources should be segmented from the enterprise's primary network and not be allowed internet access.			●
v7	4.6 Use of Dedicated Machines For All Administrative Tasks Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.			●

4.1.2.15 (L2) Set Maximum Sign-on Action (Automated)

Profile Applicability:

- Level 2

Description:

Determines the action the system takes when a user reaches the maximum number of sign-on attempts.

Disables the user profile and device when the maximum sign-on limit is reached.

Rationale:

This disables both the user profile and device when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same or different devices. This helps to prevent access to unauthorized users and devices.

Audit:

DSPSYSVAL SYSVAL(QMAXSGNACN)

Remediation:

To establish the recommended configuration, set the following system value to "3":
QMAXSGNACN
CHGSYSVAL SYSVAL(QMAXSGNACN) VALUE('3')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-action-when-sign-attempts-reached-qmaxsgnacn

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

4.1.2.16 (L2) Set Maximum Sign-on Attempts (Automated)

Profile Applicability:

- Level 2

Description:

Determines the maximum number of invalid sign-on attempts a user is allowed.

Rationale:

This setting helps to prevent unauthorized access into user profiles by giving the user a limited number of login attempts before disabling the user profile

Audit:

DSPSYSVAL SYSVAL(QMAXSIGN)

Remediation:

To establish the recommended configuration, set the following system value to "3":
QMAXSIGN
CHGSYSVAL SYSVAL(QMAXSIGN) VALUE('3')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-maximum-sign-attempts-qmaxsign

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.2.17 (L2) Set Block Password Change (Automated)

Profile Applicability:

- Level 2

Description:

Specifies the time period during which a password is blocked from being changed following the prior successful password change operation. This system value does not restrict password changes made by the Change User Profile (CHGUSRPRF) command.

Rationale:

By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Audit:

DSPSYSVAL SYSVAL(QPWDCHGBLK)

Remediation:

To establish the recommended configuration, set the following system value to "99":
QPWDCHGBLK
CHGSYSVAL SYSVAL(QPWDCHGBLK) VALUE('99')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-block-password-change-qpwdchgblk

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.2.18 (L2) Set Password Level (Automated)

Profile Applicability:

- Level 2

Description:

Determines the length of password that is supported as well as weak and deprecated NTLM passwords for Windows 95/98/ME clients will be removed from the system. User passwords with a length of 1-128 characters are supported and excludes the use of decryptable password hashes (NTLM) for older 16 bit clients.

For systems running at QPWDLVL 4, the OS uses a Password-based Key Derivation Function 2 (PBKDF2) with HMAC SHA512 (SHA-2 512 bit) encryption for the scheme.

Note that NTLM or Lan Manager authentication uses a method of hashing a user's password into 14 (7+7) characters and the hash is calculated into the two halves separately making it easily decryptable. NTLM was replaced by NTLMv2 in the late 1990s and has since been deprecated.

Rationale:

This provides additional security by having options to only support passwords that meets specified length and security requirements.

Impact:

All encrypted passwords that are used at QPWDLVL 0, 1, 2, and 3 are removed from the system when QPWDLVL is changed to 4.

Changing from QPWDLVL 4 back to QPWDLVL 0 or 1 requires a change to QPWDLVL 2 before going to 0 or 1. QPWDLVL 2 allows for the creation of the one-way encrypted password that can be used at QPWDLVL 0 or 1 as long as the length and syntax requirements for the password meet the QPWDLVL 0 or 1 rules.

Audit:

DSPSYSVAL SYSVAL(QPWDLVL)

Remediation:

To establish the recommended configuration, set the following system value to "4":
QPWDLVL
CHGSYSVAL SYSVAL(QPWDLVL) VALUE(4)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-level-qpwdlvl

Additional Information:

Avoid changing password system values, such as QPWDMINLEN, QPWDMAXLEN, and QPWDRULES, until after you have tested QPWDLVL 2, 3 or 4. This makes it easier to transition back to QPWDLVL 1 or 0 if necessary. The QPWDVLDPGM system value must specify either *REGFAC or *NONE before the system allows QPWDLVL to be changed to 2, 3 or 4. Therefore, if you use a password validation program, you might want to write a new one that can be registered for the QIBM_QSY_VLD_PASSWRD exit point, format VLDP0100, by using the ADDEXITPGM command.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.1.2.19 (L2) Set Required Difference in Passwords (Automated)

Profile Applicability:

- Level 2

Description:

Specifies a code that determines how many of the most recent prior passwords are not allowed.

Rationale:

This value provides additional security by preventing users from specifying passwords that were used previously. It also prevents a user whose password has expired from changing it and then immediately changing it back to the old password.

Audit:

DSPSYSVAL SYSVAL(QPWDRQDDIF)

Remediation:

To establish the recommended configuration, set the following system value to "1":
QPWDRQDDIF
CHGSYSVAL SYSVAL(QPWDRQDDIF) VALUE('1')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-required-difference-in-qpwdrqddif

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.2.20 (L2) Set Password Rules (Automated)

Profile Applicability:

- Level 2

Description:

Specifies the rules used to check whether a password is formed correctly.

Rationale:

This provides additional security by having a system in place to verify if a password meets the specified rules set.

Audit:

DSPSYSVAL SYSVAL(QPWDRULES)

Remediation:

• CALL QCMD
• CHGSYSVAL SYSVAL(QPWDRULES) VALUE('*ALLCRTCHG *DGTLMTAJC *DGTLMTFST *DGTLMTLST *DGTMIN1 *LMTPRFNAME *MAXLEN128 *MINLEN14 *REQANY3 *SPCCHRLMTAJC *SPCCHRLMTFST *SPCCHRLMTLST')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-rules-qpwdrules

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.2.21 (L2) Set Password Validation Program (Automated)

Profile Applicability:

- Level 2

Description:

This provides the ability for a user-written program to do additional validation on passwords.

Rationale:

This provides additional security by using the programs to do additional checking of user-assigned passwords before they are accepted by the system.

Audit:

DSPSYSVAL SYSVAL(QPWDVLDPGM)

Remediation:

To establish the recommended configuration, create a password validation program and set the following system value to *REGFAC:
QPWDVLDPGM
CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(*REGFAC)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-approval-program-qpwdvldpgm

Additional Information:

Note: When the current or pending value of the password level (QPWDLVL) system value is 2 or 3, a program name cannot be specified for the Password Approval Program system value QPWDVLDPGM. Therefore, at QPWDLVL = 3, system value QPWDVLDPGM should be set to a value of *REGFAC or *NONE.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.1.2.22 (L2) Set Remote Sign-on Value (Automated)

Profile Applicability:

- Level 2

Description:

Determine whether and how automatic sign-on from a remote system is allowed.

Rationale:

Audit:

DSPSYSVAL SYSVAL(QRMTSIGN)

Remediation:

To establish the recommended configuration, set the following system value to *FRCSIGNON:
QRMTSIGN
CHGSYSVAL SYSVAL(QRMTSIGN) VALUE('*FRCSIGNON')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-remote-sign-control-qrmtsign

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.1.2.23 (L2) Set System Security Level (Automated)

Profile Applicability:

- Level 2

Description:

Determines the level of security features supported. Level 40 is the recommend level of security for non-DoD production systems. In addition to password authentication and privileged access controls, level 40 can effectively safeguard data, programs, and other production objects and prevent unintentional data loss or modification. Level 50 can add considerable overhead depending on how the application is written and would need to be tested for performance impact before being implemented.

Rationale:

Security level 50 provides enhanced integrity protection, in addition to what is provided by security level 40, for installations with strict security requirements.

Audit:

DSPSYSVAL SYSVAL(QSECURITY)

Remediation:

To establish the recommended configuration, set the following system value to "50":
QSECURITY
CHGSYSVAL SYSVAL(QSECURITY) VALUE('50')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=reference-using-system-security-qsecurity-system-value

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.24 (L2) Set Shared Memory Control (Automated)

Profile Applicability:

- Level 2

Description:

The Share Memory Control (QSHRMEMCTL) system value defines which users are allowed to use shared memory or mapped memory that has write capability.

Rationale:

Your environment may contain applications, each running different jobs, but sharing pointers within these applications. Using these APIs provides for better application performance and streamlines the application development by allowing shared memory and stream files among these different applications and jobs. However, use of these APIs might potentially pose a risk to your system and assets. A programmer can have write access and can add, change, and delete entries in the shared memory or stream file.

Audit:

DSPSYSVAL SYSVAL(QSHRMEMCTL)

Remediation:

To establish the recommended configuration, set the following value to "0":
QSHRMEMCTL
CHGSYSVAL SYSVAL(QSHRMEMCTL) VALUE('0')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-share-memory-control-qshrmemctl

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.1.2.25 (L2) Verify Object On Restore (Automated)

Profile Applicability:

- Level 2

Description:

Determines when signatures will be verified and if the object will be restored without a valid signature. (See also QALWOBJRST & QFRCCVNRST, 2.1.2.1 and 2.1.2.10)

Rationale:

You can prevent anyone from restoring an object, unless that object has a correct digital signature from a trusted software provider.

Impact:

When your system is shipped, the QVFYOBJRST system value is set to 3. If you change the value of QVFYOBJRST, it is important to set the QVFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

Audit:

DSPSYSVAL SYSVAL(QVFYOBJRST)

Remediation:

To establish the recommended configuration, set the following system value to "5":
QVFYOBJRST
CHGSYSVAL SYSVAL(QVFYOBJRST) VALUE('5')

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-verify-object-restore-qvfyobjrst

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

4.2 Network Services

Access to the *IOSYSCFG special authority must be limited to only those individuals responsible for changing how the system is configured. Users with *IOSYSCFG special authority can add or remove communications configuration information, work with TCP/IP servers, and configure the internet connection server (ICS). Most commands for configuring communications require *IOSYSCFG special authority. Access to the *ALLOBJ and *SECADM special authority must be limited to those who need access. Access to both of these privileges is required to change the following network security attributes using the CHGNETA command. All changes must be documented and approved.

Giving special authorities to users represents a security exposure. For each user, carefully evaluate the need for any special authorities. Keep track of which users have special authorities and periodically review their requirement for the authority.

4.2.1 (L1) Network Attribute JOBACN (Network Job Action) (Automated)

Profile Applicability:

- Level 1

Description:

The JOBACN network attribute determines how the system processes incoming requests to run jobs.

The values for JOBACN are:

- *FILE: The input stream is filed in the queue of network files for the recipient. An authorized user may then view, delete, receive, or submit the job stream.
- *SEARCH: The table of network job entries is searched to determine the action to take for the input job stream.
- *REJECT: The input job stream is rejected by the system. This allows the target to secure itself from input streams received through the network.

The JOBACN value should be set to *REJECT to secure your system from job streams received through the network.

Rationale:

Incoming job streams from remote systems do not authenticate remote credentials (passwords) and thus present an unauthenticated access vulnerability. A value of *FILE files the remote job on a local users queue of network files where they may or may not choose to submit the job without viewing the contents of the job stream. A value of *SEARCH searches the table of network job entries to determine the action to take which may file, reject or automatically submit the job where the target system's network job entries will specify a user profile under which the job will run. For example, distribution directory update jobs could run under a user with administration rights. System operations, such as shutdown or network activation/deactivation, could run under a powerful system profile.

Setting the value of the JOBACN to any value other than *REJECT makes the local system's security dependent on remote systems where security may be less certain making the local system vulnerable to an unauthenticated network attack.

Unauthenticated access of a system can be carried out by malicious attackers to gain access to sensitive information anonymously with no accountability for actions performed that may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

Changing Network Attribute JOBACN to *REJECT may disable SNA network job streams from entering your system without proper credentialed authentication.

Audit:

•DSPNETA
•Page Down and verify that the value for Job action is set to *REJECT.

Remediation:

To establish the recommended configuration, change the Network Attribute JOBACN to *REJECT:
CHGNETA JOBACN(*REJECT)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=attributes-job-action-jobacn-network-attribute

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.2.2 (L1) DDM Remote Configuration List (SNA) Attributes (Automated)

Profile Applicability:

- Level 1

Description:

The Secure Location (SECURELOC) defines how security information is handled for program start requests received from remote system. Setting SECURELOC to a value of *NO specifies that the local system is not a secure system.

All DDM Remote Configuration List entries shall specify *VFYENCPWD for the Secure Location (SECURELOC) parameter. *VFYENCPWD requires the same user ID and password on each source and target system.

Rationale:

Setting the SECURELOC value of any Remote Location to a value of *NO for DDM/DRDA conversations presents an unauthenticated access vulnerability. Unauthenticated access of a system can be carried out by malicious attackers to gain access to sensitive information anonymously with no accountability for actions performed that may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

Shared (non-unique) accounts in an APPN network may be impacted.

Audit:

• DSPCFGL CFGL(QAPPNRMT)
-Note that if you receive the message “Configuration list QAPPNRMT not found”, this indicates that your
system does is not configured for DDM over SNA and this setting is irrelevant.
• Ensure that all Secure Loc parameters = *VFYENCPWD.

Remediation:

To establish the recommended configuration, change all Remote Location Secure Loc parameters to *VFYENCPWD.
WRKCFGL CFGL(QAPPNRMT)
Select 2 to change the QAPPNRMT Configuration List
Change all Secure Loc parameters to *VFYENCPWD

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=network-drda-server-security-in-appc

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

4.2.3 (L1) DDM TCP/IP Attributes (Automated)

Profile Applicability:

- Level 1

Description:

The default setting for the DDM server has a default security of *USRIDPWD which allows clear-text password. Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources. A setting lower than *USRIDPWD including values of *YES, *VLDONLY or *USRID does not require a password on a DDM Connection request allowing un-authenticated access to system resources possibly with elevated privileges.

Rationale:

Not requiring a password for DDM/DRDA conversations presents an unauthenticated access vulnerability. Unauthenticated access of a system can be carried out by malicious attackers to gain access to sensitive information anonymously with no accountability for actions performed that may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

DDM/DRDA communications not using encrypted passwords may be impacted.

Audit:

Type CHGDDMTCPA and press F4.
The screen will display the DDM TCP/IP Attributes. Ensure that the Lowest authentication method equals *USRENCPWD and the Lowest encryption algorithm is equal to *AES.

Remediation:

CHGDDMTCPA AUTOSTART(*YES) PWDRQD(*USRENCPWD) ENCALG(*AES)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=security-elements-in-tcpip-network

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

4.2.4 (L2) DDM TCP/IP Attributes (Automated)

Profile Applicability:

- Level 2

Description:

The default setting for the DDM server has a default security of *USRIDPWD which allows clear-text password. Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources. A setting lower than *USRIDPWD including values of *YES, *VLDONLY or *USRID does not require a password on a DDM Connection request allowing un-authenticated access to system resources possibly with elevated privileges.

Rationale:

Not requiring a password for DDM/DRDA conversations presents an unauthenticated access vulnerability. Unauthenticated access of a system can be carried out by malicious attackers to gain access to sensitive information anonymously with no accountability for actions performed that may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Impact:

DDM/DRDA communications not using encrypted passwords may be impacted.

Audit:

Type CHGDDMTCPA and press F4.
The screen will display the DDM TCP/IP Attributes. Ensure that the Lowest authentication method equals *ENCUSRPWD and the Lowest encryption algorithm is equal to *AES.

Remediation:

CHGDDMTCPA AUTOSTART(*YES) PWDRQD(*ENCUSRPWD) ENCALG(*AES)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=security-elements-in-tcpip-network

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

4.2.5 (L1) NFS Shares (Automated)

Profile Applicability:

- Level 1

Description:

The Network File System (NFS) provides the user with access to data and objects that are stored on a remote NFS server.

In addition, any file system mounted locally through the Network File System will have the features, characteristics, limitations, and dependencies of the directory or file system it was mounted from on the remote server. Operations on mounted file systems are not performed locally. Requests flow through the connection to the server and must obey the requirements and restrictions of the type of file system on the server.

Rationale:

NFS anonymous shares present an unauthenticated access vulnerability. Unauthenticated access of a system can be carried out by malicious attackers to gain access to sensitive information anonymously with no accountability for actions performed that may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability the entire system and/or critical components with serious consequences.

Audit:

- CALL QCMD
- Press F10 to include detailed messages
- CALL QZNFRTVE
- Place your cursor on each of the exports and press F1 to display the export
- Ensure that on the detailed message that "ANON=4294967295(*NONE)" is displayed
- Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Remediation:

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=security-network-file-system-nfs
2. https://www.tenable.com/plugins/nessus/11356

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.2.6 (L2) NFS Shares (Automated)

Profile Applicability:

- Level 2

Description:

Disable NFS completely of force NFSv4 with Kerberos.

NFS in general with AUTH_SYS security is not considered a secure protocol. If NFS is used in a L2 environment, NFSv4 should be the only protocol version allowed and RPCSEC_GSS authentication with Kerberos should be required.

Rationale:

With the RPCSEC_GSS Kerberos mechanism, the server no longer depends on the client to correctly represent which user is accessing the file, as is the case with AUTH_SYS. Instead, it uses cryptography to authenticate users to the server, preventing a malicious client from impersonating a user without having that user's kerberos credentials.

Audit:

- CALL QCMD
- Press F10 to include detailed messages
- CALL QZNFRTVE
- Place your cursor on each of the exports and press F1 to display the export
- Ensure that on the detailed message that VERS=4, SEC=KRB5 is displayed
- NFSv4 should be the only protocol version allowed and RPCSEC_GSS authentication with Kerberos should be required.

Remediation:

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=security-network-file-system-nfs
2. https://www.ibm.com/docs/en/i/7.5?topic=nfs-setting-up-network-rpcsec-gss
3. https://www.tenable.com/plugins/nessus/11356

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.2.7 (L1) Exit Points (Automated)

Profile Applicability:

- Level 1

Description:

The IBM i provides several host servers and related objects that are common for the IBM® i Access family. For each Host server, IBM provides one or more exit points to control the activity of the host server.

The registration facility (WRKREGINF) shows information about IBM® i exit points and their associated exit programs.

Exit points provide an additional layer of network defense but are not a replacement for object and resource security covered in Chapter 5 of the IBM I Security Reference and IBM I online documentation.

Some shipped services such as SSH, SFTP and others, user defined and 3rd party ports and services do not have protocol specific host server exit points. Network security for these ports and services can be controlled with Socket Server Exit Points and/or IP Packet Filtering.

Additional information:

- Only IBM i registered host server functions (WRKREGINF) have protocol specific exit point formats
- Not all IBM developed and 3rd party applications call configured user exit programs
- Socket exits may provide connection specific conditions for a job at runtime only if API sockets are available
- Socket exits cannot provide connection control for any application that does not use sockets APIs for network communications
- Socket exits cannot provide connection control for system tasks that do not call user exit programs
- Socket exits may provide limited control of Network specific IP and port and protocol properties but lack the advanced user functionality of the IBM i Access family host server exits.

Rationale:

Lack of registered exit point security may leave your system open to remote network attacks through ODBC, remote command, FTP etc. Exit points are an added layer of monitoring and security but are not a replacement for IBM i resource and access controls.

Audit:

- On a command line type WRKREGINF
- Place an 8 next to each of the following registered exit points at a minimum and ensure that user written programs are registered to the correct exit point format to provide additional validity and monitoring.
- Note that some exit points have multiple formats. Ensure that your programs are registered to the correct exit point format for your environment.
- QIBM_QDB_CLOSE
- QIBM_QDB_OPEN
- QIBM_QHQ_DTAQ
- QIBM_QMF_MESSAGE
- QIBM_QPWFS_FILE_SERV
- QIBM_QP0L_SCAN_CLOSE
- QIBM_QP0L_SCAN_OPEN
- QIBM_QRQ_SQL
- QIBM_QTF_TRANSFER
- QIBM_QTG_DEVINIT
- QIBM_QTG_DEVTERM
- QIBM_QTMF_CLIENT_REQ
- QIBM_QTMF_SERVER_REQ
- QIBM_QTMF_SVR_LOGON
- QIBM_QTMX_SERVER_REQ
- QIBM_QTMX_SVR_LOGON
- QIBM_QTMX_SVR_SELECT
- QIBM_QTOD_SERVER_REQ
- QIBM_QZDA_INIT
- QIBM_QZDA_NDB1
- QIBM_QZDA_ROI1
- QIBM_QZDA_SQL1
- QIBM_QZDA_SQL2
- QIBM_QZHQ_DATA_QUEUE
- QIBM_QZRC_RMT
- QIBM_QZSO_SIGNONSRV

Note that some exit points may have multiple exit point formats. Ensure that programs are registered to the exit point format specific to your environment. Information on specific exit point formats can be viewed online.

Remediation:

Write or purchase user exit programs and register to associated exit points using the WRKREGINF and ADDEXITPGM commands.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=security-securing-your-workstations
2. https://www.ibm.com/docs/en/i/7.5?topic=security-using-exit-programs
3. https://www.ibm.com/docs/en/i/7.5?topic=programs-exit-program-parameter-formats
4. https://www.ibm.com/docs/en/i/7.5?topic=concepts-sockets-related-user-exit-points
5. https://www.ibm.com/docs/en/i/7.5?topic=handling-ip-packet-filtering

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.2.8 (L1) Telnet Protocol (Automated)

Profile Applicability:

- Level 1

Description:

Restrict Telnet to SSL only to prevent sniffing of clear text passwords.

Rationale:

Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources.

Impact:

Unencrypted telnet may be impacted.

Audit:

Type command CHGTELNA and press F4.
Ensure that the Allow Secure Socket Layer is set to *ONLY.

Remediation:

To establish the recommended configuration, change telnet to use SSL only:
CHGTELNA ALWSSL(*ONLY)

References:

1. https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_75/rzamv/rzamvtcpsockets.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

4.2.9 (L1) FTP Protocol (Automated)

Profile Applicability:

- Level 1

Description:

Restrict FTP to SSL only to prevent sniffing of clear text passwords.

Rationale:

Allowing the use of clear-text passwords permits credentials to be intercepted over the network by sniffers, packet monitoring and communication trace tools which could easily lead to unauthorized access to system resources.

Impact:

Unencrypted ftp may be impacted.

Audit:

Type command CHGFTPA and press F4.
Ensure that the Allow Secure Socket Layer is set to *ONLY.

Remediation:

To establish the recommended configuration, change FTP to use SSL only:
CHGFTPA ALWSSL(*ONLY)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=ssl-configuration-details

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

4.3 IBM i Netserver security

"IBM i Support for Windows Network Neighborhood (IBM i NetServer) is an IBM i function that enables Server Message Block (SMB) clients to access IBM i shared directory paths and shared output queues.

Server and share access can be further restricted to specific users with access to specified AUTLs. Refer to https://www.ibm.com/support/pages/node/6579379 for information for Remediation instructions

By using IBM i NetServer securely, you can ensure that only authorized users can access IBM i NetServer resources, configuration, or shared data.

This section contains settings for configuring IBM i NetServer security settings using the IBM i Go Nets Menu. The IBM i Go Nets Menu is not enabled by default. Instructions for enabling the IBM i Go Nets Menu is available from IBM at this link.

4.3.1 (L1) IBM i NetServer Guest Profile (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether a Guest account is configured. The Guest account allows unauthenticated network users to gain access to the system.

The recommended state for this setting is: *NONE.

Rationale:

The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

Impact:

Setting the IBM i NetServer Guest profile to a value of *NONE may impact users access NetServer resources with a shared Guest profile. Additionally, changing the IBM i NetServer Guest profile requires you to end IBM i NetServer access (ENDNSV) and restart IBM i NetServer access (STRNSV RESET(*YES) which may impact active sessions.

Audit:

- Type ADDLIBLE NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Guest profile *NONE is displayed
- Ensure that *SAME is displayed for the Guest profile Pending value to ensure no changes are pending.

Remediation:

To establish the recommended configuration, do the following:

- Type ADDLIBLE NETSRVCMD
- Type CHGNSVA GUESTPRF(*NONE)
- Type ENDNSV
- Type STRNSV RESET(*YES)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

4.3.2 (L1) IBM i NetServer LANMAN Password Hash (Automated)

Profile Applicability:

- Level 1

Description:

The underlying system LANMAN hash was removed in 7.5. The NetServer LANMAN setting is obsolete and no longer used regardless of the setting.

Rationale:

Audit:

Remediation:

References:

1. https://en.wikipedia.org/wiki/LAN_Manager

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.3.3 (L1) IBM i SMB Signing (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines whether packet signing is required by the SMB client component.

Rationale:

Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data.

SMB is the resource sharing protocol that is supported by many operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

Impact:

The network client will not communicate with a network server unless that server agrees to perform SMB packet signing.

Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks.

Audit:

- Type ADDLIBLE NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Message authentication *REQUIRED is displayed
- Ensure that *SAME is displayed for the Message authentication Pending value to ensure no changes are pending.

Remediation:

To establish the recommended configuration, do the following:

- Type ADDLIBLE NETSRVCMD
- Type CHGNSVA MSGAUT(*REQUIRED)
- Type ENDNSV
- Type STRNSV RESET(*YES)

References:

1. https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/overview-server-message-block-signing

Additional Information:

When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide.

The recommended state for this setting is: Enabled.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.3.4 (L1) IBM i SMBv2 Server (Automated)

Profile Applicability:

- Level 1

Description:

This setting configures the server-side processing of the Server Message Block version 2 (SMBv2) protocol.

Rationale:

Since September 2016, vendors have strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30 year old design that is much more vulnerable to attacks then much newer designs such as SMBv2 and SMBv3.

Impact:

Some legacy OSes (e.g. Windows XP, Server 2003 or older), applications and appliances may no longer be able to communicate with the system once SMBv1 is disabled. We recommend careful testing be performed to determine the impact prior to configuring this as a widespread control, and where possible, remediate any incompatibilities found with the vendor of the incompatible system. Microsoft is also maintaining a thorough (although not comprehensive) list of known SMBv1 incompatibilities at this link: SMB1 Product Clearinghouse | Storage at Microsoft

Audit:

You can control which version(s) of SMB the NetServer will support by calling the NetServer maintenance utility to set the SMB flags and then restart the NetServer.

A good starting point is to see what those flags are presently set to.
In order to view the SMB flags do the following:

- CALL QZLSMAINT PARM('40' '0')
- Type WRKSPLF and locate your spool file with the name QPCSMPRT. Verify that the data in the flags is as follows which indicates that the server supports only SMBv2 and SMBv3:
  OLD FLAGS
  0000000000000100
  NEW FLAGS
  0000000000000100

To recap, the SMB version support and the corresponding flag values for IBM i 7.4:
SMB1 only: 080
SMB1, SMB2 & SMB3: 000
SMB2 & SMB3 only: 100
SMB2 only: 1000
Setting the flags to any other value may have unpredictable results

Remediation:

To allow SMB2 and SMB3 only, set the flags to a value of 100.

- CALL QZLSMAINT PARM('40' '3')
- CALL QZLSMAINT PARM('40' '1' '0X100')

References:

1. https://docs.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.3.5 (L1) IBM i NetServer Shares (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting defines the network file shares available to authenticated users.

Rationale:

Allowing an IBM i NetServer File Shares allows authenticated users to access Server Message Block (SMB) file shares on the system.

Allowing users access to IBM i NetServer File shares grants authenticated users access to Integrated File System (IFS) directories. Use this link to learn more about the IFS. A file share to the root (‘/’) of the IBM i file system is never recommended to be configured as this would effectively give an attacker access to the root and all directories including qsys.lib (the operating system).

Additionally, pay careful attention to your existing share permissions. It is highly recommended to limit shares to Read only to prevent alteration of contents and protect from increasingly harmful crypto/ramsomware attacks which detect network shares and may indiscriminately encrypt ubiquitous file systems of all types including qsys.lib. Use Read/Write permissions with diligence according to business requirements.

Impact:

Removing the root (/) file share will limit users to specific shares configured and prevent access to the root (/).

Audit:

- Type ADDLIBLE NETSRVCMD
- Type GO NETS
- Select Option 11. Work with Shares
- Place a 5 by each Share Name and observe the path of each share to ensure it is allowed by the business.
- Pay careful attention to ensure that no share allows access to the root (path /)

Remediation:

To establish the recommended configuration, do the following:

- Type ADDLIBLE NETSRVCMD
- Type GO NETS
- Select option 4 to remove the root (/) file share if detected

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

4.3.6 (L2) NetServer Browse Interval (Automated)

Profile Applicability:

- Level 2

Description:

Browse Announcements specify whether the server should announce its presence to the network.

Rationale:

For an added measure of security, you can hide IBM i NetServer from the Windows My Network Places.

Audit:

- Type ADDLIBLE NETSRVCMD
- Type GO NETS
- Select option 10. Display Attributes
- Ensure that Browse interval is 0 is displayed
- Ensure that 0 is displayed for the Browse interval Pending value to ensure no changes are pending.

Remediation:

To establish the recommended configuration, do the following:

- Type ADDLIBLE NETSRVCMD
- Type CHGNSVA BROWSEITV(*NONE)
- Type ENDNSV
- Type STRNSV RESET(*YES)

References:

1. https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_75/rzahl/rzahlhidenetserver.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.4 IBM i SSH Server security

The use of SSH provides a secure and encrypted mechanism for connecting to an IBM i server.

This section of the benchmark will focus on the installation and configuration of SSH. Some of the parameters specified in this section are actually the default values, but explicit declaration is preferred, to ensure that these recommendations remain constant over time.

Note: The SSH product directory is different between IBM i V7R2 and previous versions. After upgrading to V7R2, it is recommended that you migrate all settings to the V7R2 directory /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc and remove the older SSH product directories.

Remove the older product directories to prevent insecure settings from these directories from being used:

V5R4 - /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.5p1/etc

V6R1 – /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-3.8.1p1/etc/

V7R1 – /QOpenSys/QIBM/UserData/SC1/OpenSSH/openssh-4.7p1/etc/

4.4.1 (L1) Configuring SSH – server protocol 2 (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and allow the SSH2 protocol only. This is the SSH server configuration file.

Rationale:

There are publicly known vulnerabilities in SSH1 protocol, because of which the SSH1 protocol was deprecated in early 2001. SSH2 is a complete re-write of SSH1 with additional security features. All SSH connections should communicate over the SSH2 protocol. There are numerous benefits of utilizing SSH2 over SSH1, these include: an enhanced and stronger crypto integrity check and support for RSA and DSA keys, rather than just RSA key support in SSH1. The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and allow the SSH2 protocol only.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type Protocol and press F16 (shift F4)
Control: Protocol_____
• The display should yield the following output:
Protocol 2

Remediation:

EDTF ‘/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config’ file and explicitly define the SSH2 protocol:
• Replace:
#Protocol 2,1
• With:
Protocol 2
Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.4.2 (L1) Configuring SSH – banner configuration (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file and configure a path to a login herald message.

Rationale:

The login herald configured previously is not displayed during the initiation of a new SSH connection. Prior to a password being entered the user should accept the terms and conditions of the corporate acceptable usage policy.

Audit:

DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
On the Control field, type Banner and press F16 (shift F4)
Control: Banner_____
The display should yield the following output:
Banner /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh_banner

Remediation:

• Create an SSH banner file:
• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh_banner'
• Enter appropriate text and save the file.
• NOTE: The content of the banner file can reflect any internal acceptable usage policy standards
• EDTF ‘/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config’ file and customize the Banner parameter
• Replace:
#Banner /some/path
• With:
Banner /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/ssh_banner
• Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.4.3 (L1) Configuring SSH – disallow host based authentication (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file to ensure that host-based authentication is disallowed.

Rationale:

Using host-based authentication, any user on a trusted host can log into another host on which this feature is enabled. Since this feature depends only on system authentication and not on user authentication, it must be disabled.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type HostbasedAuthentication and press F16 (shift F4)
• Control: HostbasedAuthentication_____
• The display should yield the following output:
HostbasedAuthentication no

Remediation:

•EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' file to ensure that host based authentication is disallowed:
•Replace:
#HostbasedAuthentication no
•With:
HostbasedAuthentication no
•Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.4.4 (L1) Configuring SSH – set privilege separation (Automated)

Profile Applicability:

- Level 1

Description:

The recommendation is to edit the /QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config file to ensure that privilege separation is enabled. Note, that as of OpenSSH 7.5 this configuration directive has been deprecated.

Rationale:

Setting privilege separation helps to secure remote ssh access. Once a user is authenticated the sshd daemon creates a child process which has the privileges of the authenticated user and this then handles incoming network traffic. The aim of this is to prevent privilege escalation through the initial root process.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type UsePrivilegeSeparation and press F16 (shift F4)
• Control: UsePrivilegeSeparation _____
The display should yield the following output:
UsePrivilegeSeparation yes

Remediation:

• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' file to ensure that privilege separation is enabled:
• Replace:
UsePrivilegeSeparation no
• With:
UsePrivilegeSeparation yes
• Re-cycle the sshd daemon to pick up the configuration changes:
Note: In IBM i OpenSSH 6.9p1, UsePrivilegeSeparation is explicitly set to "no". Once upgrading to 8.0p1, UsePrivilegeSeparation is deprecated. There is a warning message generated when the sshd server is started when the option exists in sshd_config. To disable the warning, you can comment out or remove the line containing UsePrivilegeSeparation from the sshd_config file.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.4.5 (L1) Configuring SSH – set MaxAuthTries to 4 or Less (Automated)

Profile Applicability:

- Level 1

Description:

The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure.

Rationale:

Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, it is set the number based on site policy.

Audit:

• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type MaxAuthTries and press F16 (shift F4)
• Control: MaxAuthTries_____
• The display should yield the following output:
MaxAuthTries 4

Remediation:

• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config' file:
• Replace:
#MaxAuthTries 4
• With:
MaxAuthTries 4
• Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.4.6 (L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Automated)

Profile Applicability:

- Level 1

Description:

The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time.

Rationale:

Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type ClientAliveCountMax and press F16 (shift F4)
• Control: ClientAliveCountMax_____
• Verify the ClientAliveInterval is between 1 and 300 and ClientAliveCountMax is 0:
ClientAliveCountMax 0
ClientAliveInterval 300

Remediation:

• EDTF ‘/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config’ file:
• Replace:
#ClientAliveCountMax 0
#ClientAliveInterval 300
• With:
ClientAliveCountMax 0
ClientAliveInterval 300
• Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 Configure Automatic Session Locking on Enterprise Assets Configure automatic session locking on enterprise assets after a defined period of inactivity. For general purpose operating systems, the period must not exceed 15 minutes. For mobile end-user devices, the period must not exceed 2 minutes.	●	●	●
v7	16.11 Lock Workstation Sessions After Inactivity Automatically lock workstation sessions after a standard period of inactivity.	●	●	●

4.4.7 (L1) Configuring SSH – restrict Cipher list (Automated)

Profile Applicability:

- Level 1

Description:

This variable limits the types of ciphers that SSH can use during communication.

Rationale:

Based on research conducted at various institutions, it was determined that the symmetric portion of the SSH Transport Protocol (as described in RFC 4253) has security weaknesses that allowed recovery of up to 32 bits of plaintext from a block of ciphertext that was encrypted with the Cipher Block Chaining (CBD) method. From that research, new Counter mode algorithms (as described in RFC4344) were designed that are not vulnerable to these types of attacks and these algorithms are now recommended for standard use.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type Ciphers and press F16 (shift F4)
• Control: Ciphers_____
• The display should yield the following output:
Ciphers aes256-ctr,aes192-ctr,aes128-ctr

Remediation:

• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd'_config file:
• Insert:
Ciphers aes256-ctr,aes192-ctr,aes128-ctr
• Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.4.8 (L1) Configuring SSH – Limit Access Via SSH (Automated)

Profile Applicability:

- Level 1

Description:

There are several options available to limit which users and group can access the system via SSH. It is recommended that at least of the following options be leveraged:

AllowUsers

The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host.

AllowGroups

The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

DenyUsers

The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of comma separated user names. Numeric userIDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host.

DenyGroups

The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of comma separated group names. Numeric groupIDs are not recognized with this variable.

Rationale:

Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Audit:

• DSPF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd_config'
• On the Control field, type Allow and press F16 (shift F4)
• Control: Allow_____
• The display should yield the following output:
AllowUsers <*userlist*>
AllowGroups <*grouplist*>
DenyUsers <*userlist*>
DenyGroups <*grouplist*>

Remediation:

• EDTF '/QOpenSys/QIBM/UserData/SC1/OpenSSH/etc/sshd'_config file:
• Set one of the following:
AllowUsers <*userlist*>
AllowGroups <*grouplist*>
DenyUsers <*userlist*>
DenyGroups <*grouplist*>
• Re-cycle the sshd daemon to pick up the configuration changes:

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			
v7	16 Account Monitoring and Control Account Monitoring and Control			

4.5 IBM i Patch Management

Patch management is important in order to ensure that operating systems and applications are running the most recent security updates provided by IBM and software vendors.

4.5.1 (L1) IBM i Patch Management (Automated)

Profile Applicability:

- Level 1

Description:

This settings describes the IBM i patch management process.

Rationale:

Important IBM i updates are obtained through PTF (Program Temporary Fix) levels. Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible.

Impact:

None, this is the required process.

Audit:

• On a command line, type STRSQL and press Enter
• Enter the following SQL statement and press Enter.
SELECT ALL
GRP_CRNCY, GRP_ID, GRP_LVL, GRP_IBMLVL,
GRP_LSTUPD, GRP_RLS, GRP_SYSSTS, GRP_TITLE
FROM SYSTOOLS/GRPPTFCUR T01
WHERE GRP_ID IN ('SF99738', 'SF99665', 'SF99662', 'SF99739')
• The following 4 PTF Groups should show that the INSTALLED LEVEL IS CURRENT.
SF99958 750 Group Security
SF99995 750 Java
SF99952 750 IBM HTTP Server for i
SF99959 750 Group Hiper

Remediation:

Download and apply the current PTF group levels.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=services-group-ptf-currency-view

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

4.6 System Service Tools

Service tools provide various functions that you can perform through dedicated service tools (DST) or system service tools (SST), including diagnosing system problems, managing disk units, and managing system security. With the service tools server, you can also use your PC to perform service functions through TCP/IP.

To access these service tools functions through DST, SST, IBM Navigator for i (for disk unit management), and Operations Console, service tools user IDs are required. To change or reset the passwords for the service tools user IDs, you must comply with certain password policies.

Auditors will need a System Service Tool ID with security officer privileges to audit System Service Tools. Although profiles such as QSECOFR exist in System Service Tools, they are for the most part not linked to the Operating System equivalent of QSECOFR and will most likely not have the same password.

4.6.1 (L1) System Service Tools Password Expiration Interval (Automated)

Profile Applicability:

- Level 1

Description:

This setting describes changing the System Service Tools Password Expiration Interval from the default setting, 180 days.

Rationale:

Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current.

The recommended state for this setting is 90 or fewer days but not 0.

Audit:

On a command line type DSPSSTSECA and press ENTER
Verify that the Service tools password expiration interval is 90

Remediation:

To change the default password expiration interval from 180 days, follow these steps.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) PWDEXPITV(90)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=policies-changing-service-tools-system-password-expiration-interval

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.6.2 (L1) System Service Tools Changing the maximum failed sign-on attempts (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines the number of failed logon attempts before the account is locked.

The recommended state for this setting is: 3

Rationale:

Setting an account lockout threshold reduces the likelihood that an attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

Audit:

On a command line type DSPSSTSECA and press ENTER
Verify that the Service tools Maximum sign-on attempts is set to 3

Remediation:

To change the default maximum failed sign-on attempts before the user ID is disabled, follow these steps.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) MAXSGN(3)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=policies-changing-maximum-failed-sign-attempts

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.6.3 (L1) System Service Tools Changing the duplicate password control (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines the duplicate password control.

The recommended state for this setting is: 18

Rationale:

The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced.

Audit:

On a command line type DSPSSTSECA and press ENTER
Verify that the Service Duplicate password control is set to 18

Remediation:

To change the default duplicate password control, complete these steps.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) DUPPWDCTL(18)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=policies-changing-duplicate-password-control

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.6.4 (L1) System Service Tools Password Level (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines the password level for System Service Tools.

The recommended state for this setting is: PWLVL 2

Rationale:

The default password level (PWLVL 1) uses deprecated DES encryption. To change to use SHA encryption, the System Service Tools Password Level should be set to PWLVL 2 for better security.

Audit:

- On a command line type DSPSSTSECA and press ENTER
- Verify that the Service tools password level is 2

Remediation:

To change the service tools password level.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) SSTPWDLVL(2)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=concepts-password-policies-service-tools-user-ids

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	9 Limitation and Control of Network Ports, Protocols, and Services Limitation and Control of Network Ports, Protocols, and Services			

4.6.5 (L1) System Service Tools Allow New Digital Certificates (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines if new certificates can be added to the local system's *SIGNATUREVERIFICATION certificate store and also allows passwords for digital certificate stores to be reset by any user with *ALLOBJ and *SECADM.

The recommended state for this setting is: 0

Rationale:

Under normal operations, new certificates should rarely be added to the local system's *SIGNATUREVERIFICATION certificate store. More importantly, passwords for digital certificate stores should be secured from being reset by any user with *ALLOBJ and *SECADM.

Audit:

On a command line type DSPSSTSECA and press ENTER
Verify that the Service tools Allow add of digital certificates is set to *NO

Remediation:

To change the service tools Allow add of digital certificates value.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) ADDDIGCERT(*NO)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.6.6 (L1) System Service Tools IDs and Privileges (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines the functional privileges of System Service Tool Users.

Rationale:

All System Service Tools Users are powerful administrators. Service Tools Users should follow the same policy as Operating System Users.

• Each Service Tool User should be unique (no shared passwords)

• Each Service Tool User should follow the Principle of Least Privilege to perform their job role

• Inactive Service Tool Users should be disabled/removed.

• IBM provides the following service tools User IDs:

o QSECOFR

o QSRV

Audit:

1. Type DSPSSTUSR OUTPUT(*PRINT) and press Enter.
2. Type WRKSLPF and press Enter.
3. Locate and display your spool file named QPSYSSTUSR with User Data DSPSSTUSR.
4. Review this information with your system administrator and ensure that all SST users have unique profiles. Do not use the shipped IBM User IDs.
5. Ensure that all Service Tools IDs have the proper functional privileges for their job roles.

Remediation:

Disable/Remove inactive IDs and ensure that each ID has the required privileges.

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=ids-recommendations-managing-service-tools-user

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

4.6.7 (L1) System Service Tools locking security-related system values (Automated)

Profile Applicability:

- Level 1

Description:

This policy setting determines is users are prevented from changing security-related system values during normal operations.

The recommended state for this setting is: 0

Rationale:

During normal operations, changes to the security related system values should be locked to prevent them from being changed. Changes to security related system values should only be performed during maintenance, licensed program installations or system upgrades.

Audit:

DSPSSTSECA and press Enter.
Observe the value for Allow change of security related system values and verify it = *NO

Remediation:

To lock System Security Values.
CHGSSTSECA REQUSRID(<*xxxxxx*>) REQPWD(<*xxxxxx*>) SECSYSVAL(*NO)

References:

1. https://www.ibm.com/docs/en/i/7.5?topic=values-locking-unlocking-security-related-system

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

4.6.8 (L1) System Service Tools Password Rules (Automated)

Profile Applicability:

- Level 1

Description:

Specifies the rules used to check whether a password is formed correctly.

Rationale:

This provides additional security by having a system in place to verify if a password meets the specified rules set.

Audit:

- From a command line type DSPSSTSECA and press Enter
- Verify the following Password Rules are set:
    1. Limit profile name is *YES
    2. Hours to block password change is 24
    3. Minimum password length is 10
    4. Maximum password length is 128
    5. Use characters from three groups is *YES
    6. Minimum digits is 1
    7. Limit adjacent digits is *YES
    8. Limit digit first position is *YES
    9. Limit digit last position is *YES
    10. Limit adjacent special characters is *YES
    11. Limit special character first position is *YES
    12. Limit special character last position is *YES

Remediation:

- Access service tools using SST. On a command line, type STRSST and press Enter.
- Select option 8 (Work with service tools user IDs and Devices)
- Select option 5 (Work with service tools security options)
- Set the following options to the following values
    1. Block password change is 24
    2. Maximum password length is 128
    3. Minimum password length is 10
    4. Limit profile name is 1 (1=Yes)
    5. Limit digit first is 1 (1=Yes)
    6. Limit digit last is 1 (1=Yes)
    7. Limit digit adjacent is 1 (1=Yes)
    8. Limit special character first is *YES 1 (1=Yes)
    9. Limit special character last is *YES 1 (1=Yes)
    10. Limit special characters adjacent is 1 (1=Yes)
    11. Require 3 of 4 characters adjacent is 1 (1=Yes)
    12. Minimum digits required is 1

Press Enter to save changes.
Press F3 2 times and press Enter to exit System Service Tools.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

4.6.9 (L1) System Service Tools Allow add and remove of password exit programs (Automated)

Profile Applicability:

- Level 1

Description:

Controls the ability of system administrators to add or remove a registered password exit program.

Rationale:

This provides additional security by having a control in place to prevent system administrator's ability to add or remove a password exit program.

Audit:

- From a command line type DSPSSTSECA and press Enter
- Verify that the Allow add and remove of password exit program is set to *NO

Remediation:

To change the service tools Add and remove pwd exit pgms value.
CHGSSTSECA REQUSRID() REQPWD() PWDEXITPGM(*NO)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			
v7	16.13 Alert on Account Login Behavior Deviation Alert when users deviate from normal login behavior, such as time-of-day, workstation location and duration.			●

5 QSECOFR Profile

QSECOFR shall be configured with a non-trivial password which shall be transferred by the IBM i Security Officer to a document placed inside a sealed envelope and stored in a secure location such as a bank vault or secure on-site lock box or safe. QSECOFR's password shall not be shared or used under normal system operations and shall only be used in emergencies.

The password shall be changed at regular intervals and replaced in the secure location.

*5.1 (L1) QSECOFR Profile Shall Be *DISABLED (Automated)*

Profile Applicability:

- Level 1

Description:

The QSECOFR profile shall be *DISABLED to prevent interactive use. You can always sign on with the QSECOFR profile at the console, even if the status of QSECOFR is *DISABLED.

Rationale:

QSECOFR is the most powerful profile on the IBM i and is equivalent to the UNIX Root Profile. Additionally, you should prevent QSECOFR from interactively signing on by *DISABLING it and create unique security officer profiles as required by the business.

Impact:

*DISABLEing QSECOFR will prevent anonymous and un-accountable use of QSECOFR for normal operations.

Audit:

- DSPUSRPRF USRPRF(QSECOFR)
- Observe the Status to ensure that it is *DISABLED

Remediation:

CHGUSRPRF USRPRF(QSECOFR) STATUS(*DISABLED)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

5.2 (L1) QSECOFR Shall Not be Configured as a Group Profile (Automated)

Profile Applicability:

- Level 1

Description:

QSECOFR shall not be a group profile as this would allow group members to inherit root privileges from the shipped IBM QSECOFR profile.

Rationale:

Do not use IBM profiles as groups. Instead, create your own group profiles with appropriate privileges (special authorities) commensurate with your job roles and the Principle of Least Privilege (PoLP).

Audit:

DSPUSRPRF USRPRF(QSECOFR) TYPE(*GRPMBR)
Ensure that message states that "User profile QSECOFR not a group profile".

Remediation:

Change any QSECOFR group members to another user created group with appropriate privileges (special authorities) commensurate with your job roles and the Principle of Least Privilege (PoLP).

- CHGUSRPRF USRPRF(<*XXXXXX*>) GRPPRF(<*XXXXXX*>)

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			
v7	16 Account Monitoring and Control Account Monitoring and Control			

6 Auditing

Auditing shall be enabled to capture security related user access and actions, special privilege access and actions, configuration changes, and privileged administrative methods. The IBM i security audit journal, associated journal receivers and receiver library shall be secured as follows:

- QAUDJRN = *PUBLIC *EXCLUDE and owned by QSYS
- Associated QAUDJRN journal receivers = *PUBLIC *EXCLUDE and owned by QSYS
- Associated QAUDJRN library = *PUBLIC *EXCLUDE and owned by QSYS

Relevant security events shall be examined on a regular basis to determine if attacks or malicious activity has occurred. Audit logs must be retained according to policy and/or regulatory requirements.

7 Monitoring

The IBM i must be monitored to ensure compliance network security policies and standards. Security personnel must test the IBM i configuration and security controls for effectiveness and compliance.

8 Documentation

Procedures to implement IBM i security must be documented. User accounts and associated privileges must be documented. All documentation must be reviewed at least annually to ensure compliance with network security policies and standards. Account documentation must be reviewed quarterly to ensure that it is current and accurate. Documentation must be stored in a secure location and must be readily available.

9 Physical Security

There must be strong physical security around the IBM i server. All production IBM i servers need to be housed in physically secure environments with limited access.

10 Disaster Recovery

During a complete disaster recovery after a catastrophic system failure, some of the system values in Table 1 will need to be changed to allow a full system restore. Follow the normal procedures found in IBM i Backup & Recovery (SC41-5304) and then follow the steps below:

• After the LIC and Operating System restore completes, you will see the IPL Options screen. On the IPL Options screen, ensure that the “Define or change system at IPL” option is set to Y for yes as shown below.

```
                      IPL Options

Type choices, press Enter.

System date . . . . . . . . . . . . . . . 08/01/04  MM/DD/Y
System time . . . . . . . . . . . . . . . 16:58:00  HH:MM:S
System time zone . . . . . . . . . . . . .  Q0000UTC  F4 for list
Clear job queues . . . . . . . . . . . . .  N         Y=Yes, N=NO
Clear output queues . . . . . . . . . . . N         Y=Yes, N=NO
Clear incomplete job logs . . . . . . . . N         Y=Yes, N=NO
Start print writers . . . . . . . . . . . N         Y=Yes, N=NO
Start system to restricted state . . . .  Y         Y=Yes, N=NO

Set major system options . . . . . . . . .  Y         Y=Yes, N=NO
Define or change system at IPL . . . . .  Y         Y=Yes, N=NO
```

• On the Set Major System Options screen, select Y to enable automatic configuration.

• Select 3, System Value Commands.

• On the System Value Commands screen, select 3, Work with System Values.

• On the Work with System Values screen, select the System Value that you plan to change by placing a ″2″ next to it. Press Enter ONLY after you select all the values that you wish to change.

• Update the following System Values. Write down the existing values so you can update them after the recovery, if necessary.

- Change QALWOBJRST to *ALL
- Change QJOBMSGQFL to *PRTWRAP
- Change QJOBMSGQMX size to a minimum value of 30
- Change QPFRADJ to 2
- Change QVFYOBJRST to 1
- Change QFRCCVNRST to 0

After changing the system values listed above and restoring your licensed programs and user data, set the system values back to the previous value that you wrote down above and ensure that they meet the standards value in Table 1.

11 Licensed Program Installation Procedure

During an installation of IBM i licensed program options and products, the following system values require a change. Write down the current value prior to changing and change it back to its previous value when the licensed program installation is complete.

- Change QALWOBJRST to *ALL

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Access Control**		
2	**Adopted Authority**		
3	**User Profiles**		
3.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority) (Automated)	☐	☐
3.2	(L1) User Profile (*USRPRF) Access Controls (Private authority) (Automated)	☐	☐
3.3	(L1) User Profile (*USRPRF) Object Ownership (Automated)	☐	☐
3.4	(L1) Administrative Special Authorities (Automated)	☐	☐
3.5	(L1) User Profile Action Auditing (Automated)	☐	☐
3.6	(L1) Default Passwords (Automated)	☐	☐
3.7	(L1) Inactive Profiles (Automated)	☐	☐
3.8	(L1) User Profile With Non-Expiring Passwords (Automated)	☐	☐
3.9	(L1) User Profiles With Command Line Access (Automated)	☐	☐
3.10	(L1) IBM Supplied User Profiles (Automated)	☐	☐
3.11	(L1) Group Profiles With Passwords (Automated)	☐	☐
4	**System Configuration**		
4.1	**Security System Values**		
4.1.1	**Level 1**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.1.1	(L1) Allow Restoration of Security-Sensitive Objects (Automated)	☐	☐
4.1.1.2	(L1) Set Attention Program (Automated)	☐	☐
4.1.1.3	(L1) Set Auditing Control (Automated)	☐	☐
4.1.1.4	(L1) Set Auditing End Action (Automated)	☐	☐
4.1.1.5	(L1) Set Auditing Force Level (Automated)	☐	☐
4.1.1.6	(L1) Set Auditing Level (Automated)	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions (Automated)	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration (Automated)	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration (Automated)	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation (Automated)	☐	☐
4.1.1.11	(L1) Set Create Authority (Automated)	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval (Automated)	☐	☐
4.1.1.13	(L1) Set Display User Sign-on Information (Automated)	☐	☐
4.1.1.14	(L1) Set Force Conversion On Restore (Automated)	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval (Automated)	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue (Automated)	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions (Automated)	☐	☐
4.1.1.18	(L1) Set Limit Security Officer Access to Workstations (Automated)	☐	☐
4.1.1.19	(L1) Set Maximum Sign-on Action (Automated)	☐	☐
4.1.1.20	(L1) Set Maximum Sign-on Attempts (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.1.21	(L1) Set Block Password Change (Automated)	☐	☐
4.1.1.22	(L1) Set Password Expiration Interval (Automated)	☐	☐
4.1.1.23	(L1) Set Password Expiration Warning (Automated)	☐	☐
4.1.1.24	(L1) Set Password Level (Automated)	☐	☐
4.1.1.25	(L1) Set Required Difference in Passwords (Automated)	☐	☐
4.1.1.26	(L1) Set Password Rules (Automated)	☐	☐
4.1.1.27	(L1) Retain Server Security (Automated)	☐	☐
4.1.1.28	(L1) Set Remote IPL (Automated)	☐	☐
4.1.1.29	(L1) Set Remote Sign-on Value (Automated)	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute (Automated)	☐	☐
4.1.1.31	(L1) Scan File System (Automated)	☐	☐
4.1.1.32	(L1) Set Scan File System Control (Automated)	☐	☐
4.1.1.33	(L1) Set System Security Level (Automated)	☐	☐
4.1.1.34	(L1) Set Shared Memory Control (Automated)	☐	☐
4.1.1.35	(L1) Secure Sockets Layer Cipher Specification List (Automated)	☐	☐
4.1.1.36	(L1) Secure Sockets Layer Cipher Control (Automated)	☐	☐
4.1.1.37	(L1) Secure Socket Layer Security protocols (Automated)	☐	☐
4.1.1.38	(L1) System Library List (Automated)	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority (Automated)	☐	☐
4.1.1.40	(L1) Verify Object On Restore (Automated)	☐	☐
4.1.2	**Level 2**		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.2.1	(L2) Allow Restoration of Security-Sensitive Objects (Automated)	☐	☐
4.1.2.2	(L2) Allow User Domain Objects in These Libraries (Automated)	☐	☐
4.1.2.3	(L2) Set Auditing Control (Automated)	☐	☐
4.1.2.4	(L2) Set Auditing End Action (Automated)	☐	☐
4.1.2.5	(L2) Set Auditing Force Level (Automated)	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation (Automated)	☐	☐
4.1.2.7	(L2) Set Create Authority (Automated)	☐	☐
4.1.2.8	(L2) Set Create Object Audit Level (Automated)	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval (Automated)	☐	☐
4.1.2.10	(L2) Set Force Conversion On Restore (Automated)	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval (Automated)	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue (Automated)	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions (Automated)	☐	☐
4.1.2.14	(L2) Set Limit Security Officer Access to Workstations (Automated)	☐	☐
4.1.2.15	(L2) Set Maximum Sign-on Action (Automated)	☐	☐
4.1.2.16	(L2) Set Maximum Sign-on Attempts (Automated)	☐	☐
4.1.2.17	(L2) Set Block Password Change (Automated)	☐	☐
4.1.2.18	(L2) Set Password Level (Automated)	☐	☐
4.1.2.19	(L2) Set Required Difference in Passwords (Automated)	☐	☐
4.1.2.20	(L2) Set Password Rules (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.2.21	(L2) Set Password Validation Program (Automated)	☐	☐
4.1.2.22	(L2) Set Remote Sign-on Value (Automated)	☐	☐
4.1.2.23	(L2) Set System Security Level (Automated)	☐	☐
4.1.2.24	(L2) Set Shared Memory Control (Automated)	☐	☐
4.1.2.25	(L2) Verify Object On Restore (Automated)	☐	☐
4.2	**Network Services**		
4.2.1	(L1) Network Attribute JOBACN (Network Job Action) (Automated)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes (Automated)	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes (Automated)	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes (Automated)	☐	☐
4.2.5	(L1) NFS Shares (Automated)	☐	☐
4.2.6	(L2) NFS Shares (Automated)	☐	☐
4.2.7	(L1) Exit Points (Automated)	☐	☐
4.2.8	(L1) Telnet Protocol (Automated)	☐	☐
4.2.9	(L1) FTP Protocol (Automated)	☐	☐
4.3	**IBM i Netserver security**		
4.3.1	(L1) IBM i NetServer Guest Profile (Automated)	☐	☐
4.3.2	(L1) IBM i NetServer LANMAN Password Hash (Automated)	☐	☐
4.3.3	(L1) IBM i SMB Signing (Automated)	☐	☐
4.3.4	(L1) IBM i SMBv2 Server (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.5	(L1) IBM i NetServer Shares (Automated)	☐	☐
4.3.6	(L2) NetServer Browse Interval (Automated)	☐	☐
4.4	**IBM i SSH Server security**		
4.4.1	(L1) Configuring SSH – server protocol 2 (Automated)	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration (Automated)	☐	☐
4.4.3	(L1) Configuring SSH – disallow host based authentication (Automated)	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation (Automated)	☐	☐
4.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less (Automated)	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Automated)	☐	☐
4.4.7	(L1) Configuring SSH – restrict Cipher list (Automated)	☐	☐
4.4.8	(L1) Configuring SSH – Limit Access Via SSH (Automated)	☐	☐
4.5	**IBM i Patch Management**		
4.5.1	(L1) IBM i Patch Management (Automated)	☐	☐
4.6	**System Service Tools**		
4.6.1	(L1) System Service Tools Password Expiration Interval (Automated)	☐	☐
4.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts (Automated)	☐	☐
4.6.3	(L1) System Service Tools Changing the duplicate password control (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.6.4	(L1) System Service Tools Password Level (Automated)	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates (Automated)	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges (Automated)	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values (Automated)	☐	☐
4.6.8	(L1) System Service Tools Password Rules (Automated)	☐	☐
4.6.9	(L1) System Service Tools Allow add and remove of password exit programs (Automated)	☐	☐
5	**QSECOFR Profile**		
5.1	(L1) QSECOFR Profile Shall Be *DISABLED (Automated)	☐	☐
5.2	(L1) QSECOFR Shall Not be Configured as a Group Profile (Automated)	☐	☐
6	**Auditing**		
7	**Monitoring**		
8	**Documentation**		
9	**Physical Security**		
10	**Disaster Recovery**		
11	**Licensed Program Installation Procedure**		

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
3.9	(L1) User Profiles With Command Line Access	☐	☐
3.10	(L1) IBM Supplied User Profiles	☐	☐
3.11	(L1) Group Profiles With Passwords	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes	☐	☐
4.2.8	(L1) Telnet Protocol	☐	☐
4.2.9	(L1) FTP Protocol	☐	☐
4.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
3.9	(L1) User Profiles With Command Line Access	☐	☐
3.10	(L1) IBM Supplied User Profiles	☐	☐
3.11	(L1) Group Profiles With Passwords	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.18	(L1) Set Limit Security Officer Access to Workstations	☐	☐
4.1.1.19	(L1) Set Maximum Sign-on Action	☐	☐
4.1.1.20	(L1) Set Maximum Sign-on Attempts	☐	☐
4.1.1.21	(L1) Set Block Password Change	☐	☐
4.1.1.22	(L1) Set Password Expiration Interval	☐	☐
4.1.1.25	(L1) Set Required Difference in Passwords	☐	☐
4.1.1.26	(L1) Set Password Rules	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.14	(L2) Set Limit Security Officer Access to Workstations	☐	☐
4.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
4.1.2.16	(L2) Set Maximum Sign-on Attempts	☐	☐
4.1.2.17	(L2) Set Block Password Change	☐	☐
4.1.2.19	(L2) Set Required Difference in Passwords	☐	☐
4.1.2.20	(L2) Set Password Rules	☐	☐
4.1.2.21	(L2) Set Password Validation Program	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes	☐	☐
4.2.8	(L1) Telnet Protocol	☐	☐
4.2.9	(L1) FTP Protocol	☐	☐
4.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.1	(L1) System Service Tools Password Expiration Interval	☐	☐
4.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts	☐	☐
4.6.3	(L1) System Service Tools Changing the duplicate password control	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐
4.6.8	(L1) System Service Tools Password Rules	☐	☐
4.6.9	(L1) System Service Tools Allow add and remove of password exit programs	☐	☐
5.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v7.0	☐	☐

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
3.10	(L1) IBM Supplied User Profiles	☐	☐
3.11	(L1) Group Profiles With Passwords	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes	☐	☐
4.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
3.9	(L1) User Profiles With Command Line Access	☐	☐
3.10	(L1) IBM Supplied User Profiles	☐	☐
3.11	(L1) Group Profiles With Passwords	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes	☐	☐
4.2.8	(L1) Telnet Protocol	☐	☐
4.2.9	(L1) FTP Protocol	☐	☐
4.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.4	(L1) Administrative Special Authorities	☐	☐
3.5	(L1) User Profile Action Auditing	☐	☐
3.6	(L1) Default Passwords	☐	☐
3.7	(L1) Inactive Profiles	☐	☐
3.9	(L1) User Profiles With Command Line Access	☐	☐
3.10	(L1) IBM Supplied User Profiles	☐	☐
3.11	(L1) Group Profiles With Passwords	☐	☐
4.1.1.2	(L1) Set Attention Program	☐	☐
4.1.1.3	(L1) Set Auditing Control	☐	☐
4.1.1.6	(L1) Set Auditing Level	☐	☐
4.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
4.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
4.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
4.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
4.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
4.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
4.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
4.1.1.17	(L1) Set Limit Device Sessions	☐	☐
4.1.1.18	(L1) Set Limit Security Officer Access to Workstations	☐	☐
4.1.1.27	(L1) Retain Server Security	☐	☐
4.1.1.28	(L1) Set Remote IPL	☐	☐
4.1.1.30	(L1) Set Remote Service Attribute	☐	☐
4.1.1.33	(L1) Set System Security Level	☐	☐
4.1.1.34	(L1) Set Shared Memory Control	☐	☐
4.1.1.38	(L1) System Library List	☐	☐
4.1.1.39	(L1) Set Use Adopted Authority	☐	☐
4.1.2.3	(L2) Set Auditing Control	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
4.1.2.8	(L2) Set Create Object Audit Level	☐	☐
4.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
4.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
4.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
4.1.2.13	(L2) Set Limit Device Sessions	☐	☐
4.1.2.14	(L2) Set Limit Security Officer Access to Workstations	☐	☐
4.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
4.1.2.23	(L2) Set System Security Level	☐	☐
4.1.2.24	(L2) Set Shared Memory Control	☐	☐
4.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
4.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
4.2.3	(L1) DDM TCP/IP Attributes	☐	☐
4.2.4	(L2) DDM TCP/IP Attributes	☐	☐
4.2.8	(L1) Telnet Protocol	☐	☐
4.2.9	(L1) FTP Protocol	☐	☐
4.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
4.3.3	(L1) IBM i SMB Signing	☐	☐
4.3.6	(L2) NetServer Browse Interval	☐	☐
4.4.2	(L1) Configuring SSH – banner configuration	☐	☐
4.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
4.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
4.5.1	(L1) IBM i Patch Management	☐	☐
4.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
4.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
4.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
3.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority)	☐	☐
3.2	(L1) User Profile (*USRPRF) Access Controls (Private authority)	☐	☐
3.3	(L1) User Profile (*USRPRF) Object Ownership	☐	☐
3.8	(L1) User Profile With Non-Expiring Passwords	☐	☐
4.1.1.1	(L1) Allow Restoration of Security-Sensitive Objects	☐	☐
4.1.1.4	(L1) Set Auditing End Action	☐	☐
4.1.1.5	(L1) Set Auditing Force Level	☐	☐
4.1.1.11	(L1) Set Create Authority	☐	☐
4.1.1.13	(L1) Set Display User Sign-on Information	☐	☐
4.1.1.14	(L1) Set Force Conversion On Restore	☐	☐
4.1.1.19	(L1) Set Maximum Sign-on Action	☐	☐
4.1.1.20	(L1) Set Maximum Sign-on Attempts	☐	☐
4.1.1.21	(L1) Set Block Password Change	☐	☐
4.1.1.22	(L1) Set Password Expiration Interval	☐	☐
4.1.1.23	(L1) Set Password Expiration Warning	☐	☐
4.1.1.24	(L1) Set Password Level	☐	☐
4.1.1.25	(L1) Set Required Difference in Passwords	☐	☐
4.1.1.26	(L1) Set Password Rules	☐	☐
4.1.1.29	(L1) Set Remote Sign-on Value	☐	☐
4.1.1.31	(L1) Scan File System	☐	☐
4.1.1.32	(L1) Set Scan File System Control	☐	☐
4.1.1.35	(L1) Secure Sockets Layer Cipher Specification List	☐	☐
4.1.1.36	(L1) Secure Sockets Layer Cipher Control	☐	☐
4.1.1.37	(L1) Secure Socket Layer Security protocols	☐	☐
4.1.1.40	(L1) Verify Object On Restore	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.1.2.1	(L2) Allow Restoration of Security-Sensitive Objects	☐	☐
4.1.2.2	(L2) Allow User Domain Objects in These Libraries	☐	☐
4.1.2.4	(L2) Set Auditing End Action	☐	☐
4.1.2.5	(L2) Set Auditing Force Level	☐	☐
4.1.2.7	(L2) Set Create Authority	☐	☐
4.1.2.10	(L2) Set Force Conversion On Restore	☐	☐
4.1.2.16	(L2) Set Maximum Sign-on Attempts	☐	☐
4.1.2.17	(L2) Set Block Password Change	☐	☐
4.1.2.18	(L2) Set Password Level	☐	☐
4.1.2.19	(L2) Set Required Difference in Passwords	☐	☐
4.1.2.20	(L2) Set Password Rules	☐	☐
4.1.2.21	(L2) Set Password Validation Program	☐	☐
4.1.2.22	(L2) Set Remote Sign-on Value	☐	☐
4.1.2.25	(L2) Verify Object On Restore	☐	☐
4.2.5	(L1) NFS Shares	☐	☐
4.2.6	(L2) NFS Shares	☐	☐
4.2.7	(L1) Exit Points	☐	☐
4.3.2	(L1) IBM i NetServer LANMAN Password Hash	☐	☐
4.3.4	(L1) IBM i SMBv2 Server	☐	☐
4.3.5	(L1) IBM i NetServer Shares	☐	☐
4.4.1	(L1) Configuring SSH – server protocol 2	☐	☐
4.4.3	(L1) Configuring SSH – disallow host based authentication	☐	☐
4.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less	☐	☐
4.4.7	(L1) Configuring SSH – restrict Cipher list	☐	☐
4.4.8	(L1) Configuring SSH – Limit Access Via SSH	☐	☐
4.6.1	(L1) System Service Tools Password Expiration Interval	☐	☐
4.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts	☐	☐
4.6.3	(L1) System Service Tools Changing the duplicate password control	☐	☐
4.6.4	(L1) System Service Tools Password Level	☐	☐

Recommendation		Set Correctly	
		Yes	No
4.6.8	(L1) System Service Tools Password Rules	☐	☐
4.6.9	(L1) System Service Tools Allow add and remove of password exit programs	☐	☐
5.2	(L1) QSECOFR Shall Not be Configured as a Group Profile	☐	☐