

CIS IBM i V7R5M0 Benchmark

v2.1.0 - 08-15-2025

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/>

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is **NEVER** acceptable to host a CIS Benchmark in **ANY** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Terms of Use	1
Table of Contents	2
Overview	7
Important Usage Information	7
Key Stakeholders.....	7
Apply the Correct Version of a Benchmark	8
Exceptions	8
Remediation	9
Summary.....	9
Target Technology Details	10
Intended Audience	10
Consensus Guidance.....	11
Typographical Conventions	12
Recommendation Definitions	13
Title.....	13
Assessment Status	13
Automated	13
Manual.....	13
Profile.....	13
Description	13
Rationale Statement.....	13
Impact Statement.....	14
Audit Procedure.....	14
Remediation Procedure	14
Default Value	14
References	14
CIS Critical Security Controls® (CIS Controls®).....	14
Additional Information	14
Profile Definitions	15
Acknowledgements.....	16
Recommendations	17
1 Introduction to IBM i Security	17
Preventing and Detecting Security Exposures	20
DevSecOps	22
Effective Data Security is a Marathon not a Sprint	22
Introduction to Governance, Risk Management and Compliance	23

CIS and NIST 800-53 Mappings	23
2 Adopted Authority	23
CIS Controls:	24
3 Resource Security	25
CIS Controls:	26
4 User Profiles	29
4.1 (L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority) (Automated)	30
4.2 (L1) User Profile (*USRPRF) Access Controls (Private authority) (Automated)	33
4.3 (L1) User Profile (*USRPRF) Object Ownership (Automated)	37
4.4 (L1) Administrative Special Authorities (Automated)	40
4.5 (L1) User Profile Action Auditing (Automated)	43
4.6 (L1) Default Passwords (Automated)	45
4.7 (L1) Inactive Profiles (Automated)	47
4.8 (L1) User Profile With Non-Expiring Passwords (Automated)	49
4.9 (L1) User Profiles With Command Line Access (Automated)	51
4.10 (L1) IBM Supplied User Profiles (Automated)	53
4.11 (L1) Group Profiles With Passwords (Automated) (Automated)	57
4.12 (L1) Implement Multi-factor authentication (MFA) (Manual)	59
5 System Configuration	61
5.1 Security System Values	62
5.1.1 Level 1	63
5.1.1.1 (L1) Set Allow Restoration of Security-Sensitive Objects (Automated)	64
5.1.1.2 (L1) Set Attention Program (Automated)	67
5.1.1.3 (L1) Set Auditing Control (Automated)	68
5.1.1.4 (L1) Set Auditing End Action (Automated)	69
5.1.1.5 (L1) Set Auditing Force Level (Automated)	70
5.1.1.6 (L1) Set Auditing Level (Automated)	71
5.1.1.7 (L1) Set Security Auditing Level Extensions (Automated)	73
5.1.1.8 (L1) Set Automatic Device Configuration (Automated)	74
5.1.1.9 (L1) Set Automatic Remote Controller Configuration (Automated)	75
5.1.1.10 (L1) Set Automatic Virtual Device Creation (Automated)	76
5.1.1.11 (L1) Set Create Authority (Automated)	77
5.1.1.12 (L1) Set Disconnect-Job Interval (Automated)	78
5.1.1.13 (L1) Set Display User Sign-on Information (Automated)	79
5.1.1.14 (L1) Set Force Conversion On Restore (Automated)	80
5.1.1.15 (L1) Set Inactivity Time-out Interval (Automated)	81
5.1.1.16 (L1) Set Inactivity Message Queue (Automated)	82
5.1.1.17 (L1) Set Limit Device Sessions (Automated)	83
5.1.1.18 (L1) Set Limit Security Officer Access to Workstations (Automated)	84
5.1.1.19 (L1) Set Maximum Sign-on Action (Automated)	85
5.1.1.20 (L1) Set Maximum Sign-on Attempts (Automated)	86
5.1.1.21 (L1) Set Block Password Change (Automated)	87
5.1.1.22 (L1) Set Password Expiration Interval (Automated)	88
5.1.1.23 (L1) Set Password Expiration Warning (Automated)	89
5.1.1.24 (L1) Set Password Level (Automated)	90
5.1.1.25 (L1) Set Required Difference in Passwords (Automated)	92
5.1.1.26 (L1) Set Password Rules (Automated)	94
5.1.1.27 (L1) Set Retain Server Security (Automated)	95
5.1.1.28 (L1) Set Remote IPL (Automated)	96
5.1.1.29 (L1) Set Remote Sign-on Value (Automated)	97
5.1.1.30 (L1) Set Remote Service Attribute (Automated)	98
5.1.1.31 (L1) Set Scan File System (Automated)	99
5.1.1.32 (L1) Set Scan File System Control (Automated)	100

5.1.1.33 (L1) Set System Security Level (Automated)	101
5.1.1.34 (L1) Set Shared Memory Control (Automated)	102
5.1.1.35 (L1) Set Secure Sockets Layer Cipher Specification List (Automated)	103
5.1.1.36 (L1) Set Secure Sockets Layer Cipher Control (Automated)	105
5.1.1.37 (L1) Set Secure Socket Layer Security Protocols (Automated)	106
5.1.1.38 (L1) Set System Library List (Automated)	108
5.1.1.39 (L1) Set Use Adopted Authority (Automated)	110
5.1.1.40 (L1) Set Verify Object On Restore (Automated)	111
5.1.2 Level 2	113
5.1.2.1 (L2) Set Allow Restoration of Security-Sensitive Objects (Automated)	114
5.1.2.2 (L2) Set Allow User Domain Objects in These Libraries (Automated)	116
5.1.2.3 (L2) Set Auditing Control (Automated)	118
5.1.2.4 (L2) Set Auditing End Action (Automated)	119
5.1.2.5 (L2) Set Auditing Force Level (Automated)	121
5.1.2.6 (L2) Set Automatic Virtual Device Creation (Automated)	122
5.1.2.7 (L2) Set Create Authority (Automated)	123
5.1.2.8 (L2) Set Create Object Audit Level (Automated)	125
5.1.2.9 (L2) Set Disconnect-Job Interval (Automated)	126
5.1.2.10 (L2) Set Force Conversion On Restore (Automated)	127
5.1.2.11 (L2) Set Inactivity Time-out Interval (Automated)	128
5.1.2.12 (L2) Set Inactivity Message Queue (Automated)	129
5.1.2.13 (L2) Set Limit Device Sessions (Automated)	130
5.1.2.14 (L2) Set Limit Security Officer Access to Workstations (Automated)	131
5.1.2.15 (L2) Set Maximum Sign-on Action (Automated)	133
5.1.2.16 (L2) Set Maximum Sign-on Attempts (Automated)	134
5.1.2.17 (L2) Set Block Password Change (Automated)	135
5.1.2.18 (L2) Set Password Expiration Interval (Automated)	136
5.1.2.19 (L2) Set Required Difference in Passwords (Automated)	138
5.1.2.20 (L2) Set Password Rules (Automated)	139
5.1.2.21 (L2) Set Password Validation Program (Automated)	140
5.1.2.22 (L2) Set Remote Sign-on Value (Automated)	142
5.1.2.23 (L2) Set System Security Level (Automated)	143
5.1.2.24 (L2) Set Shared Memory Control (Automated)	144
5.1.2.25 (L2) Set Verify Object On Restore (Automated)	145
5.2 Network Services	146
5.2.1 (L1) Network Attribute JOBACN (Network Job Action) (Automated)	147
5.2.2 (L1) DDM Remote Configuration List (SNA) Attributes (Automated)	149
5.2.3 (L1) DDM TCP/IP Attributes (Automated)	151
5.2.4 (L2) DDM TCP/IP Attributes (Automated)	154
5.2.5 (L1) NFS Shares (Automated)	157
5.2.6 (L2) NFS Shares (Automated)	159
5.2.7 (L1) Exit Points (Automated)	161
5.2.8 (L1) Function Usage (Automated)	164
5.2.9 (L1) Intrusion Detection (Manual)	167
5.2.10 (L1) Telnet Protocol (Automated)	168
5.2.11 (L1) FTP Protocol (Automated)	170
5.2.12 (L1) SMTP Mail Relay (Manual)	172
5.2.13 (L1) SNMP Access (Manual)	174
5.3 IBM i NetServer security	176
5.3.1 (L1) IBM i NetServer Guest Profile (Automated)	177
5.3.2 (L1) IBM i NetServer LANMAN Password Hash (Automated)	179
5.3.3 (L1) IBM i SMB Signing (Automated)	180
5.3.4 (L1) IBM i SMBv2 Server (Automated)	182
5.3.5 (L1) IBM i NetServer Shares (Automated)	185
5.3.6 (L2) NetServer Browse Interval (Automated)	187
5.3.7 (L1) Malware Defenses (Manual)	189

5.4 IBM i SSH Server security.....	191
5.4.1 (L1) Configuring SSH – server protocol 2 (Automated)	192
5.4.2 (L1) Configuring SSH – banner configuration (Automated)	194
5.4.3 (L1) Configuring SSH – disallow host based authentication (Automated)	196
5.4.4 (L1) Configuring SSH – set privilege separation (Automated)	197
5.4.5 (L1) Configuring SSH – set MaxAuthTries to 4 or Less (Automated)	199
5.4.6 (L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Automated)	200
5.4.7 (L1) Configuring SSH – restrict Cipher list (Automated)	202
5.4.8 (L1) Configuring SSH – Limit Access Via SSH (Automated)	203
5.5 IBM i Patch Management	205
5.5.1 (L1) IBM i Patch Management (Automated).....	206
5.6 System Service Tools	208
5.6.1 (L1) System Service Tools Password Expiration Interval (Automated)	209
5.6.2 (L1) System Service Tools Changing the maximum failed sign-on attempts (Automated)	211
5.6.3 (L1) System Service Tools Changing the duplicate password control (Automated).....	212
5.6.4 (L1) System Service Tools Password Level (Automated).....	213
5.6.5 (L1) System Service Tools Allow New Digital Certificates (Automated)	214
5.6.6 (L1) System Service Tools IDs and Privileges (Automated)	215
5.6.7 (L1) System Service Tools locking security-related system values (Automated)	217
5.6.8 (L1) System Service Tools Password Rules (Automated)	218
5.6.9 (L1) System Service Tools Allow add and remove of password exit programs (Automated)	219
6 QSECOFR Profile.....	220
6.1 (L1) QSECOFR Profile Shall Be *DISABLED (Automated)	221
6.2 (L1) QSECOFR Shall Not be Configured as a Group Profile (Automated)	222
7 Auditing and Monitoring.....	223
Turning Down the Noise: Adding Context to the SIEM With Modern Data Security	223
CIS Controls:.....	224
8 Penetration Testing.....	225
CIS Controls:.....	226
9 Documentation	227
10 Physical Security.....	228
Disk Encryption	228
CIS Controls:.....	228
11 Disaster Recovery	229
12 Licensed Program Installation Procedure.....	230
Appendix: Summary Table.....	231
Appendix: CIS Controls v8 IG 1 Mapped Recommendations	239
Appendix: CIS Controls v8 IG 2 Mapped Recommendations	243
Appendix: CIS Controls v8 IG 3 Mapped Recommendations	248
Appendix: CIS Controls v8 Unmapped Recommendations.....	253
Appendix: Change History	254

Overview

All CIS Benchmarks™ (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 and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

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

Important Usage Information

All Benchmarks are available free for non-commercial use from the [CIS Website](#). They can be used to manually assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- [CIS Configuration Assessment Tool \(CIS-CAT® Pro Assessor\)](#)
- [CIS Benchmarks™ Certified 3rd Party Tooling](#)

These tools make the hardening process much more scalable for large numbers of systems and applications.

NOTE: Some tooling focuses only on the Benchmark Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that **ALL** Recommendations (**Automated** and **Manual**) be addressed since all are important for properly securing systems and are typically in scope for audits.

Key Stakeholders

Cybersecurity is a collaborative effort, and cross functional cooperation is imperative within an organization to discuss, test, and deploy Benchmarks in an effective and efficient way. The Benchmarks are developed to be best practice configuration guidelines applicable to a wide range of use cases. In some organizations, exceptions to specific Recommendations will be needed, and this team should work to prioritize the problematic Recommendations based on several factors like risk, time, cost, and labor. These exceptions should be properly categorized and documented for auditing purposes.

Apply the Correct Version of a Benchmark

Benchmarks are developed and tested for a specific set of products and versions and applying an incorrect Benchmark to a system can cause the resulting pass/fail score to be incorrect. This is due to the assessment of settings that do not apply to the target systems. To assure the correct Benchmark is being assessed:

- **Deploy the Benchmark applicable to the way settings are managed in the environment:** An example of this is the Microsoft Windows family of Benchmarks, which have separate Benchmarks for Group Policy, Intune, and Stand-alone systems based upon how system management is deployed. Applying the wrong Benchmark in this case will give invalid results.
- **Use the most recent version of a Benchmark:** This is true for all Benchmarks, but especially true for cloud technologies. Cloud technologies change frequently and using an older version of a Benchmark may have invalid methods for auditing and remediation.

Exceptions

The guidance items in the Benchmarks are called recommendations and not requirements, and exceptions to some of them are expected and acceptable. The Benchmarks strive to be a secure baseline, or starting point, for a specific technology, with known issues identified during Benchmark development are documented in the Impact section of each Recommendation. In addition, organizational, system specific requirements, or local site policy may require changes as well, or an exception to a Recommendation or group of Recommendations (e.g. A Benchmark could Recommend that a Web server not be installed on the system, but if a system's primary purpose is to function as a Webserver, there should be a documented exception to this Recommendation for that specific server).

In the end, exceptions to some Benchmark Recommendations are common and acceptable, and should be handled as follows:

- The reasons for the exception should be reviewed cross-functionally and be well documented for audit purposes.
- A plan should be developed for mitigating, or eliminating, the exception in the future, if applicable.
- If the organization decides to accept the risk of this exception (not work toward mitigation or elimination), this should be documented for audit purposes.

It is the responsibility of the organization to determine their overall security policy, and which settings are applicable to their unique needs based on the overall risk profile for the organization.

Remediation

CIS has developed [Build Kits](#) for many technologies to assist in the automation of hardening systems. Build Kits are designed to correspond to Benchmark's "Remediation" section, which provides the manual remediation steps necessary to make that Recommendation compliant to the Benchmark.

When remediating systems (changing configuration settings on deployed systems as per the Benchmark's Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

- CIS Build Kits, or internally developed remediation methods should never be applied to production systems without proper testing.
- Proper testing consists of the following:
 - Understand the configuration (including installed applications) of the targeted systems. Various parts of the organization may need different configurations (e.g., software developers vs standard office workers).
 - Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.
 - Test the configuration changes with representative lab system(s). If issues arise during testing, they can be resolved prior to deploying to any production systems.
 - When testing is complete, initially deploy to a small sub-set of production systems and monitor closely for issues. If there are issues, they can be resolved prior to deploying more broadly.
 - When the initial deployment above is completed successfully, iteratively deploy to additional systems and monitor closely for issues. Repeat this process until the full deployment is complete.

Summary

Using the Benchmarks Certified tools, working as a team with key stakeholders, being selective with exceptions, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the [CIS Website](#). All other formats of the CIS Benchmarks™ (MS Word, Excel, and [Build Kits](#)) are available for CIS [SecureSuite®](#) members.

CIS-CAT® Pro is also available to CIS [SecureSuite®](#) members.

Target Technology Details

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
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
<code>Monospace font</code>	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
<Monospace font in brackets>	Text set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like Notes , Warnings , or Cautions (usually just the word itself and the rest of the text normal).

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

Leonardo Villalobos

John Vriezen

Shmuel Zailer

Kari Byrd

Editor

Edward Byrd , Center for Internet Security, New York

Recommendations

1 Introduction to IBM i Security

The IBM Systems family covers a wide range of users. Security on the IBM® i platform is flexible enough to meet the requirements of this wide range of users and situations.

A small system might have three to five users, and a large system might have several thousand users. Some installations have all their workstations in a single, relatively secure area. Others have widely distributed users, including users who connect by dialing in and indirect users connected through personal computers or system networks. You need to understand the features and options available so that you can adapt them to your own security requirements.

System security has three important objectives:

Confidentiality:

- Protecting against disclosing information to unauthorized people
- Restricting access to confidential information
- Protecting against curious system users and outsiders

Integrity:

- Protecting against unauthorized changes to data
- Restricting manipulation of data to authorized programs
- Providing assurance that data is trustworthy

Availability:

- Preventing accidental changes or destruction of data
- Protecting against attempts by outsiders to abuse or destroy system resources

System security is often associated with external threats, such as hackers or business rivals. However, protection against system accidents by authorized system users is often the greatest benefit of a well-designed security system. In a system without good security features, pressing the wrong key might result in deleting important information. System security can prevent this type of accident.

The best security system functions cannot produce good results without good planning. Security that is set up in small pieces, without planning, can be confusing. It is difficult to maintain and to audit. Planning does not imply designing the security for every file, program, and device in advance. It does imply establishing an overall approach to security on the system and communicating that approach to application designers, programmers, and system users.

As you plan security on your system and decide how much security you need, consider these questions:

- Is there a company policy or standard that requires a certain level of security?
- Do the company auditors require some level of security?
- How important is your system and the data on it to your business?
- How important is the error protection provided by the security features?
- What are your company security requirements for the future?

To facilitate installation, many of the security capabilities on your system are not activated when your system is shipped. Recommendations are provided in this topic collection to bring your system to a reasonable level of security. Consider the security requirements of your own installation as you evaluate the recommendations.

- Physical security

Physical security includes protecting the system unit, system devices, and backup media from accidental or deliberate damage. Most measures you take to ensure the physical security of your system are external to the system.

- Security level

The IBM i platform offers five levels of security. You can choose which level of security you want the system to enforce by setting the security level (QSECURITY) system value.

- System values

System values provide customization on many characteristics of your IBM i platform. You can use system values to define system-wide security settings.

- Signing

You can reinforce integrity by signing software objects that you use.

- Single sign-on enablement

Single sign-on is an authentication process in which a user can access more than one system by entering a single user ID and password. In today's heterogeneous networks with partitioned systems and multiple platforms, administrators must cope with the complexities of managing identification and authentication for network users.

- User profiles

On the IBM i operating system, every system user has a user profile. One of the most important features of a user profile are special authorities which allow users to perform administrative system functions. When users and groups on your system have unnecessary special authorities, your efforts to develop a good resource-authority scheme may be wasted. 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. In addition, control if user profiles with special authorities can be used to submit jobs and if programs run using their authority (adopted authority).

- Group profiles

A group profile is a special type of user profile. Rather than giving authority to each user individually, you can use group profiles to define authority for a group of users, including administrative special authorities. Giving special authorities to group profiles represents a security exposure. For each group, carefully evaluate the need for any special authorities. Keep track of which group profiles have special authorities and periodically review their requirement for the authority. In addition, control if group profiles with special authorities can be used to submit jobs and if programs run using their authority (adopted authority).

- Resource security

The ability to access an object is called authority. Resource security on the IBM i operating system enables you to control object authorities by defining who can use which objects and how those objects can be used.

- Security audit journal

You can use security audit journals to audit the effectiveness of security on your system.

- Independent disk pool

Independent disk pools provide the ability to group together storage that can be taken offline or brought online independent of system data or other unrelated data. The terms independent auxiliary storage pool (IASP) and independent disk pool are synonymous.

<https://www.ibm.com/docs/en/i/7.5?topic=reference-introduction-i-security>

Preventing and Detecting Security Exposures

The following information is a collection of tips to help you detect potential security exposures.

Monitoring and keeping your security policy current is a continuous process. Your system has several ways to help automate the monitoring process for you.

- Evaluating registered exit programs

You can use the system registration function to register exit programs that should be run when certain events occur. To list the registration information about your system, type `WRKREGINF OUTPUT(*PRINT)`.

- Checking scheduled programs

Since jobs can be scheduled to run in advance, it is a good idea to periodically ensure that all scheduled programs are legitimate. Before leaving the company, an employee can schedule a job that will harm your system to run some time in the future.

- Checking for user objects in protected libraries

Use object authority to control who can add programs to protected libraries. User objects other than programs can represent a security exposure when they are in system libraries.

- Limiting the use of adopted authority

When a program runs, the program can use adopted authority to gain access to objects. Be careful when allowing programs to adopt authority as it may grant permissions you do not want all the program's users to have.

- Monitoring abnormal deletions

The Print Private Authorities (PRTPVTAUT) command allows you to print a report of all the private authorities for objects of a specified type in a specified library, folder, or directory.

- Monitoring abnormal system use and access attempts

You need to monitor your system in order to watch for abnormal use and attempts to access the system. Abnormal use and access attempts will be logged on the server and will warn you of possible attacks against your system.

- Monitoring user profiles and authorities

Prevent or restrict users from installing their own programs. No program should be installed on the system without the approval of the security administrator.

- Monitoring the use of trigger programs

A trigger program is code that causes something to be done automatically once a given event occurs. Trigger programs are a productive way both to provide application functions and to manage information. Trigger programs are also a way for malicious users to damage your system.

- Preventing new programs from using adopted authority

The passing of adopted authority to programs located later in the stack provides an opportunity for a knowledgeable programmer to create a Trojan horse program.

- Mitigating Spectre and Meltdown vulnerabilities in new and existing programs

Spectre and Meltdown vulnerabilities could allow untrusted programs to obtain unauthorized access to data as described in CVE-2017-5753, CVE-2017-5715, CVE-2017-5754, and CVE-2018-3639.

- Using digital signatures to protect software integrity

Using digital signatures gives you greater control over which software can be loaded onto your system and allows you more power to detect changes once it has been loaded.

- Modifying architected transaction program names

Architecture TPNs are a normal way for communications to function and do not necessarily represent a security exposure. However, architecture TPNs might provide an unexpected entrance into your system. Learn the techniques used to prevent architected transaction program names from running on the system.

<https://www.ibm.com/docs/en/i/7.5?topic=security-preventing-detecting-exposures>

DevSecOps

DevSecOps represents a natural and necessary evolution in the way development organizations approach security. In the past, security was 'tacked on' to software at the end of the development cycle (almost as an afterthought) by a separate security team and was tested by a separate quality assurance (QA) team.

This was manageable when software updates were released just once or twice a year. But as software developers adopted Agile and DevOps practices, aiming to reduce software development cycles to weeks or even days, the traditional 'tacked-on' approach to security created an unacceptable bottleneck of technical debt and security debt.

<https://www.ibm.com/topics/devsecops#:~:text=the%20next%20step-.What%20is%20DevSecOps%3F,%2C%20deployment%2C%20and%20software%20delivery>

Integrated security testing in the software development process (DevSecOps) showed sizable ROI in 2023. Organizations with high DevSecOps adoption saved USD 1.68 million compared to those with low or no adoption. Compared to other cost-mitigating factors, DevSecOps demonstrated the largest cost savings and that goes for the IBM i too.

<https://www.ibm.com/reports/data-breach>

Effective Data Security is a Marathon not a Sprint

Enterprises often scramble to address database misconfigurations and outdated access policies prior to an annual audit. Vulnerability and risk assessments should be ongoing activities.

- Minimal effort

Many businesses adopt data security solutions just to fulfill legal or business partner requirements. This mindset of "let's implement a minimum standard and get back to business" can work against good cybersecurity practices. Effective data security is a marathon not a sprint.

- Fading urgency

Businesses can become complacent toward managing controls when regulations mature, such as the Sarbanes-Oxley Act (SOX), the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) and the California Privacy Rights Act (CPRA), formerly known as the CCPA. While, over time, leaders can be less considerate about the privacy, security and protection of regulated data, the risks and costs associated with noncompliance remain.

<https://www.ibm.com/downloads/cas/LKV1EVYD>

Introduction to Governance, Risk Management and Compliance

Over \$1 trillion USD is lost annually due to unprincipled misconduct, mistakes, and miscalculations. In a forward-thinking organization, GRC is viewed as an integrated collection of all capabilities necessary to support Principled Performance. GRC doesn't burden the business; it supports and improves it, making it a critical piece of business operations.

<https://www.oceg.org/ideas/what-is-grc>

CIS and NIST 800-53 Mappings

Both the NIST cybersecurity and CIS controls version 8 frameworks are designed to help organizations mitigate cybersecurity risks, providing recommendations for implementation no matter the organization's size or industry. While the NIST is a non-OS specific cybersecurity framework, CIS Benchmarks are OS specific settings and configurations that map closely to international frameworks like the NIST. The CIS Critical Security Controls v8 Mapping to NIST 800-53 provides a mapping of the relationships between CIS Critical Security Controls (CIS Controls) v8 and NIST SP 800-53 to help organizations understand the relationship.

<https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-800-53-rev-5>

NIST 800-53 Framework

<https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>

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.

CIS Controls:

3.7 Establish and Maintain a Data Classification Scheme Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as “Sensitive,” “Confidential,” and “Public,” and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

3 Resource Security

Resource security defines which users are allowed to use objects on the system and what operations they are allowed to perform on those objects. Also, deciding who will be allowed access to what information on your system is an important part of your security policy.

System values and user profiles control who has access to your system and prevent unauthorized users from signing on. Resource security controls the actions that authorized system users can perform after they have signed on successfully. Resource security supports the main goals of security on your system to protect:

- Confidentiality of information
- Accuracy of information to prevent unauthorized changes
- Availability of information to prevent accidental or deliberate damage

You may plan resource security differently, depending on whether your company develops applications or purchases them. For applications you develop, you should communicate the requirements for security of the information to the programmer during the application design process. When you purchase applications, you need to determine your security needs and match those needs with the way your provider has designed your applications.

Begin your resource security planning by defining your objectives.

The system offers many options for protecting the information on your system. This gives you the flexibility to design the resource security plan that is best for your company. For a basic approach to planning resource security, use these guidelines:

- Move from the general to the specific:
 - Plan security for libraries. Deal with individual objects only when necessary.
 - Plan public authority first, followed by group authority, and individual authority.
- Make the public authority for new objects in a library (CRTAUT) the same as the public authority you defined for the majority of existing objects in the library.
- Try not to give groups or individuals less authority than the public has. This diminishes performance, may lead to mistakes later, and makes auditing difficult. If you know that everyone has at least the same authority to an object that the public has, it makes planning and auditing security easier.
- Use authorization lists to group objects with the same security requirements. Authorization lists are simpler to manage than individual authorities and aid in recovery of security information.
- Create special user profiles as application owners. Set the owner password to *NONE.
- Avoid having applications owned by IBM-supplied profiles, such as QSECOFR or QPGMR.

- Use special output queues for confidential reports. Put the output queue in the same library as the confidential information.
- Limit the number of people who have security officer authority.
- Be careful when granting *ALL authority to objects or libraries. People with *ALL authority can accidentally delete things.

The Plan and set up system security in the information center is intended for the security administrator. It contains forms, examples, and guidelines for planning security for applications that have already been developed. If you have responsibility for designing an application, you might find it useful to review the forms and examples in the Plan and set up system security topic for details. They can help you view your application from the perspective of a security administrator and understand what information you need to provide.

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

<https://www.ibm.com/docs/en/i/7.5?topic=security-planning-setting-up-system>

<https://www.ibm.com/docs/en/i/7.5?topic=overview-row-column-access-control>

<https://www.ibm.com/docs/en/i/7.5?topic=language-defining-field-procedures>

CIS Controls:

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.

3.7 Establish and Maintain a Data Classification Scheme - Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.

6.1 Establish an Access Granting Process - Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.

6.2 Establish an Access Revoking Process - Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.

6.8 Define and Maintain Role-Based Access Control - Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.

16.1 Establish and Maintain a Secure Application Development Process - Establish and maintain a secure application development process. In the process, address such items as: secure application design standards, secure coding practices, developer training, vulnerability management, security of third-party code, and application security testing procedures. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.

16.2 Establish and Maintain a Process to Accept and Address Software Vulnerabilities - a means for external entities to report. The process is to include such items as: a vulnerability handling policy that identifies reporting process, responsible party for handling vulnerability reports, and a process for intake, assignment, remediation, and remediation testing. As part of the process, use a vulnerability tracking system that includes severity ratings, and metrics for measuring timing for identification, analysis, and remediation of vulnerabilities. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. Third-party application developers need to consider this an externally-facing policy that helps to set expectations for outside stakeholders.

16.3 Perform Root Cause Analysis on Security Vulnerabilities - Perform root cause analysis on security vulnerabilities. When reviewing vulnerabilities, root cause analysis is the task of evaluating underlying issues that create vulnerabilities in code, and allows development teams to move beyond just fixing individual vulnerabilities as they arise.

16.4 Establish and Manage an Inventory of Third-Party Software Components - Establish and manage an updated inventory of third-party components used in development, often referred to as a “bill of materials,” as well as components slated for future use. This inventory is to include any risks that each third-party component could pose. Evaluate the list at least monthly to identify any changes or updates to these components, and validate that the component is still supported.

16.5 Use Up-to-Date and Trusted Third-Party Software Components - Use up-to-date and trusted third-party software components. When possible, choose established and proven frameworks and libraries that provide adequate security. Acquire these components from trusted sources or evaluate the software for vulnerabilities before use.

16.6 Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities - Establish and maintain a severity rating system and process for application vulnerabilities that facilitates prioritizing the order in which discovered vulnerabilities are fixed. This process includes setting a minimum level of security acceptability for releasing code or applications. Severity ratings bring a systematic way of triaging vulnerabilities that improves risk management and helps ensure the most severe bugs are fixed first. Review and update the system and process annually.

16.7 Use Standard Hardening Configuration Templates for Application Infrastructure - Use standard, industry-recommended hardening configuration templates for application infrastructure components. This includes underlying servers, databases, and web servers, and applies to cloud containers, Platform as a Service (PaaS) components, and SaaS components. Do not allow in-house developed software to weaken configuration hardening.

16.8 Separate Production and Non-Production Systems - Maintain separate environments for production and non-production systems.

16.9 Train Developers in Application Security Concepts and Secure Coding - Ensure that all software development personnel receive training in writing secure code for their specific development environment and responsibilities. Training can include general security principles and application security standard practices. Conduct training at least annually and design in a way to promote security within the development team, and build a culture of security among the developers.

16.10 Apply Secure Design Principles in Application Architectures - Apply secure design principles in application architectures. Secure design principles include the concept of least privilege and enforcing mediation to validate every operation that the user makes, promoting the concept of “never trust user input.” Examples include ensuring that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Secure design also means minimizing the application infrastructure attack surface, such as turning off unprotected ports and services, removing unnecessary programs and files, and renaming or removing default accounts.

16.11 Leverage Vetted Modules or Services for Application - Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers’ workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.

16.12 Implement Code-Level Security Checks - Apply static and dynamic analysis tools within the application life cycle to verify that secure coding practices are being followed.

16.13 Conduct Application Penetration Testing - Conduct application penetration testing. For critical applications, authenticated penetration testing is better suited to finding business logic vulnerabilities than code scanning and automated security testing. Penetration testing relies on the skill of the tester to manually manipulate an application as an authenticated and unauthenticated user.

16.14 Conduct Threat Modeling - Conduct threat modeling. Threat modeling is the process of identifying and addressing application security design flaws within a design, before code is created. It is conducted through specially trained individuals who evaluate the application design and gauge security risks for each entry point and access level. The goal is to map out the application, architecture, and infrastructure in a structured way to understand its weaknesses.

4 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 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 user profile (*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>

*4.1 (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
v8	3.7 Establish and Maintain a Data Classification Scheme Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

4.2 (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', 'QMQMQMADM', '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(<xxxxxxx>) OBJTYPE(*USRPRF) USER(<xxxxxxx>) AUT(*ALL)

- Note: Replace xxxxxx for OBJ(<xxxxxxx>) with the SYSTEM_OBJECT_NAME from the audit
- Replace xxxxxx for USER(<xxxxxxx>) 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
v8	3.7 Establish and Maintain a Data Classification Scheme Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

4.3 (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(<xxxxxx>) 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
v8	3.7 Establish and Maintain a Data Classification Scheme Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

4.4 (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:

Special authority is a type of authority a user can have to perform system functions, including all object authority, save system authority, job control authority, security administrator authority, spool control authority, service authority, and system configuration authority.

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://www.ibm.com/docs/en/i/7.5?topic=authority-monitoring-special-authorities>
5. 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 <u>Establish and Maintain an Inventory of Accounts</u> 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 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u> 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	6.8 <u>Define and Maintain Role-Based Access Control</u> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			

4.5 (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	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.			
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.			

4.6 (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 QPWDRLUES 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](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               | <b><u>4.7 Manage Default Accounts on Enterprise Assets and Software</u></b><br>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               | <b><u>5.2 Use Unique Passwords</u></b><br>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.                                                     |  |  |  |

## 4.7 (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 LASTUSED 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.			

4.8 (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.

Note: Service profiles may be set to a non-expiring password (*NOMAX) commensurate with your organization policy.

```
CHGUSRPRF USRPRF(<xxxxxx>) PWDEXPITV(*SYSVAL)
```

References:

1. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 <u>Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

4.9 (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 <u>Collect Command-Line Audit Logs</u> Collect command-line audit logs. Example implementations include collecting audit logs from PowerShell®, BASH™, and remote administrative terminals.			

4.10 (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) parameters.

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	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> 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	<u>5.2 Use Unique Passwords</u> 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.			

4.11 (L1) Group Profiles With Passwords (Automated) (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	<u>4.7 Manage Default Accounts on Enterprise Assets and Software</u> 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	<u>5.2 Use Unique Passwords</u> 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.			

4.12 (L1) Implement Multi-factor authentication (MFA) (Manual)

Profile Applicability:

- Level 1

Description:

Multi-factor authentication (MFA) is a layered approach to securing physical and logical access where a system requires a user to present a combination of two or more different authenticators to verify a user's identity for login. MFA increases security because even if one authenticator becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space or computer system.

MFA requires users to present two or more authentication factors at login to verify their identity before they are granted access using some combination of the following:

- Something you know: like a password or Personal Identification Number (PIN)
- Something you have: like a smart card, mobile token, or hardware token
- Some form of biometric factor (e.g., fingerprint, palm print, or voice recognition)

Rationale:

Adversaries are increasingly capable of guessing or harvesting passwords to gain illicit access. Password cracking techniques are becoming more sophisticated and high-powered computing is increasingly affordable. In addition, adversaries harvest credentials through phishing emails or by identifying passwords reused from other systems. MFA adds a strong protection against account takeover by greatly increasing the level of difficulty for adversaries. An effective MFA solution requires a unique account/password combination and should not include shared accounts or default passwords.

Audit:

IBM and third-party vendors provide MFA solutions for IBM i, and organizations often choose to buy and implement one of these solutions or develop an in-house MFA solution. The business should provide implementation details from the vendor or in-house solution to provide an adequate audit procedure.

Remediation:

Evaluate 3rd party MFA solutions available from various vendors or develop an in-house MFA solution.

References:

1. <https://www.linkedin.com/pulse/microsoft-phishing-bypassed-mfa-attacks-against-10000-moriah-hara>
2. <https://duo.com/blog/mfa-fatigue-what-is-it-how-to-respond>
3. <https://fidoalliance.org/>

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.			
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.			
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.			
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.			

5 System Configuration

The recommendations that follow detail the IBM i configuration settings.

5.1 Security System Values

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

5.1.1 Level 1

Corporate/Enterprise Environment (general use)

5.1.1.1 (L1) Set 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 recovery 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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.1 Establish and Maintain a Software Inventory</u> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.			
v8	<u>2.2 Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v8	<u>2.3 Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<u>2.4 Utilize Automated Software Inventory Tools</u> Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.			
v8	<u>2.5 Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.			
v8	<u>2.6 Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.			
v8	<u>2.7 Allowlist Authorized Scripts</u> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			

5.1.1.2 (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.			

5.1.1.3 (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.		●	●

5.1.1.4 (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 of 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-gaudendacn>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8 <u>Audit Log Management</u> Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.			
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●

5.1.1.5 (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
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			

5.1.1.6 (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 <u>Collect Audit Logs</u> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v8	8.5 <u>Collect Detailed Audit Logs</u> 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.			

5.1.1.7 (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.			

5.1.1.8 (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-gautocfg>

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.			

5.1.1.9 (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.			

5.1.1.10 (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 that 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.			

5.1.1.11 (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
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			

5.1.1.12 (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(QDSCJOBTV)

Remediation:

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

QDSCJOBTV

CHGSYSVAL SYSVAL(QDSCJOBTV) VALUE('30')

References:

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.1.1.13 (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
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.			

5.1.1.14 (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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10 Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.			

5.1.1.15 (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.			

5.1.1.16 (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 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.1.1.17 (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.			

5.1.1.18 (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 <u>Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> 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.			

5.1.1.19 (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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			

5.1.1.20 (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:

DPSYSVAL 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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			

5.1.1.21 (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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>14.3 Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.1.22 (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 service accounts may have their 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 number of days.

Audit:

DSPSYSVAL SYSVAL(QPWDEXPITV)

Remediation:

To establish the recommended configuration, set the following system value to "45":
QPWDEXPITV
CHGSYSVAL SYSVAL(QPWDEXPITV) VALUE('45')

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-expiration-interval-qpwdexpitv>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 Train Workforce Members on Authentication Best Practices Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.1.23 (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-gpwxpwrn>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>14.3 Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.1.24 (L1) Set Password Level (Automated)

Profile Applicability:

- Level 1

Description:

Determines the length of password that is supported as well as removing weak and deprecated NTLM passwords for Windows 95/98/ME clients from the system. User passwords with a length of 1-128 characters are supported and exclude the use of decryptable password hashes (NTLM) for older 16-bit clients. For systems running at QPWLVL 4, the OS uses a Password-based Key Derivation Function 2 (PBKDF2) with HMAC SHA512 (SHA-2 512 bit) encryption for the scheme.

Password level 4 is a one-way password encryption algorithm that provides improved password security over password level 2 or 3.

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:

At QPWLVL 4, all password level 0 and 1 passwords and all password level 2 and 3 passwords are cleared. If the user profile does not have a password that is usable at password level 4, the password will be *NONE after moving to QPWLVL 4.

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

Audit:

DSPSYSVAL SYSVAL(QPWLVL)

Remediation:

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

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-level-gpwwdlv/>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.1.1.25 (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:

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.

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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 <u>Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.1.26 (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 *DGTLMATAJC *DGTLMTFST *DGTLMTLST *LMTPRFNAME *MAXLEN10 *MINLEN8 *REQANY3 *SPCCHRLMTAJC *SPCCHRLMTFST *SPCCHRLMTLST')

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-rules-qpwdrules>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

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.			

5.1.1.27 (L1) Set 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.			

5.1.1.28 (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.			

5.1.1.29 (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
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.			

5.1.1.30 (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-grmtrsrvatr>

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.			

5.1.1.31 (L1) Set 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:

DPSYSVAL 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
v8	10 Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.			
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.			

5.1.1.32 (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 prevents the associated operations, and also disallows 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
v8	10 Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.			
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.			

5.1.1.33 (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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

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.			

5.1.1.34 (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 the system's 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.			

5.1.1.35 (L1) Set 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:

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=srv-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
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.1.1.36 (L1) Set 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:

DPSYSVAL 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-qsslctl>
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
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.1.1.37 (L1) Set 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 protocol to the default list results in opening up all applications that use the default list to known security vulnerabilities.

The IBM i System Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocols and cipher suites are managed through the interconnect of the QSSLPCL, QSSLCSLCTL, and QSSLCSL system values, Digital Certificate Manager application definitions, and the SSLCONFIG/TLSCONFIG IBM i System Service Tools (SST) Advanced Analysis (AA) Command. When configuring your IBM i System SSL/TLS protocols and cipher suites, it is not always required to change your existing configuration. In some cases, only your SSL/TLS protocol configuration needs to be changed. In reverse, some cases will only require you to change your SSL/TLS cipher suite configuration. IBM recommends you carefully consider your SSL/TLS protocol and cipher suite requirements before making any changes.

Audit:

DSPPSYVAL 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
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.1.1.38 (L1) Set 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 <u>Configure Data Access Control Lists</u> 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.			
v8	4 <u>Secure Configuration of Enterprise Assets and Software</u> Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).			

5.1.1.39 (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 <u>Configure Data Access Control Lists</u> 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.			

5.1.1.40 (L1) Set 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 QVIFYOBJRST system value is set to 3. If you change the value of QVIFYOBJRST, it is important to set the QVIFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

Audit:

DSPSYSVAL SYSVAL(QVIFYOBJRST)

Remediation:

To establish the recommended configuration, set the following system value to "3":

QVIFYOBJRST

CHGSYSVAL SYSVAL(QVIFYOBJRST) VALUE('3')

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=objects-qvfyobjrst-system-value>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

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.			

5.1.2 Level 2

High Security/Sensitive Data Environment (limited functionality)

5.1.2.1 (L2) Set 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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>2.1 Establish and Maintain a Software Inventory</u> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	●	●	●
v8	<u>2.2 Ensure Authorized Software is Currently Supported</u> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v8	<u>2.3 Address Unauthorized Software</u> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	<u>2.4 Utilize Automated Software Inventory Tools</u> Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		●	●
v8	<u>2.5 Allowlist Authorized Software</u> Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v8	<u>2.6 Allowlist Authorized Libraries</u> Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.		●	●
v8	<u>2.7 Allowlist Authorized Scripts</u> Use technical controls, such as digital signatures and version control, to ensure that only authorized scripts, such as specific .ps1, .py, etc., files, are allowed to execute. Block unauthorized scripts from executing. Reassess bi-annually, or more frequently.			●

5.1.2.2 (L2) Set 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
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.			

5.1.2.3 (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.		●	●

5.1.2.4 (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-gaudendacn>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8 <u>Audit Log Management</u> Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.			
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			

5.1.2.5 (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
v8	8.1 <u>Establish and Maintain an Audit Log Management Process</u> Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v8	8.3 <u>Ensure Adequate Audit Log Storage</u> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.			

5.1.2.6 (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.			

5.1.2.7 (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
v8	6.1 <u>Establish an Access Granting Process</u> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			

5.1.2.8 (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.			

5.1.2.9 (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(QDSCJOBTV)

Remediation:

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

QDSCJOBTV

CHGSYSVAL SYSVAL(QDSCJOBTV) VALUE('15')

References:

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

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.			

5.1.2.10 (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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10 Malware Defenses Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.			

5.1.2.11 (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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.1.2.12 (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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.1.2.13 (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.			

5.1.2.14 (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	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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.	●	●	●
v8	<u>12.8 Establish and Maintain Dedicated Computing Resources for All Administrative Work</u> 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.			●

5.1.2.15 (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 the user profile when the number of incorrect sign-on attempts for the user reaches the value in the QMAXSIGN system value. This also disables the device when the number of incorrect sign-on attempts for the device reaches the value in the QMAXSIGN system value, regardless of whether the incorrect sign-on attempts were from the same user. This helps to prevent unlimited attempts even when the user profile does not exist.

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	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			

5.1.2.16 (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
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.			

5.1.2.17 (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-qpwdchgbk>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>14.3 Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.2.18 (L2) Set Password Expiration Interval (Automated)

Profile Applicability:

- Level 2

Description:

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

Numerous studies had found that excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. Instead, longer passphrases that do not expire frequently promote better composition, strength, and create better secrets that are harder to crack.

Immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization

NOTE: Longer password expiry intervals should only be implemented in conjunction with a longer password/passphrase minimum length of 14 characters. See (L2) Set Password Level (QPWDLVL) and (L2) Set Password Rules (QPWDRULES) for additional information.

Rationale:

This helps to prevent access to unauthorized persons by promoting longer passphrases that are more difficult to crack.

Audit:

DSPSYSVAL SYSVAL(QPWDEXPITV)

Remediation:

To establish the recommended configuration, set the following system value to "365":
QPWDEXPITV

CHGSYSVAL SYSVAL(QPWDEXPITV) VALUE('365')

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=passwords-block-password-change-gpwdchgbk>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>
3. <https://pages.nist.gov/800-63-3/sp800-63b.html>
4. <https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 Train Workforce Members on Authentication Best Practices Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.2.19 (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-gpwdrqddif>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 Train Workforce Members on Authentication Best Practices Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.1.2.20 (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 *LMTPRFNAME *MAXLEN128 *MINLEN14 *REQANY3')

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=passwords-password-rules-qpwdrules>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

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.			

5.1.2.21 (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)
- Ensure that the value specified the name of a Password Validation Program or *REGFAC.

Remediation:

To establish the recommended configuration, create a password validation program and set the following system value to either a value of the name of your program and library or *REGFAC:

QPWDVLDPGM

CHGSYSVAL SYSVAL(QPWDVLDPGM) VALUE(<pgmxxx libxxx>)

Note that if using a value of *REGFAC, you must also register the program to the QIBM_QSY_VLD_PASSWORD exit point, format VLDP0200.

ADDEXITPGM EXITPNT(QIBM_QSY_VLD_PASSWORD) FORMAT(VLDP0200)

PGMNBR(*HIGH) PGM(<libxxx/pgmxxx>)

See the References for additional information.

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
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.			

5.1.2.22 (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
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.			

5.1.2.23 (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>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

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.			

5.1.2.24 (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.			

5.1.2.25 (L2) Set 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 QVIFYOBJRST system value is set to 3. If you change the value of QVIFYOBJRST, it is important to set the QVIFYOBJRST value to 3 or lower before installing a new release of the IBM i operating system.

Audit:

DSPSYSVAL SYSVAL(QVIFYOBJRST)

Remediation:

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

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=values-verify-object-restore-qvfyobjrst>
2. <https://www.ibm.com/docs/en/i/7.5?topic=40-preventing-use-unsupported-interfaces>

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.			

5.2 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.

5.2.1 (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. This may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability of the entire system and/or critical components, which may result in serious consequences.

Impact:

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

Audit:

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

```
SELECT JOB_ACTION FROM QSYS2/NET_ATTR
```

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.			

5.2.2 (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. This may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability of the entire system and/or critical components, which may result in 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 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 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v8	5.2 <u>Use Unique Passwords</u> 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.			

5.2.3 (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.

Additionally, to encrypt sensitive data in transit, ensure that all *IP Type Relational Data Base Directory Entries specify Secure Connection (SECCNN) *SSL. See the following link for additional information:

<https://www.ibm.com/support/pages/ddm-drda-ssl-connectivity>

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. This may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability of the entire system and/or critical components, which may result in serious consequences.

Impact:

DDM/DRDA communications not using encrypted passwords 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  
  
CASE  
  
WHEN LAND(DBXRSEC,X'E0') = X'00' THEN '*USRID'  
  
WHEN LAND(DBXRSEC,X'E0') = X'20' THEN '*VLDONLY'  
  
WHEN LAND(DBXRSEC,X'E0') = X'40' THEN '*USRIDPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'C0' THEN '*USRENCPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'80' THEN '*ENCUSRPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'A0' THEN '*KERBEROS'  
  
ELSE '*UNKNOWN'  
  
END AS LOWAUT,  
  
CASE WHEN LAND(DBTFLGS,X'01') = X'01' THEN '*AES'  
  
ELSE '*DES' END AS LOWENC  
  
FROM QSYS/QADBXRDBD WHERE DBXRMTN = '*LOCAL'
```

- 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>
2. <https://www.ibm.com/support/pages/ddm-drda-ssl-connectivity>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v8	5.2 <u>Use Unique Passwords</u> 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.			

5.2.4 (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.

Additionally, to encrypt sensitive data in transit, ensure that all *IP Type Relational Data Base Directory Entries specify Secure Connection (SECCNN) *SSL. See the following link for additional information:

<https://www.ibm.com/support/pages/ddm-drda-ssl-connectivity>

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. This may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability of the entire system and/or critical components, which may result in serious consequences.

Impact:

DDM/DRDA communications not using encrypted passwords 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  
  
CASE  
  
WHEN LAND(DBXRSEC,X'E0') = X'00' THEN '*USRID'  
  
WHEN LAND(DBXRSEC,X'E0') = X'20' THEN '*VLDONLY'  
  
WHEN LAND(DBXRSEC,X'E0') = X'40' THEN '*USRIDPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'C0' THEN '*USRENCPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'80' THEN '*ENCUSRPWD'  
  
WHEN LAND(DBXRSEC,X'E0') = X'A0' THEN '*KERBEROS'  
  
ELSE '*UNKNOWN'  
  
END AS LOWAUT,  
  
CASE WHEN LAND(DBTFLGS,X'01') = X'01' THEN '*AES'  
  
ELSE '*DES' END AS LOWENC  
  
FROM QSYS/QADBXRDBD WHERE DBXRMTN = '*LOCAL'
```

- 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>
2. <https://www.ibm.com/support/pages/ddm-drda-ssl-connectivity>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			
v8	5.2 <u>Use Unique Passwords</u> 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.			

5.2.5 (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. This may include privilege escalation that can increase the scope of the attack and scale of access to impact the Confidentiality, Integrity, and Availability of the entire system and/or critical components, which may result in 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:

To change existing exports that allow anonymous access you can either modify the `/etc/exports` file or use the `CHGNFSEXP` command. Specify the `ANON=-1` option and any additional required options.

Example:

```
CHGNFSEXP '-O XX,ANON=-1' '/xxxxxx'
```

A sample entry in `/etc/exports` might look like: `/home/data -anon=-1`.

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/7.5.0?topic=ssw_ibm_i_75/cl/chgnfsexp.html
3. <https://www.tenable.com/plugins/nessus/11356>

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.			
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.			

5.2.6 (L2) NFS Shares (Automated)

Profile Applicability:

- Level 2

Description:

Disable NFS completely or 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:

To change existing exports to require NFSv4 and RPCSEC_GSS authentication with Kerberos you can either modify the /etc/exports file or use the CHGNFSEXP command. Specify VERS=4 and SEC=KRB5 and any additional required options.

Example:

```
CHGNFSEXP '-O XX,VERS=4,SEC=KRB5' '/xxxxxx'
```

A sample entry in /etc/exports might look like: /home/data -vers=4,sec=krb5.

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.ibm.com/docs/en/i/7.5.0?topic=ssw_ibm_i_75/cl/chgnfsexp.html
4. <https://www.tenable.com/plugins/nessus/11356>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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.			
v8	<u>5.2 Use Unique Passwords</u> 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.			
v8	<u>12.6 Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.2.7 (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 STRSQL and press Enter
- Copy or type the following SQL statement to the terminal and press Enter.

SELECT

T01.EXIT_NAME, T01.EXIT_FMT, T01.REGISTERED, T01.EXIT_PGMS,
T02.NUMBER, T02.LIBRARY, T02."PROGRAM", T02.TEXT

FROM QSYS2/EXIT_POINT T01 LEFT OUTER JOIN

QSYS2/EXIT_PGM T02

ON T01.EXIT_NAME = T02.EXIT_NAME

WHERE T01.EXIT_NAME LIKE 'QIBM_QTMF%'
OR T01.EXIT_NAME LIKE 'QIBM_QZRC_RMT%'
OR T01.EXIT_NAME LIKE 'QIBM_QMF_MESSAGE%'
OR T01.EXIT_NAME LIKE 'QIBM_QZDA%'
OR T01.EXIT_NAME LIKE 'QIBM_QZRC%'
OR T01.EXIT_NAME LIKE 'QIBM_QDB_OPEN%'
OR T01.EXIT_NAME LIKE 'QIBM_QDB_CLOSE%'
OR T01.EXIT_NAME LIKE 'QIBM_QZHQ_DATA_QUEUE%'
OR T01.EXIT_NAME LIKE 'QIBM_QJO_DLT_JRNRCV%'
OR T01.EXIT_NAME LIKE 'QIBM_QNPS_ENTRY%'
OR T01.EXIT_NAME LIKE 'QIBM_QNPS_SPLF%'
OR T01.EXIT_NAME LIKE 'QIBM_QPWFS_FILE_SERV%'
OR T01.EXIT_NAME LIKE 'QIBM_QPOL_SCAN_CLOSE%'
OR T01.EXIT_NAME LIKE 'QIBM_QPOL_SCAN_OPEN%'
OR T01.EXIT_NAME LIKE 'QIBM_QRQ_SQL%'
OR T01.EXIT_NAME LIKE 'QIBM_QSO_ACCEPT%'
OR T01.EXIT_NAME LIKE 'QIBM_QSO_CONNECT%'
OR T01.EXIT_NAME LIKE 'QIBM_QSO_LISTEN%'
OR T01.EXIT_NAME LIKE 'QIBM_QTF_TRANSFER%'
OR T01.EXIT_NAME LIKE 'QIBM_QTG_DEVINIT%'
OR T01.EXIT_NAME LIKE 'QIBM_QTG_DEVTERM%'
OR T01.EXIT_NAME LIKE 'QIBM_QTMX%'
OR T01.EXIT_NAME LIKE 'QIBM_QTOD_SERVER_REQ%'
OR T01.EXIT_NAME LIKE 'QIBM_QVP_PRINTERS%'
OR T01.EXIT_NAME LIKE 'QIBM_QWC_PWRDWNSYS%'
OR T01.EXIT_NAME LIKE 'QIBM_QZSC%'
OR T01.EXIT_NAME LIKE 'QIBM_QZSO_SIGNONSRV%'

Ensure that the number of "Exit Programs" is greater than 0 and that the "Exit Program Number", "Exit Program Library" and "Exit Program" properly displays your requirements to secure your Exit Points.

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
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.			
v8	13 Network Monitoring and Defense Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.			

5.2.8 (L1) Function Usage (Automated)

Profile Applicability:

- Level 1

Description:

You need to set up security for every person who will be authorized to use your system. User security setup involves installing application libraries and setting up user groups and profiles.

Several tasks are necessary to set up user security on your system by using the command line interface. Setting up Function Usage security is one of the steps involved in setting up user security.

The Work with Function Usage (WRKFCNUSG) command shows a list of function identifiers and allows you to change or display specified functions that determine whether a user can use the function if they or one of their groups do not have a specific usage setting.

The system administrator specifies who is allowed or denied access to a function.

You should allow only authorized users access to network and required functions and limit administrators in accordance with the Principle of Least Privilege (PoLP).

Rationale:

Limiting users access to security related functions provides an additional layer of defense. Access to powerful administrative functions should be limited in accordance with the Principle of Least Privilege (PoLP).

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 FCNID, DFTUSG FROM QSYS2/FCN_INFO WHERE FCNID IN  
( 'QIBM_ACCESS_ALLOBJ_JOBLOG', 'QIBM_ACCESS_ALLOBJ_JOBLOG',  
'QIBM_ACS_HTTP_PROXY', 'QIBM_ACS_HTTP_PROXY_OSPM',  
'QIBM_ALLOBJ_TRACE_ANY_USER', 'QIBM_DB_DDMDRDA', 'QIBM_DB_ZDA',  
'QIBM_DB_SECADM', 'QIBM_DB_SQLADM', 'QIBM_DB_SYSMON',  
'QIBM_DIRSRV_ADMIN', 'QIBM_ENVVAR_SYS', 'QIBM_LIST_ALL_OBJS',  
'QIBM_LIST_ALL_OBJS_SQL', 'QIBM_QSY_SYSTEM_CERT_STORE',  
'QIBM_QYAS_SERVICE_DISKMGMT', 'QIBM_SERVICE_DISK_WATCHER',  
'QIBM_SERVICE_DUMP', 'QIBM_SERVICE_JOB_WATCHER',  
'QIBM_SERVICE_THREAD', 'QIBM_SERVICE_TRACE', 'QIBM_SERVICE_WATCH',  
'QIBM_WATCH_ANY_JOB', 'QIBM_DB2_MIRROR') AND DFTUSG <> 'DENIED'  
ORDER BY FCNID ASC
```

- Ensure that the results do not return any functions with a DFTUSG setting ALLOWED.

Remediation:

Set all functions in the audit procedure to a default usage of DENIED and authorize specific administrative users/groups in accordance with the Principle of Least Privilege (PoLP) using the CHGFCNUSG command as in the following example.

```
CHGFCNUSG FCNID(QIBM_XXXXXX_XXXXXX) DEFAULT(*DENIED).
```

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=strategy-setting-up-user-security>
2. <https://www.ibm.com/docs/en/i/7.5?topic=security-function-usage>
3. <https://www.ibm.com/docs/en/i/7.5?topic=commands-function-usage-information>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 <u>Establish and Maintain a Secure Configuration Process</u> 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.			
v8	13 <u>Network Monitoring and Defense</u> Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.			

5.2.9 (L1) Intrusion Detection (Manual)

Profile Applicability:

- Level 1

Description:

The intrusion detection and prevention system (IDS) notifies you of attempts to hack into, disrupt, or deny service to the system. IDS also monitors for potential extrusions, where your system might be used as the source of the attack. These potential intrusions and extrusions are logged as intrusion monitor audit records in the security audit journal and displayed as intrusion events in the Intrusion Detection System graphical user interface (GUI). You can configure IDS to prevent intrusions and extrusions from occurring.

Rationale:

Most intrusions follow a pattern of information gathering, attempted access, and then destructive attacks. Some attacks can be detected and neutralized by the target system. Other attacks cannot be effectively neutralized by the target system. Most of the attacks also make use of spoofed packets, which are not easily traceable to their true origin. Many attacks make use of unwitting accomplices, which are machines or networks that are used without authorization to hide the identity of the attacker. For these reasons, a vital part of intrusion detection is gathering information, and detecting and preventing system attacks.

Audit:

Review IBM i Intrusion Detection Policies with your network security team and ensure that Intrusion Detection Policies are configured per your specific requirements.

Remediation:

To establish the recommended configuration, review Intrusion Detection in the IBM i Knowledge Center and Configure Intrusion Detection per your specific requirements.

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=security-intrusion-detection>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.2 <u>Deploy a Host-Based Intrusion Detection Solution</u> Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.			

5.2.10 (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/docs/en/i/7.5?topic=server-securing-telnet-tls>
2. https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_75/rzamv/rzamvtpsockets.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

5.2.11 (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=ftp-scenario-securing-ssl>
2. https://www.ibm.com/support/knowledgecenter/en/ssw_ibm_i_75/rzamv/rzamvtpsockets.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 <u>Encrypt Sensitive Data in Transit</u> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v8	4.6 <u>Securely Manage Enterprise Assets and Software</u> Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

5.2.12 (L1) SMTP Mail Relay (Manual)

Profile Applicability:

- Level 1

Description:

Simple Mail Transfer Protocol (SMTP) is the protocol that allows the operating system to send and receive e-mail. SMTP on the IBM i operating system supports the distribution of notes, messages, and ASCII text documents.

An SMTP relay is a process of transferring an email from one server to another which if improperly configured can allow unauthenticated relay of email commonly used in Spam and Malware delivery.

Rationale:

Spammers can connect to the server and forge sender information to send spam to legitimate users. The business may suffer financial as well as reputational loss through the use of a mail relay used to send spam.

Impact:

All SMTP mail relay communications may be impacted.

Audit:

- Type command CHGSMTPA and press F4 and then press F9 to display all parameters.
- Page down one time and ensure that Allowed relayed mail is set to a value of *NONE.
- Page down again and ensure that Allow authentication is not set to a value of *RELAY or *LCLRLY.

Remediation:

To establish the recommended configuration, disable mail relay for SMTP:
CHGSMTPA ALWRLY(*NONE) ALWAUTH(*NONE)

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=concepts-smtp-i>
2. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/chgsmtpa.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>9.7 Deploy and Maintain Email Server Anti-Malware Protections</u> Deploy and maintain email server anti-malware protections, such as attachment scanning and/or sandboxing.			

5.2.13 (L1) SNMP Access (Manual)

Profile Applicability:

- Level 1

Description:

SNMPv3 allows SNMP access based on the configuration of SNMPv3 users. These users are not the same as an IBM i user profile. The authentication and privacy protocols used by SNMPv3 provide enhanced security over SNMPv1.

Rationale:

SNMPv3 is highly recommended because it provides enhanced security over SNMPv1. An SNMPv1 community name is not encrypted, and is therefore vulnerable to packet sniffing.

Impact:

All SNMPv1 communications may be impacted.

Audit:

- Type command CHGSNMPA and press F4.
- Page down several times and ensure that Allow SNMPv3 support is set to a value of *V3ONLY.

Remediation:

To establish the recommended configuration, change SNMP to use *V3ONLY only:
CHGSNMPA ALWSNMPV3(*V3ONLY)

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=snmp-controlling-access>
2. https://www.stigviewer.com/stig/layer_2_switch_-_cisco/2019-01-09/finding/V-3196

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.			

5.3 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](#).

5.3.1 (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 ADDLIBL 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 ADDLIBL 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.			

5.3.2 (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
v8	<u>12.6 Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.3.3 (L1) IBM i SMB Signing (Automated)

Profile Applicability:

- Level 1

Description:

SMB signing (also known as security signatures) is a security mechanism in the SMB protocol. This setting requires clients connecting to the IBM i NetServer to sign requests for more secure communications.

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

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=netserver-i-security>
2. <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.			
v8	12.6 Use of Secure Network Management and Communication Protocols Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.3.4 (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 than 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 restarting 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 7.5:

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
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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.			
v8	<u>12.6 Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.3.5 (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).

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/ransomware 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.

Additionally, the QPWFSEVER is an authorization list (object type *AUTL) that provides additional access requirements for all objects in the QSYS.LIB file system being accessed through remote clients.

The default authority to this object is PUBLIC *USE authority. The administrator can use the EDTAUTL (Edit Authorization List) or WRKAUTL (Work With Authorization List) commands to change the value of this authority. The administrator can assign PUBLIC *EXCLUDE authority to the authorization list so that the *PUBLIC cannot access QSYS.LIB objects from remote clients.

Impact:

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

Audit:

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

```
SELECT SHARE, SHARE_TYPE, TEXT, ENCRYPTION, CAST(PATH_NAME AS  
VARCHAR(500)) AS PATH_NAME, PERMISSION, MAX_CONN, CUR_CONN FROM  
QSYS2/SHARE_INFO WHERE SHARE_TYPE = 'FILE'
```

Pay careful attention to ensure that no share allows access to the root (path /)

- Next run the following SQL

```
SELECT AUTL, USER_NAME, OBJ_AUTH FROM QSYS2/AUTL_USERS WHERE  
AUTL = 'QPWFSESERVER' AND USER_NAME = '*PUBLIC'
```

- Ensure that the *PUBLIC authority to the QPWFSESERVER authorization list is set to *EXCLUDE

Remediation:

To establish the recommended configuration, do the following:

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

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=qsyslib-qpwfserver-authorization-list-in-file-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.			
v8	13 Network Monitoring and Defense Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.			

5.3.6 (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 ADDLIB 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 ADDLIB 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/rzahlhide_netserver.htm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>4.1 Establish and Maintain a Secure Configuration Process</u> 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.			
v8	<u>13 Network Monitoring and Defense</u> Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.			

5.3.7 (L1) Malware Defenses (Manual)

Profile Applicability:

- Level 1

Description:

The Integrated File System (IFS) is a part of the IBM i operating system. It supports stream input/output and storage management similar to personal computer and UNIX operating systems. An infected file that is copied, moved, or saved from a PC to the IFS and then redistributed to another PC can transmit a virus to the new PC. Likewise, if a network drive is mapped to the IFS, a virus running on a PC (and which is capable of damaging files on a network drive) can damage any file stored on the IFS.

Rationale:

IBM i Scanning Support and 3rd party anti-virus products may provide some protection for the IFS. To ensure objects on the IFS are not infected, all clients susceptible to viruses, malware, spyware, ransomware, etc, should run advanced Machine Learning security suite program that monitor for unauthorized activity and behavior, and quarantines infected objects on the PC, thus preventing the spread of infected objects to IBM i server. While even the best Machine Learning Endpoint Detection and Response system may not provide 100% protection against Advanced Persistent Threats including Polymorphic and Metamorphic malware and Ransomware as a Service, signature based anti-virus are far less capable of protecting against advanced malware and ransomware threats.

Audit:

Evaluate your system requirements and ensure that any installed anti-virus product is updated and meets your organization's requirements.

Remediation:

Evaluate Scanning Options and 3rd party anti-virus products to adequately protect your system. See information on NetServer Shares for more information. Additionally, review information on system values QSCANFS and QSCANFSCTL

References:

1. <https://www.ibm.com/support/pages/viruses-malware-spyware-ransomware-ibm-i-operating-system-and-integrated-file-system>
2. <https://www.ibm.com/docs/en/i/7.5?topic=concepts-scanning-support>
3. <https://www.wired.com/story/artificial-intelligence-hacking-bruce-schneier/>
4. <https://securityintelligence.com/deeplocker-how-ai-can-power-a-stealthy-new-breed-of-malware/>
5. <https://securityintelligence.com/news/is-antivirus-protection-still-relevant/>
6. <https://www.spiceworks.com/it-security/cyber-risk-management/articles/antimalware-solutions/>
7. <https://www.hhs.gov/sites/default/files/ai-for-malware-development-analyst-note.pdf>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.			
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.			

5.4 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/

5.4.1 (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, including 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
v8	12.6 <u>Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.4.2 (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.			

5.4.3 (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
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.			

5.4.4 (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.			

5.4.5 (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
v8	4.3 <u>Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.4.6 (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	<u>4.3 Configure Automatic Session Locking on Enterprise Assets</u> 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.			

5.4.7 (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 (CBC) 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
v8	<u>12.6 Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.4.8 (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 one 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. Use specific, unique accounts and avoid the use of wildcard characters such as *.

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:

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=syntax-searching-special-characters>

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.			

5.5 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.

5.5.1 (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_SYSTST, GRP_TITLE  
FROM SYSTOOLS/GRPPTFCUR T01  
WHERE GRP_ID IN ('SF99958', 'SF99955', 'SF99952', 'SF99959')
```

- The following 4 PTF Groups should show that the INSTALLED LEVEL IS CURRENT.
- SF99958 750 Group Security
- SF99955 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>
2. <https://www.ibm.com/support/pages/ibm-i-group-ptfs-level>
3. https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/wrkptfgrp.html

Additional Information:

If your IBM i system/s do not have internet access, you can use the WRKPTFGRP command to display the installed level for the above PTF groups and compare it to the IBM i Preventative Service Planning information available at the following link.

IBM PSP

<https://www.ibm.com/support/pages/ibm-i-group-ptfs-level>

WRKPTFGRP

https://www.ibm.com/docs/en/i/7.5?topic=ssw_ibm_i_75/cl/wrkptfgrp.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>7.3 Perform Automated Operating System Patch Management</u> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			

5.6 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, 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.

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

Profile Applicability:

- Level 1

Description:

Numerous studies had found that excessive password expiration requirements do more harm than good, because these requirements make users select predictable passwords, composed of sequential words and numbers that are closely related to each other. Instead, longer passphrases that do not expire frequently promote better composition, strength, and create better secrets that are harder to crack.

Immediate password changes should be based on key events including, but not limited to:

- Indication of compromise
- Change of user roles
- When a user leaves the organization

NOTE: Longer password expiry intervals should only be implemented in conjunction with a longer password/passphrase minimum length of 14 characters.

Rationale:

This helps to prevent access to unauthorized persons by promoting longer passphrases that are more difficult to crack.

Audit:

On a command line type DSPSSTSECA and press ENTER
Verify that the Service tools password expiration interval is 365.

Remediation:

To change the default password expiration interval from 180 days, follow these steps.
CHGSSTSECA REQUSRID(<xxxxxx>) REQPWD(<xxxxxx>) PWDEXPITV(365)

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=policies-changing-service-tools-system-password-expiration-interval>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	14.3 <u>Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.6.2 (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: 5

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 5

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(5)

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=policies-changing-maximum-failed-sign-attempts>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>14.3 Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

5.6.3 (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>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>14.3 Train Workforce Members on Authentication Best Practices</u> Train workforce members on authentication best practices. Example topics include MFA, password composition, and credential management.			

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

Profile Applicability:

- Level 1

Description:

This policy setting determines the password level for System Service Tools. SST Password level 3 includes password-based Key Derivation Function 2 (PBKDF2) with HMAC SHA512 (SHA-2 512 bit) encryption

The recommended state for this setting is: PWLVL 3

Rationale:

The default password level (PWLVL 2) uses deprecated SHA encryption. To change to use HMAC SHA512 encryption, the System Service Tools Password Level should be set to PWLVL 3 for better security.

Audit:

- On a command line type DSPSSTSECA and press ENTER
- Verify that the Service tools password level is 3

Remediation:

To change the service tools password level.

CHGSSTSECA REQUSRID(<xxxxxx>) REQPWD(<xxxxxx>) SSTPWDLVL(3)

References:

1. <https://www.ibm.com/docs/en/i/7.5?topic=concepts-password-policies-service-tools-user-ids>
2. <https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide>

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<u>12.6 Use of Secure Network Management and Communication Protocols</u> Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater).			

5.6.5 (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.			

5.6.6 (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:
 - QSECOFR
 - QSRV

Audit:

1. Type DSPSSTUSR and press Enter.
2. Review the screen output information with your system administrator and ensure that all SST users have unique profiles. Do not use the shipped IBM User IDs.
3. Ensure that all Service Tools IDs have the proper functional privileges for their job roles.

Remediation:

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

Ensure that each unique SST ID has privileges commensurate with the Principle of Least Privilege for each unique job role.

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.			

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

Profile Applicability:

- Level 1

Description:

This policy setting determines if 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 REQUSTRID(<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.			

5.6.8 (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 14
 4. Maximum password length is 128
 5. Use characters from three groups is *YES
 6. Minimum digits is 1
 7. Limit adjacent digits is *NO
 8. Limit digit first position is *NO
 9. Limit digit last position is *NO
 10. Limit adjacent special characters is *NO
 11. Limit special character first position is *NO
 12. Limit special character last position is *NO

Remediation:

To establish the recommended configuration, set SST Password Rules with the following command:

```
CHGSSTSECA PWDRULES(*YES 24 14 128 *YES *NO *NO *NO 1 *NOMAX *NO *NO *NO *NONE *NOMAX *NO *NO *NO *NONE *NONE *NOMAX *NO *NO *NO)
```

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.			

5.6.9 (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
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.			

6 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.

6.1 (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.			

6.2 (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(<XXXXXXX>) GRPPRF(<XXXXXXX>)

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.			

7 Auditing and Monitoring

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.

Forwarding all important logs to analytical programs, such as Security Information and Event Management (SIEM) solutions, can provide value; however, they do not provide a complete picture. Weekly log reviews are necessary to tune thresholds and identify abnormal events. Correlation tools can make audit logs more useful for subsequent manual inspection. These tools are not a replacement for skilled information security personnel and system administrators. Even with automated log analysis tools, human expertise and intuition are often required to identify and understand attacks.

Turning Down the Noise: Adding Context to the SIEM With Modern Data Security

SIEMs are a security landfill without context. If every event is sent over without context attached — the who, what, where and when becomes useless. For example, what is the difference between authorized access to a critical IBM i resource (*LIB, *FILE, *USRPRF) vs. improper access.

<https://securityintelligence.com/posts/adding-context-siem-modern-data-security/>

<https://securityintelligence.com/articles/alert-fatigue-a-911-cyber-call-center-that-never-sleeps/>

CIS Controls:

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.

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.

13.1 Centralize Security Event Alerting Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard.

8 Penetration Testing

A successful defensive posture requires a comprehensive program of effective policies and governance, strong technical defenses, combined with appropriate action from people. However, it is rarely perfect. In a complex environment where technology is constantly evolving and new attacker tradecraft appears regularly, enterprises should periodically test their controls to identify gaps and to assess their resiliency. This test may be from external network, internal network, application, system, or device perspective. It may include social engineering of users, or physical access control bypasses. Often, penetration tests are performed for specific purposes:

- As a “dramatic” demonstration of an attack, usually to convince decision-makers of their enterprise’s weaknesses
- As a means to test the correct operation of enterprise defenses (“verification”)
- To test that the enterprise has built the right defenses in the first place (“validation”) Independent penetration testing can provide valuable and objective insights about the existence of vulnerabilities in enterprise assets and humans, and the efficacy of defenses and mitigating controls to protect against adverse impacts to the enterprise. They are part of a comprehensive, ongoing program of security management and improvement. They can also reveal process weaknesses, such as incomplete or inconsistent configuration management, or end-user training. Penetration testing differs from vulnerability testing, described in CIS Control 7. Vulnerability testing checks for presence of known, insecure enterprise assets, and stops there. Penetration testing goes further to exploit those weaknesses to see how far an attacker could get, and what business process or data might be impacted through exploitation of that vulnerability. This is an important detail, and often penetration testing and vulnerability testing are incorrectly used interchangeably. Vulnerability testing is exclusively automated scanning with sometimes manual validation of false positives, whereas penetration testing requires more human involvement and analysis, sometimes supported through the use of custom tools or scripts. However, vulnerability testing is often a starting point for a penetration test. Another common term is “Red Team” exercises. These are similar to penetration tests in that vulnerabilities are exploited; however, the difference is the focus. Red Teams simulate specific attacker TTPs to evaluate how an enterprise’s environment would withstand an attack from a specific adversary, or category of adversaries. There are three types of penetration tests: Black-box, Grey-box or White-box testing.
- Black-box testing: Testing performed without prior knowledge of the internal structure/design/implementation of the object being tested.
- Grey-box testing: Testing performed with partial knowledge of the internal structure/design/implementation of the object being tested.

- **White-box testing:** Testing performed with knowledge of the internal structure/design/implementation of the object being tested. Most penetration tests are typically performed as either white-box or grey-box assessments. These types of assessments yield more accurate results and provide a more comprehensive test of the security posture of the environment than a pure black-box assessment.

CIS Controls:

18.1 Establish and Maintain a Penetration Testing Program Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

18.2 Perform Periodic External Penetration Tests Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

18.5 Establish and Maintain a Penetration Testing Program Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.

9 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.

10 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.

Disk Encryption

Disk encryption allows you to encrypt data that is stored in basic disk pools and independent disk pools.

Disk encryption protects data from a number of different threats:

- Protects data transmission to and from the disk drive (important in a SAN environment).
- Protects data transmission in the cross site mirroring environment (only when the data being mirrored is on an encrypted independent disk pool).
- Protects data in the case of theft of the disk drive.

To use disk encryption, you must have 5770-SS1 Option 45 - Encrypted ASP Enablement installed. The option to enable encryption is available when you create a disk pool or independent disk pool.

<https://www.ibm.com/docs/en/i/7.5?topic=management-disk-encryption>

CIS Controls:

3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.

11 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.

12 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	Introduction to IBM i Security		
2	Adopted Authority		
3	Resource Security		
4	User Profiles		
4.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority) (Automated)	☐	☐
4.2	(L1) User Profile (*USRPRF) Access Controls (Private authority) (Automated)	☐	☐
4.3	(L1) User Profile (*USRPRF) Object Ownership (Automated)	☐	☐
4.4	(L1) Administrative Special Authorities (Automated)	☐	☐
4.5	(L1) User Profile Action Auditing (Automated)	☐	☐
4.6	(L1) Default Passwords (Automated)	☐	☐
4.7	(L1) Inactive Profiles (Automated)	☐	☐
4.8	(L1) User Profile With Non-Expiring Passwords (Automated)	☐	☐
4.9	(L1) User Profiles With Command Line Access (Automated)	☐	☐
4.10	(L1) IBM Supplied User Profiles (Automated)	☐	☐
4.11	(L1) Group Profiles With Passwords (Automated) (Automated)	☐	☐
4.12	(L1) Implement Multi-factor authentication (MFA) (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5	System Configuration		
5.1	Security System Values		
5.1.1	Level 1		
5.1.1.1	(L1) Set Allow Restoration of Security-Sensitive Objects (Automated)	☐	☐
5.1.1.2	(L1) Set Attention Program (Automated)	☐	☐
5.1.1.3	(L1) Set Auditing Control (Automated)	☐	☐
5.1.1.4	(L1) Set Auditing End Action (Automated)	☐	☐
5.1.1.5	(L1) Set Auditing Force Level (Automated)	☐	☐
5.1.1.6	(L1) Set Auditing Level (Automated)	☐	☐
5.1.1.7	(L1) Set Security Auditing Level Extensions (Automated)	☐	☐
5.1.1.8	(L1) Set Automatic Device Configuration (Automated)	☐	☐
5.1.1.9	(L1) Set Automatic Remote Controller Configuration (Automated)	☐	☐
5.1.1.10	(L1) Set Automatic Virtual Device Creation (Automated)	☐	☐
5.1.1.11	(L1) Set Create Authority (Automated)	☐	☐
5.1.1.12	(L1) Set Disconnect-Job Interval (Automated)	☐	☐
5.1.1.13	(L1) Set Display User Sign-on Information (Automated)	☐	☐
5.1.1.14	(L1) Set Force Conversion On Restore (Automated)	☐	☐
5.1.1.15	(L1) Set Inactivity Time-out Interval (Automated)	☐	☐
5.1.1.16	(L1) Set Inactivity Message Queue (Automated)	☐	☐
5.1.1.17	(L1) Set Limit Device Sessions (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.1.18	(L1) Set Limit Security Officer Access to Workstations (Automated)	☐	☐
5.1.1.19	(L1) Set Maximum Sign-on Action (Automated)	☐	☐
5.1.1.20	(L1) Set Maximum Sign-on Attempts (Automated)	☐	☐
5.1.1.21	(L1) Set Block Password Change (Automated)	☐	☐
5.1.1.22	(L1) Set Password Expiration Interval (Automated)	☐	☐
5.1.1.23	(L1) Set Password Expiration Warning (Automated)	☐	☐
5.1.1.24	(L1) Set Password Level (Automated)	☐	☐
5.1.1.25	(L1) Set Required Difference in Passwords (Automated)	☐	☐
5.1.1.26	(L1) Set Password Rules (Automated)	☐	☐
5.1.1.27	(L1) Set Retain Server Security (Automated)	☐	☐
5.1.1.28	(L1) Set Remote IPL (Automated)	☐	☐
5.1.1.29	(L1) Set Remote Sign-on Value (Automated)	☐	☐
5.1.1.30	(L1) Set Remote Service Attribute (Automated)	☐	☐
5.1.1.31	(L1) Set Scan File System (Automated)	☐	☐
5.1.1.32	(L1) Set Scan File System Control (Automated)	☐	☐
5.1.1.33	(L1) Set System Security Level (Automated)	☐	☐
5.1.1.34	(L1) Set Shared Memory Control (Automated)	☐	☐
5.1.1.35	(L1) Set Secure Sockets Layer Cipher Specification List (Automated)	☐	☐
5.1.1.36	(L1) Set Secure Sockets Layer Cipher Control (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.1.37	(L1) Set Secure Socket Layer Security Protocols (Automated)	☐	☐
5.1.1.38	(L1) Set System Library List (Automated)	☐	☐
5.1.1.39	(L1) Set Use Adopted Authority (Automated)	☐	☐
5.1.1.40	(L1) Set Verify Object On Restore (Automated)	☐	☐
5.1.2	Level 2		
5.1.2.1	(L2) Set Allow Restoration of Security-Sensitive Objects (Automated)	☐	☐
5.1.2.2	(L2) Set Allow User Domain Objects in These Libraries (Automated)	☐	☐
5.1.2.3	(L2) Set Auditing Control (Automated)	☐	☐
5.1.2.4	(L2) Set Auditing End Action (Automated)	☐	☐
5.1.2.5	(L2) Set Auditing Force Level (Automated)	☐	☐
5.1.2.6	(L2) Set Automatic Virtual Device Creation (Automated)	☐	☐
5.1.2.7	(L2) Set Create Authority (Automated)	☐	☐
5.1.2.8	(L2) Set Create Object Audit Level (Automated)	☐	☐
5.1.2.9	(L2) Set Disconnect-Job Interval (Automated)	☐	☐
5.1.2.10	(L2) Set Force Conversion On Restore (Automated)	☐	☐
5.1.2.11	(L2) Set Inactivity Time-out Interval (Automated)	☐	☐
5.1.2.12	(L2) Set Inactivity Message Queue (Automated)	☐	☐
5.1.2.13	(L2) Set Limit Device Sessions (Automated)	☐	☐
5.1.2.14	(L2) Set Limit Security Officer Access to Workstations (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.1.2.15	(L2) Set Maximum Sign-on Action (Automated)	☐	☐
5.1.2.16	(L2) Set Maximum Sign-on Attempts (Automated)	☐	☐
5.1.2.17	(L2) Set Block Password Change (Automated)	☐	☐
5.1.2.18	(L2) Set Password Expiration Interval (Automated)	☐	☐
5.1.2.19	(L2) Set Required Difference in Passwords (Automated)	☐	☐
5.1.2.20	(L2) Set Password Rules (Automated)	☐	☐
5.1.2.21	(L2) Set Password Validation Program (Automated)	☐	☐
5.1.2.22	(L2) Set Remote Sign-on Value (Automated)	☐	☐
5.1.2.23	(L2) Set System Security Level (Automated)	☐	☐
5.1.2.24	(L2) Set Shared Memory Control (Automated)	☐	☐
5.1.2.25	(L2) Set Verify Object On Restore (Automated)	☐	☐
5.2	Network Services		
5.2.1	(L1) Network Attribute JOBACN (Network Job Action) (Automated)	☐	☐
5.2.2	(L1) DDM Remote Configuration List (SNA) Attributes (Automated)	☐	☐
5.2.3	(L1) DDM TCP/IP Attributes (Automated)	☐	☐
5.2.4	(L2) DDM TCP/IP Attributes (Automated)	☐	☐
5.2.5	(L1) NFS Shares (Automated)	☐	☐
5.2.6	(L2) NFS Shares (Automated)	☐	☐
5.2.7	(L1) Exit Points (Automated)	☐	☐
5.2.8	(L1) Function Usage (Automated)	☐	☐
5.2.9	(L1) Intrusion Detection (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.10	(L1) Telnet Protocol (Automated)	☐	☐
5.2.11	(L1) FTP Protocol (Automated)	☐	☐
5.2.12	(L1) SMTP Mail Relay (Manual)	☐	☐
5.2.13	(L1) SNMP Access (Manual)	☐	☐
5.3	IBM i NetServer security		
5.3.1	(L1) IBM i NetServer Guest Profile (Automated)	☐	☐
5.3.2	(L1) IBM i NetServer LANMAN Password Hash (Automated)	☐	☐
5.3.3	(L1) IBM i SMB Signing (Automated)	☐	☐
5.3.4	(L1) IBM i SMBv2 Server (Automated)	☐	☐
5.3.5	(L1) IBM i NetServer Shares (Automated)	☐	☐
5.3.6	(L2) NetServer Browse Interval (Automated)	☐	☐
5.3.7	(L1) Malware Defenses (Manual)	☐	☐
5.4	IBM i SSH Server security		
5.4.1	(L1) Configuring SSH – server protocol 2 (Automated)	☐	☐
5.4.2	(L1) Configuring SSH – banner configuration (Automated)	☐	☐
5.4.3	(L1) Configuring SSH – disallow host based authentication (Automated)	☐	☐
5.4.4	(L1) Configuring SSH – set privilege separation (Automated)	☐	☐
5.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less (Automated)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability: (Automated)	☐	☐
5.4.7	(L1) Configuring SSH – restrict Cipher list (Automated)	☐	☐
5.4.8	(L1) Configuring SSH – Limit Access Via SSH (Automated)	☐	☐
5.5	IBM i Patch Management		
5.5.1	(L1) IBM i Patch Management (Automated)	☐	☐
5.6	System Service Tools		
5.6.1	(L1) System Service Tools Password Expiration Interval (Automated)	☐	☐
5.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts (Automated)	☐	☐
5.6.3	(L1) System Service Tools Changing the duplicate password control (Automated)	☐	☐
5.6.4	(L1) System Service Tools Password Level (Automated)	☐	☐
5.6.5	(L1) System Service Tools Allow New Digital Certificates (Automated)	☐	☐
5.6.6	(L1) System Service Tools IDs and Privileges (Automated)	☐	☐
5.6.7	(L1) System Service Tools locking security-related system values (Automated)	☐	☐
5.6.8	(L1) System Service Tools Password Rules (Automated)	☐	☐
5.6.9	(L1) System Service Tools Allow add and remove of password exit programs (Automated)	☐	☐
6	QSECOFR Profile		

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.1	(L1) QSECOFR Profile Shall Be *DISABLED (Automated)	☐	☐
6.2	(L1) QSECOFR Shall Not be Configured as a Group Profile (Automated)	☐	☐
7	Auditing and Monitoring		
8	Penetration Testing		
9	Documentation		
10	Physical Security		
11	Disaster Recovery		
12	Licensed Program Installation Procedure		

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
4.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority)	☐	☐
4.2	(L1) User Profile (*USRPRF) Access Controls (Private authority)	☐	☐
4.3	(L1) User Profile (*USRPRF) Object Ownership	☐	☐
4.4	(L1) Administrative Special Authorities	☐	☐
4.5	(L1) User Profile Action Auditing	☐	☐
4.6	(L1) Default Passwords	☐	☐
4.7	(L1) Inactive Profiles	☐	☐
4.8	(L1) User Profile With Non-Expiring Passwords	☐	☐
4.10	(L1) IBM Supplied User Profiles	☐	☐
4.11	(L1) Group Profiles With Passwords (Automated)	☐	☐
4.12	(L1) Implement Multi-factor authentication (MFA)	☐	☐
5.1.1.1	(L1) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.1.2	(L1) Set Attention Program	☐	☐
5.1.1.3	(L1) Set Auditing Control	☐	☐
5.1.1.4	(L1) Set Auditing End Action	☐	☐
5.1.1.5	(L1) Set Auditing Force Level	☐	☐
5.1.1.6	(L1) Set Auditing Level	☐	☐
5.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
5.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
5.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
5.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
5.1.1.11	(L1) Set Create Authority	☐	☐
5.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
5.1.1.13	(L1) Set Display User Sign-on Information	☐	☐
5.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
5.1.1.17	(L1) Set Limit Device Sessions	☐	☐
5.1.1.21	(L1) Set Block Password Change	☐	☐
5.1.1.22	(L1) Set Password Expiration Interval	☐	☐
5.1.1.23	(L1) Set Password Expiration Warning	☐	☐
5.1.1.25	(L1) Set Required Difference in Passwords	☐	☐
5.1.1.26	(L1) Set Password Rules	☐	☐
5.1.1.27	(L1) Set Retain Server Security	☐	☐
5.1.1.28	(L1) Set Remote IPL	☐	☐
5.1.1.29	(L1) Set Remote Sign-on Value	☐	☐
5.1.1.30	(L1) Set Remote Service Attribute	☐	☐
5.1.1.31	(L1) Set Scan File System	☐	☐
5.1.1.32	(L1) Set Scan File System Control	☐	☐
5.1.1.33	(L1) Set System Security Level	☐	☐
5.1.1.34	(L1) Set Shared Memory Control	☐	☐
5.1.1.38	(L1) Set System Library List	☐	☐
5.1.1.39	(L1) Set Use Adopted Authority	☐	☐
5.1.1.40	(L1) Set Verify Object On Restore	☐	☐
5.1.2.1	(L2) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.2.2	(L2) Set Allow User Domain Objects in These Libraries	☐	☐
5.1.2.3	(L2) Set Auditing Control	☐	☐
5.1.2.4	(L2) Set Auditing End Action	☐	☐
5.1.2.5	(L2) Set Auditing Force Level	☐	☐
5.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
5.1.2.7	(L2) Set Create Authority	☐	☐
5.1.2.8	(L2) Set Create Object Audit Level	☐	☐
5.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
5.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
5.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
5.1.2.13	(L2) Set Limit Device Sessions	☐	☐
5.1.2.14	(L2) Set Limit Security Officer Access to Workstations	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.2.17	(L2) Set Block Password Change	☐	☐
5.1.2.18	(L2) Set Password Expiration Interval	☐	☐
5.1.2.19	(L2) Set Required Difference in Passwords	☐	☐
5.1.2.20	(L2) Set Password Rules	☐	☐
5.1.2.21	(L2) Set Password Validation Program	☐	☐
5.1.2.22	(L2) Set Remote Sign-on Value	☐	☐
5.1.2.23	(L2) Set System Security Level	☐	☐
5.1.2.24	(L2) Set Shared Memory Control	☐	☐
5.1.2.25	(L2) Set Verify Object On Restore	☐	☐
5.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
5.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
5.2.3	(L1) DDM TCP/IP Attributes	☐	☐
5.2.4	(L2) DDM TCP/IP Attributes	☐	☐
5.2.5	(L1) NFS Shares	☐	☐
5.2.6	(L2) NFS Shares	☐	☐
5.2.7	(L1) Exit Points	☐	☐
5.2.8	(L1) Function Usage	☐	☐
5.2.10	(L1) Telnet Protocol	☐	☐
5.2.11	(L1) FTP Protocol	☐	☐
5.2.13	(L1) SNMP Access	☐	☐
5.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
5.3.3	(L1) IBM i SMB Signing	☐	☐
5.3.4	(L1) IBM i SMBv2 Server	☐	☐
5.3.5	(L1) IBM i NetServer Shares	☐	☐
5.3.6	(L2) NetServer Browse Interval	☐	☐
5.3.7	(L1) Malware Defenses	☐	☐
5.4.2	(L1) Configuring SSH – banner configuration	☐	☐
5.4.3	(L1) Configuring SSH – disallow host based authentication	☐	☐
5.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
5.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
5.4.8	(L1) Configuring SSH – Limit Access Via SSH	☐	☐
5.5.1	(L1) IBM i Patch Management	☐	☐
5.6.1	(L1) System Service Tools Password Expiration Interval	☐	☐
5.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts	☐	☐
5.6.3	(L1) System Service Tools Changing the duplicate password control	☐	☐
5.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
5.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
5.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.6.8	(L1) System Service Tools Password Rules	☐	☐
5.6.9	(L1) System Service Tools Allow add and remove of password exit programs	☐	☐
6.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐
6.2	(L1) QSECOFR Shall Not be Configured as a Group Profile	☐	☐

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
4.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority)	☐	☐
4.2	(L1) User Profile (*USRPRF) Access Controls (Private authority)	☐	☐
4.3	(L1) User Profile (*USRPRF) Object Ownership	☐	☐
4.4	(L1) Administrative Special Authorities	☐	☐
4.5	(L1) User Profile Action Auditing	☐	☐
4.6	(L1) Default Passwords	☐	☐
4.7	(L1) Inactive Profiles	☐	☐
4.8	(L1) User Profile With Non-Expiring Passwords	☐	☐
4.9	(L1) User Profiles With Command Line Access	☐	☐
4.10	(L1) IBM Supplied User Profiles	☐	☐
4.11	(L1) Group Profiles With Passwords (Automated)	☐	☐
4.12	(L1) Implement Multi-factor authentication (MFA)	☐	☐
5.1.1.1	(L1) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.1.2	(L1) Set Attention Program	☐	☐
5.1.1.3	(L1) Set Auditing Control	☐	☐
5.1.1.4	(L1) Set Auditing End Action	☐	☐
5.1.1.5	(L1) Set Auditing Force Level	☐	☐
5.1.1.6	(L1) Set Auditing Level	☐	☐
5.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
5.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
5.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
5.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
5.1.1.11	(L1) Set Create Authority	☐	☐
5.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
5.1.1.13	(L1) Set Display User Sign-on Information	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
5.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
5.1.1.17	(L1) Set Limit Device Sessions	☐	☐
5.1.1.19	(L1) Set Maximum Sign-on Action	☐	☐
5.1.1.20	(L1) Set Maximum Sign-on Attempts	☐	☐
5.1.1.21	(L1) Set Block Password Change	☐	☐
5.1.1.22	(L1) Set Password Expiration Interval	☐	☐
5.1.1.23	(L1) Set Password Expiration Warning	☐	☐
5.1.1.24	(L1) Set Password Level	☐	☐
5.1.1.25	(L1) Set Required Difference in Passwords	☐	☐
5.1.1.26	(L1) Set Password Rules	☐	☐
5.1.1.27	(L1) Set Retain Server Security	☐	☐
5.1.1.28	(L1) Set Remote IPL	☐	☐
5.1.1.29	(L1) Set Remote Sign-on Value	☐	☐
5.1.1.30	(L1) Set Remote Service Attribute	☐	☐
5.1.1.31	(L1) Set Scan File System	☐	☐
5.1.1.32	(L1) Set Scan File System Control	☐	☐
5.1.1.33	(L1) Set System Security Level	☐	☐
5.1.1.34	(L1) Set Shared Memory Control	☐	☐
5.1.1.35	(L1) Set Secure Sockets Layer Cipher Specification List	☐	☐
5.1.1.36	(L1) Set Secure Sockets Layer Cipher Control	☐	☐
5.1.1.37	(L1) Set Secure Socket Layer Security Protocols	☐	☐
5.1.1.38	(L1) Set System Library List	☐	☐
5.1.1.39	(L1) Set Use Adopted Authority	☐	☐
5.1.1.40	(L1) Set Verify Object On Restore	☐	☐
5.1.2.1	(L2) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.2.2	(L2) Set Allow User Domain Objects in These Libraries	☐	☐
5.1.2.3	(L2) Set Auditing Control	☐	☐
5.1.2.4	(L2) Set Auditing End Action	☐	☐
5.1.2.5	(L2) Set Auditing Force Level	☐	☐
5.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.2.7	(L2) Set Create Authority	☐	☐
5.1.2.8	(L2) Set Create Object Audit Level	☐	☐
5.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
5.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
5.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
5.1.2.13	(L2) Set Limit Device Sessions	☐	☐
5.1.2.14	(L2) Set Limit Security Officer Access to Workstations	☐	☐
5.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
5.1.2.16	(L2) Set Maximum Sign-on Attempts	☐	☐
5.1.2.17	(L2) Set Block Password Change	☐	☐
5.1.2.18	(L2) Set Password Expiration Interval	☐	☐
5.1.2.19	(L2) Set Required Difference in Passwords	☐	☐
5.1.2.20	(L2) Set Password Rules	☐	☐
5.1.2.21	(L2) Set Password Validation Program	☐	☐
5.1.2.22	(L2) Set Remote Sign-on Value	☐	☐
5.1.2.23	(L2) Set System Security Level	☐	☐
5.1.2.24	(L2) Set Shared Memory Control	☐	☐
5.1.2.25	(L2) Set Verify Object On Restore	☐	☐
5.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
5.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
5.2.3	(L1) DDM TCP/IP Attributes	☐	☐
5.2.4	(L2) DDM TCP/IP Attributes	☐	☐
5.2.5	(L1) NFS Shares	☐	☐
5.2.6	(L2) NFS Shares	☐	☐
5.2.7	(L1) Exit Points	☐	☐
5.2.8	(L1) Function Usage	☐	☐
5.2.9	(L1) Intrusion Detection	☐	☐
5.2.10	(L1) Telnet Protocol	☐	☐
5.2.11	(L1) FTP Protocol	☐	☐
5.2.13	(L1) SNMP Access	☐	☐
5.3.1	(L1) IBM i NetServer Guest Profile	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.3.2	(L1) IBM i NetServer LANMAN Password Hash	☐	☐
5.3.3	(L1) IBM i SMB Signing	☐	☐
5.3.4	(L1) IBM i SMBv2 Server	☐	☐
5.3.5	(L1) IBM i NetServer Shares	☐	☐
5.3.6	(L2) NetServer Browse Interval	☐	☐
5.3.7	(L1) Malware Defenses	☐	☐
5.4.1	(L1) Configuring SSH – server protocol 2	☐	☐
5.4.2	(L1) Configuring SSH – banner configuration	☐	☐
5.4.3	(L1) Configuring SSH – disallow host based authentication	☐	☐
5.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
5.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less	☐	☐
5.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
5.4.7	(L1) Configuring SSH – restrict Cipher list	☐	☐
5.4.8	(L1) Configuring SSH – Limit Access Via SSH	☐	☐
5.5.1	(L1) IBM i Patch Management	☐	☐
5.6.1	(L1) System Service Tools Password Expiration Interval	☐	☐
5.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts	☐	☐
5.6.3	(L1) System Service Tools Changing the duplicate password control	☐	☐
5.6.4	(L1) System Service Tools Password Level	☐	☐
5.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
5.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
5.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.6.8	(L1) System Service Tools Password Rules	☐	☐
5.6.9	(L1) System Service Tools Allow add and remove of password exit programs	☐	☐
6.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐
6.2	(L1) QSECOFR Shall Not be Configured as a Group Profile	☐	☐

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
4.1	(L1) User Profile (*USRPRF) Access Controls (*PUBLIC authority)	☐	☐
4.2	(L1) User Profile (*USRPRF) Access Controls (Private authority)	☐	☐
4.3	(L1) User Profile (*USRPRF) Object Ownership	☐	☐
4.4	(L1) Administrative Special Authorities	☐	☐
4.5	(L1) User Profile Action Auditing	☐	☐
4.6	(L1) Default Passwords	☐	☐
4.7	(L1) Inactive Profiles	☐	☐
4.8	(L1) User Profile With Non-Expiring Passwords	☐	☐
4.9	(L1) User Profiles With Command Line Access	☐	☐
4.10	(L1) IBM Supplied User Profiles	☐	☐
4.11	(L1) Group Profiles With Passwords (Automated)	☐	☐
4.12	(L1) Implement Multi-factor authentication (MFA)	☐	☐
5.1.1.1	(L1) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.1.2	(L1) Set Attention Program	☐	☐
5.1.1.3	(L1) Set Auditing Control	☐	☐
5.1.1.4	(L1) Set Auditing End Action	☐	☐
5.1.1.5	(L1) Set Auditing Force Level	☐	☐
5.1.1.6	(L1) Set Auditing Level	☐	☐
5.1.1.7	(L1) Set Security Auditing Level Extensions	☐	☐
5.1.1.8	(L1) Set Automatic Device Configuration	☐	☐
5.1.1.9	(L1) Set Automatic Remote Controller Configuration	☐	☐
5.1.1.10	(L1) Set Automatic Virtual Device Creation	☐	☐
5.1.1.11	(L1) Set Create Authority	☐	☐
5.1.1.12	(L1) Set Disconnect-Job Interval	☐	☐
5.1.1.13	(L1) Set Display User Sign-on Information	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.1.15	(L1) Set Inactivity Time-out Interval	☐	☐
5.1.1.16	(L1) Set Inactivity Message Queue	☐	☐
5.1.1.17	(L1) Set Limit Device Sessions	☐	☐
5.1.1.18	(L1) Set Limit Security Officer Access to Workstations	☐	☐
5.1.1.19	(L1) Set Maximum Sign-on Action	☐	☐
5.1.1.20	(L1) Set Maximum Sign-on Attempts	☐	☐
5.1.1.21	(L1) Set Block Password Change	☐	☐
5.1.1.22	(L1) Set Password Expiration Interval	☐	☐
5.1.1.23	(L1) Set Password Expiration Warning	☐	☐
5.1.1.24	(L1) Set Password Level	☐	☐
5.1.1.25	(L1) Set Required Difference in Passwords	☐	☐
5.1.1.26	(L1) Set Password Rules	☐	☐
5.1.1.27	(L1) Set Retain Server Security	☐	☐
5.1.1.28	(L1) Set Remote IPL	☐	☐
5.1.1.29	(L1) Set Remote Sign-on Value	☐	☐
5.1.1.30	(L1) Set Remote Service Attribute	☐	☐
5.1.1.31	(L1) Set Scan File System	☐	☐
5.1.1.32	(L1) Set Scan File System Control	☐	☐
5.1.1.33	(L1) Set System Security Level	☐	☐
5.1.1.34	(L1) Set Shared Memory Control	☐	☐
5.1.1.35	(L1) Set Secure Sockets Layer Cipher Specification List	☐	☐
5.1.1.36	(L1) Set Secure Sockets Layer Cipher Control	☐	☐
5.1.1.37	(L1) Set Secure Socket Layer Security Protocols	☐	☐
5.1.1.38	(L1) Set System Library List	☐	☐
5.1.1.39	(L1) Set Use Adopted Authority	☐	☐
5.1.1.40	(L1) Set Verify Object On Restore	☐	☐
5.1.2.1	(L2) Set Allow Restoration of Security-Sensitive Objects	☐	☐
5.1.2.2	(L2) Set Allow User Domain Objects in These Libraries	☐	☐
5.1.2.3	(L2) Set Auditing Control	☐	☐
5.1.2.4	(L2) Set Auditing End Action	☐	☐
5.1.2.5	(L2) Set Auditing Force Level	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.1.2.6	(L2) Set Automatic Virtual Device Creation	☐	☐
5.1.2.7	(L2) Set Create Authority	☐	☐
5.1.2.8	(L2) Set Create Object Audit Level	☐	☐
5.1.2.9	(L2) Set Disconnect-Job Interval	☐	☐
5.1.2.11	(L2) Set Inactivity Time-out Interval	☐	☐
5.1.2.12	(L2) Set Inactivity Message Queue	☐	☐
5.1.2.13	(L2) Set Limit Device Sessions	☐	☐
5.1.2.14	(L2) Set Limit Security Officer Access to Workstations	☐	☐
5.1.2.15	(L2) Set Maximum Sign-on Action	☐	☐
5.1.2.16	(L2) Set Maximum Sign-on Attempts	☐	☐
5.1.2.17	(L2) Set Block Password Change	☐	☐
5.1.2.18	(L2) Set Password Expiration Interval	☐	☐
5.1.2.19	(L2) Set Required Difference in Passwords	☐	☐
5.1.2.20	(L2) Set Password Rules	☐	☐
5.1.2.21	(L2) Set Password Validation Program	☐	☐
5.1.2.22	(L2) Set Remote Sign-on Value	☐	☐
5.1.2.23	(L2) Set System Security Level	☐	☐
5.1.2.24	(L2) Set Shared Memory Control	☐	☐
5.1.2.25	(L2) Set Verify Object On Restore	☐	☐
5.2.1	(L1) Network Attribute JOBACN (Network Job Action)	☐	☐
5.2.2	(L1) DDM Remote Configuration List (SNA) Attributes	☐	☐
5.2.3	(L1) DDM TCP/IP Attributes	☐	☐
5.2.4	(L2) DDM TCP/IP Attributes	☐	☐
5.2.5	(L1) NFS Shares	☐	☐
5.2.6	(L2) NFS Shares	☐	☐
5.2.7	(L1) Exit Points	☐	☐
5.2.8	(L1) Function Usage	☐	☐
5.2.9	(L1) Intrusion Detection	☐	☐
5.2.10	(L1) Telnet Protocol	☐	☐
5.2.11	(L1) FTP Protocol	☐	☐
5.2.12	(L1) SMTP Mail Relay	☐	☐

Recommendation		Set Correctly	
		Yes	No
5.2.13	(L1) SNMP Access	☐	☐
5.3.1	(L1) IBM i NetServer Guest Profile	☐	☐
5.3.2	(L1) IBM i NetServer LANMAN Password Hash	☐	☐
5.3.3	(L1) IBM i SMB Signing	☐	☐
5.3.4	(L1) IBM i SMBv2 Server	☐	☐
5.3.5	(L1) IBM i NetServer Shares	☐	☐
5.3.6	(L2) NetServer Browse Interval	☐	☐
5.3.7	(L1) Malware Defenses	☐	☐
5.4.1	(L1) Configuring SSH – server protocol 2	☐	☐
5.4.2	(L1) Configuring SSH – banner configuration	☐	☐
5.4.3	(L1) Configuring SSH – disallow host based authentication	☐	☐
5.4.4	(L1) Configuring SSH – set privilege separation	☐	☐
5.4.5	(L1) Configuring SSH – set MaxAuthTries to 4 or Less	☐	☐
5.4.6	(L1) Configuring SSH – set Idle Timeout Interval for User Login Profile Applicability:	☐	☐
5.4.7	(L1) Configuring SSH – restrict Cipher list	☐	☐
5.4.8	(L1) Configuring SSH – Limit Access Via SSH	☐	☐
5.5.1	(L1) IBM i Patch Management	☐	☐
5.6.1	(L1) System Service Tools Password Expiration Interval	☐	☐
5.6.2	(L1) System Service Tools Changing the maximum failed sign-on attempts	☐	☐
5.6.3	(L1) System Service Tools Changing the duplicate password control	☐	☐
5.6.4	(L1) System Service Tools Password Level	☐	☐
5.6.5	(L1) System Service Tools Allow New Digital Certificates	☐	☐
5.6.6	(L1) System Service Tools IDs and Privileges	☐	☐
5.6.7	(L1) System Service Tools locking security-related system values	☐	☐
5.6.8	(L1) System Service Tools Password Rules	☐	☐
5.6.9	(L1) System Service Tools Allow add and remove of password exit programs	☐	☐
6.1	(L1) QSECOFR Profile Shall Be *DISABLED	☐	☐

Recommendation		Set Correctly	
		Yes	No
6.2	(L1) QSECOFR Shall Not be Configured as a Group Profile	☐	☐

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	☐	☐

Appendix: Change History

Date	Version	Changes for this version