Bill of Health®

Security diagnostics and R_X for iSeries

SAMPLE ASSESSMENT REPORT

Vulnerabilities, Ltd.

Security Assessment Results

delivered by

Unbeaten Path International

June xx, 20xx

(see last page to obtain more information and to read copyright statement)

Return to the description of **Bill of Health** software

Section 1: Your Security Plan

Step 1 - Examine your System Values

The security and integrity of your system cannot be guaranteed because you are not running at security level 40 or 50. This is the most important step you can take towards securing your system and ensuring both operating system and data integrity. Moving to security level 40 will ensure that no unsupported interfaces are used, data cannot be modified without detection and users cannot exploit job descriptions that name user profiles to masquerade as another user. Detailed steps you will want to take before moving to security level 40 can be found under the explanation for the QSECURITY system value.

The following system values have settings that do not meet the recommended settings. Examine the recommended settings in Section 2 - System Values. Make sure to read the Considerations Before Changing section if one is included. Because of the side effects that changing some system values produce, it is possible that your business requirements will require that you leave the system value at its less secure setting.

- QSECURITY
- QALWOBJRST
- QLMTDEVSSN
- QLMTSECOFR
- QSHRMEMCTL

Allowing the QPWDEXPITV system value to remain at *NOMAX allows passwords to remain unchanged forever. This is a huge security risk. If someone's password is compromised (say a security administrator's password) that password will remain compromised forever since the user is never required to change it. See the Password System Value section for our recommended settings.

Even though you have changed some of the password composition system values from their defaults, we strongly encourage you to set the QPWDRQDDGT system value to require passwords to contain a digit. This will prevent a 'dictionary attack' against your system.

We strongly encourage you to set the QPWDRQDDIF system value to 1 so that passwords cannot be re-used for 32 times.

We encourage you to look through the specific recommendations found in Section 2 - System Values.

Return to the description of **Bill of Health** software

Step 2 - Examine the Users on the System

Default passwords (passwords the same as the user profile name) exist on your system. Default passwords are a significant exposure. Common reasons they exist are because no password system values have been changed from their default settings and new profiles are initially created with a default password. We recommend that you change at least one of the password system values so that OS/400 will not allow default passwords when a user changes their password. We also recommend that you examine your profile creation process to not use a default password for the initial password. Please see the 'Users with Default Passwords' topic in Section 3 - Users for more details.

Users exist on your system that have not signed on for 60 days. A common method used to gain inappropriate access to systems is to exploit profiles of employees no longer with the company. In addition, the existence of inactive users is not tolerated by most auditors. For more details, see the 'Users that have not signed on recently' topic in Section 3 - Users.

More users than is appropriate have *ALLOBJ special authority. *ALLOBJ special authority should be limited to only a small handful of users because you cannot control what *ALLOBJ users access. For more details, see the 'Powerful Users' topic in Section 3 - Users.

More users than is appropriate have *JOBCTL special authority. *JOBCTL allows the user to control all jobs on your system. For more details, see the 'Powerful Users' topic in Section 3 - Users.

More users than is appropriate have *SPLCTL special authority. *SPLCTL special authority should be limited to only a small handful of users because you cannot control the spooled files that these users can access. In other words, you cannot secure your printed output from someone that has *SPLCTL. For more details, see the 'Powerful Users' topic in Section 3 - Users.

1 group profiles were found to have *ALLOBJ special authority. This means that all of the group members also have *ALLOBJ. More investigation needs to be performed to determine if it is appropriate for all these users to have *ALLOBJ. See the 'Powerful Users' topic in Section 3 - Users for more details.

The following IBM profiles have been altered to have different capabilities (special authorities). Giving these profiles additional capabilities can cause the system to give users more authorities or allow them to perform other functions than you would prefer. Altering IBM-supplied profiles is dangerous. We encourage you to try to determine the reason the profile was altered, determine if an alternate solution is feasible and, if possible, put it back to its default settings.

User profile QSYSOPR should have *SAVSYS and *JOBCTL special authority but has been given *IOSYSCFG.

Users have been given a private authority to the following IBM-supplied profiles which allows them to run a job using this IBM profile, use its authorities, and make it appear the IBM profile performed a function rather than the user themselves. It can be quite dangerous to give users this authority to an IBM-supplied profile. We encourage you to examine the SKYIBMUSRS report that lists the IBM profiles and the users having private authority to ensure appropriateness.

QPGMR

The following IBM-supplied profiles have been made a group profile:

QPGMR

Return to the description of **Bill of Health** software

Step 2 - Examine the Users on the System, *continued ...*

Anything that these profiles own or are authorized to, the members also own or are authorized to. Making users a member of an IBM-supplied profile can open numerous security exposures. For details and recommendations, see the 'IBM Profiles that are Group Profiles' topic in Section 3 - Users.

A significant number of users are members of the same groups. Members of the same groups probably run the same applications. If the group profile owns these applications, then all of the members of the group also own the applications. This means that they can update any file, replace a program with one of their own, download confidential data or delete the entire application.

The following groups have a significant number of members:

SUPERGROUP

The SKYGRPUSRS report lists all groups and the users who are members of those groups. This report should be reviewed to ensure all users should be members of each group. The SKYGRPOWN report provides a list of all of the objects owned by group profiles. Remember, all objects listed in this report are, in effect, also owned by each member of the group. Comparing the reports will tell you which objects specific users own.

See the 'Powerful Groups' topic in Section 3 - Users for more details on the risks and recommendations.

We encourage you to look through the specific recommendations found in Section 3 - Users.

Step 3 - Examine the Object Level Authority

We highly recommend that you look at your object level authority implementation to make sure that it meets your business requirements and is implemented appropriately.

For more details, see the 'Libraries' and 'Getting Started with Object Level Security' topics in Section 4 - Object Authorities.

The *PUBLIC authority setting for the root ('/') file system has been changed from the default setting, but is not at the recommended setting of object authority *RX and data authority *NONE. See the 'Directories' topic in Section 4 - Object Authorities for more information to ensure that it is set to an appropriate value for your business requirements.

Step 4 - Exit Programs

Exit programs were found registered to the exit points for at least some of the network interfaces. Whether these programs belong to a third-party application or someone within your organization has written them, it is imperative that the programs are used to their fullest extent. Our experience is that many organizations purchase or write exit program solutions but never implement them. Please take time to make sure this is not the situation for your organization.

Step 5 - Final Considerations

We encourage you to review the TCP/IP Security, Adopt Authority, Miscellaneous, and Other Considerations sections of this document for other considerations you will want to make for your enterprise.

Return to the description of **Bill of Health** software

Section 2: System Values

System values are configuration settings that apply across your entire iSeries or AS/400 system. Numerous system values are either directly or indirectly security-relevant. This section lists the current setting for each system value, the recommended value, an explanation of the system value along with an explanation of why the value is security-relevant and considerations you will want to make before changing the system value to a more secure setting.

Security System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QSECURITY	30	40 or 50	X
QALWOBJRST	*ALWPTF *ALWPGMADP	*ALWPTF or *NONE	X
QALWUSRDMN	*ALL	*ALL	
QAUTOCFG	0	0	
QAUTOVRT	600	0 or a fixed number	
QCRTAUT	*USE	*USE or *EXCLUDE	
QDSPSGNINF	1	0 or 1	
QFRCCVNRST	4	3	
QINACTITV	30	30	
QINACTMSGQ	*DSCJOB	*DSCJOB	
QDSCJOBITV	30	60	
QLMTDEVSSN	0	1	X
QLMTSECOFR	0	1	X
QMAXSIGN	3	5	
QMAXSGNACN	3	3	
QRETSVRSEC	0	0	
QRMTIPL	0	0	
QRMTSIGN	*REJECT	*REJECT or *FRCSIGNON	
QRMTSRVATR	0	0	
QSHRMEMCTL	1	0	X
QUSEADPAUT	QUSEADPAUT	Authorization list name	
QVFYOBJRST	3	3 or 5	

QSECURITY:

Sets the level of security on your system. Unless your system is at level 40 or 50, security can easily be by-passed on your system and you have no system integrity. This means that third-party applications can use interfaces not approved by IBM. This can affect the stability of your system and allows auditing and some authority checking to be by-passed.

Recommendation:

If you are at OS/400 release V5R1 or lower, our recommendation is to set this value to 50. If you are at release V5R2 or higher, our recommendation is to set this value to 40. Parameter validation, which offers you protection against recent programming exploits, is now performed at security level 40 as well as security level 50 beginning in V5R2. This is the most important system value you can set for the security of your system.

Return to the description of **Bill of Health** software

Steps before changing:

To move from level 20 or 30 to level 40 or 50 requires that you:

- Carefully plan how users are going to get the authority to access and run applications. At security level 20, users, by default, have *ALLOBJ special authority (this special authority is explained in more detail in the User section of this document). *ALLOBJ automatically gives the user access to every object on the system. When moving from security level 20 to a higher level, *ALLOBJ is removed from all users except those in the *SECOFR user class. Users can get access to run applications through a number of methods - *PUBLIC authority, adopted authority, authority to an authorization list or users' individual private authorities. The method you choose will depend on the types of users accessing the application, the sensitivity of the data being stored and how the application data is being accessed.
- Audit to find out if any applications will fail at security level 40 or 50. Do this by adding *PGMFAIL to the QAUDLVL system value. In addition, make sure auditing is turned on. *AUDLVL must be specified for the QAUDCTL system value.
- Handle the use of job descriptions that name user profiles. At security level 40 or 50, anyone using the job description needs authority to both the job description and the user profile. At security level 20 or 30, you only need authority to the job description. To discover who is currently using a job description that doesn't have authority to the named user profile, add *AUTFAIL to the QAUDLVL system value.

Note. You must audit long enough so that you know that a significant portion of your applications have been run - for example, over month or quarter end.

Detailed Steps:

1. To determine whether programs will run at security level 40 or 50:

When you have audited for *PGMFAIL for a month or longer, run the Display Audit Journal Entry (DSPAUDJRNE) command specifying AF for the Journal Entry Type parameter. This will produce a report of violations. Look for the following violation types (each entry will be preceded with AF and one of the following):

- B Restricted (blocked) instruction violation.
- C Object validation failure.
- D Unsupported interface (domain) violation.
- R Attempt to access protected areas of disk (enhanced hardware storage protection).
- S Default sign-on attempt.

2. To determine if you must accommodate any job descriptions that name user profiles:

When you have audited for *AUTFAIL for a month or longer, run the DSPAUDJRNE command specifying AF for the Journal Entry Type parameter. Look for the following violation type:

- J Job description and user profile authorization failure (using a *JOBD that names a user profile).

Return to the description of **Bill of Health** software

Alternative Method:

Rather than running the DSPAUDJRNE command, you can run the Display Journal (DSPJRN) command. Run this command (vs DSPAUDJRNE) if you intend to send the information to an outfile. You will want to specify the following parameters in addition to the outfile name and any time or date ranges you wish to specify:

DSPJRN JRN(QAUDJRN) JRNCDE((T)) ENTTYPE(AF)

OUTFILFMT(*TYPE4) ... for V5R1 and earlier.
OUTFILFMT(*TYPE5) ... for V5R2 and later.

Once you have resolved any issues, you can set the QSECURITY system value to 40 or 50 and IPL. You can see the current and pending values for QSECURITY by running the Display Security Attributes (DSPSECA) command.

Note. Sometimes you will get audit journal entries flagging third party applications. It is rare today that a third party application does not run at security level 40 or 50. So if you have entries, contact the vendor. It is likely that they take one code path at security level 20 or 30 and another, that does not cause violations, at security level 40 or 50.

Details about OS/400 auditing can be found in either the iSeries Security Reference manual or the book Implementing AS/400 Security.

QALWOBJRST:

Determines whether system state or programs that adopt their owner's authority are allowed to be restored onto the system. In a production environment, it is critical to take control of what is restored onto your system.

Considerations before changing:

If you specify *NONE, you will have to change the system value to *ALWPTF before you can load IBM PTFs.

Many third-party applications will not be able to be restored to your system because they use adopted authority. You will have to change the system value to *ALWPGMADP to allow this activity.

QALWUSRDMN:

Determines where user spaces, user queues and user indexes are allowed to be created. Only configurations with very high security requirements will have to specify specific libraries to contain these objects.

QAUTOCFG and QAUTOVRT:

Both values determine whether devices are automatically created. QAUTOCFG controls auto-creation of devices and controllers. Turn this value on when configuring these objects then turn it off. QAUTOVRT controls auto-creation of virtual devices. The default value, *NOMAX, allows an unlimited number of virtual devices to be created. This opens up the system to a denial of service attack where someone continuously attempts to access your system, getting a new virtual device with each attempt.

Return to the description of **Bill of Health** software

QCRTAUT:

Sets the default *PUBLIC authority for every newly created object. This value can be controlled at the system level with this value or at the library level.

Considerations before changing:

If you change this value from the default *CHANGE, you will also need to change the following:

- CRTAUT value of QSYS to *CHANGE (so *MSGQs and *DEVDs are usable).
- Default value for AUT parameter on CRTLIB from *LIBCRTAUT to *USE (or *EXCLUDE).

QDSPSGNINF:

Causes the user's last sign on date and time to be displayed when the user signs on.

Considerations before changing:

While this is valuable information to display, most users don't pay attention to the information and if they do, have no idea what to do with it if they notice a problem. Rather than turning this on for all users, change the profiles of your powerful users to display the last sign on information and leave this value off.

QFRCCVNRST:

Determines whether programs and service programs are going to be converted when they are restored.

Recommendation:

New values were added for V5R2 that allow you to take control of what is being restored onto your system. If you are at V5R2 we recommend that you set this value to 3. If you have cause to not trust the vendor whose objects are being restored to your system, consider setting this value to 5. Be aware, however, that the restore process could take a significant amount of time.

Return to the description of **Bill of Health** software

QINACTITV, QINACTMSGQ, QDSCJOBITV:

These three system value work together. QINACTITV is the time interval for inactive jobs before some action - determined by the QINACTMSGQ system value - is taken. If you specify the value *DSCJOB - disconnect job - for the QINACTMSGQ system value, the value of DSCJOBITV determines how long the job will stay in disconnected status before the job is ended.

Considerations before changing:

The inactivity timeout value applies to all users across the system. This can often be inappropriate if you have a large enterprise with widely varying user requirements. If that is the case, there are third party products available that provide granular timeout values for varying needs.

QLMTDEVSSN:

Determines whether a user can sign on to more than one device at a time. This prevents users sharing passwords and inadvertently signing on to more than one workstation at a time.

Considerations before changing:

Occasions exists where users must sign on to more than one workstation at a time - especially in an application development environment where programs are being developed and debugged. In addition, while not recommended, some applications have all users sign on using the same user name. Make sure you don't have these conditions before changing this system value.

QLMTSECOFR:

Restricts QSECOFR as well as all other users with *ALLOBJ or *SERVICE special authority from signing on to a workstation unless they have explicit authority to the device. This prevents powerful users from signing on to remote workstations or otherwise gaining access in locations where they are not readily noticed.

Considerations before changing:

If you are using virtual devices and have not implemented named devices, it is unlikely that you will be able to implement this system value. Without named devices you will have to grant authority to QSECOFR and your security administrators to ALL virtual devices, thus defeating the purpose of this system value.

QMAXSIGN and QMAXSIGNACN:

QMAXSIGN determines how many times a user can attempt to sign on before the action defined by QMAXSIGNACN takes place.

Considerations before changing:

You might consider purchasing a product that allows you to define security events, such as 50 invalid sign on attempts in 5 minutes, and choose to be notified when the event occurs rather than using these system values. Choosing to disable the profile being used and/or disabling the device can be two areas to attack your system with a denial of service attack.

QRETSVRSEC:

Determines whether decryptable passwords can be stored on your system. Note that this value does not apply to OS/400 user passwords. These passwords are typically used in server authentication entries (used in DDM and other communication protocols) and validation lists (used by many web applications).

Return to the description of **Bill of Health** software

Considerations before changing:

If you run DDM over TCP/IP or a protocol such as PPP, you probably need to allow decryptable passwords. If you change from allowing passwords to not allowing passwords, when you change the system values, at V5R1 and earlier OS/400 will delete all the decryptable passwords in validation lists and server authentication entries. As of V5R2, the decryptable passwords will not be retrievable but they won't be deleted. If you change the system value back, the decryptable passwords are once again available.

QRMTIPL:

Determines whether power on/off and IPLs can be initiated remotely to your system.

QRMTSIGN:

Determines whether remote signons are allowed and whether users making the remote request will be required to enter a user id and password before the connection is made.

QRMTSVRATR:

Determines whether remote problem analysis can be performed on your system. Unless IBM specifically requests this value to be turned on, leave this value off.

QSHRMEMCTL:

Defines whether applications are allowed to use shared memory APIs. These APIs are typically used by applications that have been ported from POSIX or that run in the PASE environment. Allowing shared memory allows one job to access the memory of another job. It also allows jobs to share pointers. This means that one job which has authority to access an object may allow another job to access the same object through the use of a shared pointer.

Considerations before changing:

Some ported applications or applications running in PASE may depend on the use of these APIs and may fail if their use is not permitted. However, for installations requiring the highest security, these APIs should not be allowed to run on your system.

Note. The APACHE web server instances and the *ADMIN instance of the web server require this value to be 1 (on). If you are running either of these, this system value must be On.

QUSEADPAUT:

Determines whether a user can create a program that uses adopted authority. In a production environment programming compilations should not be taking place. Use this value to make sure the use of adopted authority is not exploited by devious users.

QVFYOBJRST:

Beginning in V5R1, most of OS/400 is digitally signed. OS/400 also provided ways for user written and third party applications to be digitally signed. This system value determines whether a program is allowed to be restored onto your system without being digitally signed or without having a valid digital signature.

Return to the description of **Bill of Health** software

Considerations before changing:

Most vendors have not yet signed their applications. Setting this system value to require signatures to be verified will prevent most applications from being restored. To restore an unsigned application you will have to change this value. However, this allows you to have tremendous control over what is restored to your system.

Recommendation:

If you want to take very tight control of what is restored on to your system, set this value to 5. Otherwise, the value of 3 is sufficient.

Password System Values

The password system values determine the composition of users' passwords. It is important to set at least one of the system values to something other than the default. Setting one of these values also activates checking so that passwords cannot be the same as the user's profile name.

The more password system values that you activate or turn on, the more difficult it will be for hackers or a disgruntled employee to guess a password. However, the more password rules you enforce, the harder the passwords will become to come up with and remember. Therefore, it is more and more likely that passwords will be written down. This is one of those tradeoffs between tighter security and end user convenience and satisfaction.

If you do nothing else, turn on QPWDRQDDGT so a digit is required in all passwords, and set the minimum length, QPWDMINLEN, to 7.

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QPWDEXPITV	*NOMAX	180	X
QPWDLVL	3	Anything but 0	
QPWDRQDDIF	0	1	X
QPWDMINLEN	4	7	X
QPWDMAXLEN	25	10	
QPWDRQDDGT	0	1	X
QPWDLMTAJC	1	0	X
QPWDLMTCHR	*NONE	*NONE	
QPWDLMTREP	2	2	
QPWDPOSDIF	0	0	
QPWDVLDPGM	*NONE	*NONE	

QPWDVLDPGM:

If a program name is specified for QPWDVLDPGM, it should be examined to determine its intent. The use of a password validation program is not inherently bad or harmful. However, passwords are passed to this program in clear text (e.g. not encrypted) so the program should be examined to ensure those passwords are not being stored or otherwise compromised.

QPWDLVL:

You are already using passphrase support. This is an excellent choice.

Return to the description of **Bill of Health** software

Auditing System Values

System Value	Current Value	Recommended Setting	Deviation from Recommendation (X)
QAUDCTL	*AUDLVL *OBJAUD *NOQTEMP	*AUDLVL *OBJAUD *NOQTEMP	
QAUDLVL	*SECURITY *CREATE *AUTFAIL *SERVICE *DELETE	*AUTFAIL *CREATE *DELETE *SAVRST *SECURITY *SERVICE	X
QCRTOBJAUD	*NONE	*NONE	
QAUDFRCLVL	*SYS	*SYS	
QAUDENDACN	*NOTIFY	*NOTIFY	

QAUDCTL:

The On/Off switch for auditing OS/400. If no values are specified, auditing is not active.

If auditing is active, it is important to understand the intent of why you are auditing. If it is to check for inappropriate behavior then you need to make sure to have a process to ensure the proper analysis is taking place.

If the intent is just to gather the data for regulatory or for forensics data (should it be required) then what needs to be examined is your retention period for the audit journal receivers to make sure the receivers are saved and stored appropriately.

QAUDLVL:

Determines what actions and events are audited. The Security - Reference Guide from IBM describes what audit entries are produced for each value.
The absolute minimum auditing setting we recommend is:

- *AUTFAIL
- *SECURITY

Recommended setting:

- *AUTFAIL
- *SECURITY
- *CREATE
- *DELETE
- *SAVRST
- *SERVICE

Additional considerations:

More auditing might be required depending on the industry or government sector your company is in. This assessment is not a substitute for turning on OS/400 auditing and examining the audit journal entries. You can either use OS/400 commands, such as Display Audit Journal Entry (DSPAUDJRNE) to examine the audit journal entries or you can buy a third party solution.

Return to the description of **Bill of Health** software

QAUDFRCLVL and QAUDENDACN:

QAUDFRCLVL determines how often an audit record is forced to disk.

QAUDENDACN determines the action taken when OS/400 cannot send audit records.

Do not change these values. The default (our recommended) settings are sufficient. Changing them could produce undesirable results such as performance problems or the system ending immediately.

System Library List

The system portion of the library list is defined in the system value QSYSLIBL. If any of the libraries in this list have *PUBLIC authority of *CHANGE or greater, this poses a security risk. *CHANGE authority allows a user to create objects into a library. If a user can create a program and place it into one of these libraries, it will be ahead of application libraries and it is possible that adopted authority (discussed later in this Assessment) or other mechanisms could be exploited. We strongly suggest that libraries in the system portion of the library list be no greater than *PUBLIC(*USE).

All libraries in the system portion of the library list on your system are either *USE or *EXCLUDE.

Return to the description of **Bill of Health** software

Section 3: Users

User profiles are how the iSeries understands and knows how to deal with a user. For example, the user profile defines the highest priority the user's job can run at, the maximum amount of storage they're allowed to have, the national language they will use (Spanish, French, Chinese, etc) not to mention all the security settings the user profile defines. This assessment focuses on the security attributes of the user profile.

Users with Default Passwords

- There are 5 user profiles with default passwords.
- Of these profiles 3 are NOT set to status of *DISABLED.
- Passwords are set to expired and must be changed when 1 users next sign on.

Default passwords mean that the password is the same as the user profile name. If the QPSECPWD report shows users with passwords the same as the profile, this is a very dangerous situation. Someone trying to guess a profile's password will most likely try the password the same as the profile name.

However, the risk is mitigated if the profile's status is set to *DISABLED. That's because you cannot sign on with a profile whose status is *DISABLED.

Obviously the remedy for this situation is to require the users to change their password, by setting the password expired flag in the user profile to *YES. This means that they will have to change their password the next time they log on. However, do not be complacent and assume this will fix the problem. You will want to monitor the situation to make sure that everyone signs on in an appropriate timeframe to get the situation fully rectified.

The QSECPWD report lists the users with default passwords.

Users that have not signed on recently

33 users have not signed on in 60 days.

Users that have not signed on recently are considered to be inactive users. If the person assigned to this profile wishes to break in to your system, the first profile they will try is their own. Leaving old profiles on the system is an exposure. They also take up space on your system. Finally, most auditors will take exception to having inactive profiles on your system.

The Analyze Profile Activity (ANZPRFACT) command can be used to automatically disable a profile that has not been used for sign on in the timeframe of your choice (we recommend 60 days). The Change Active Profile List (CHGACTPRFL) command allows you to specify profiles that should never be disabled by OS/400.

The SKYINAUSRS report lists users that haven't signed on in 60 days.

Return to the description of **Bill of Health** software

Powerful Users

Powerful users are users that have special authorities. Special authorities give users the ability to perform some function. By default, users should not be given any special authorities. Special authorities should only be given if the user has a specific job need for that capability. Most end users need no special authorities. It is usually system administrators, system operators, security officers and some application owner profiles that will require special authorities.

***AUDIT**

- Of 84 profiles on your system, 9 users have audit special authority.

*AUDIT special authority allows users to change the auditing system values and set up auditing on individual users or objects. *AUDIT special authority needs to be limited to a very few users who have a direct need to manage the auditing on your system. Auditors are going to look for a separation of duties. So they typically want to see *AUDIT only given to auditors - not security officers. For smaller companies, this is probably not practical. However, even in a small shop, its use should be strictly limited.

***JOBCTL**

- Of 84 profiles on your system, 27 users have job control special authority.

*JOBCTL allows users to manipulate the attributes of all jobs on the system, including holding or ending jobs, changing the priority, etc. *JOBCTL used to be given by default to programmers and is still part of the QPGMR user profile shipped from IBM. However, it is often not necessary or desirable for programmers to have this capability.

***IOSYSCFG**

- Of 84 profiles on your system, 19 users have network system configuration authority.

*IOSYSCFG allows users to configure both SNA and TCP/IP communications as well as start, stop and configure all TCP/IP servers. *IOSYSCFG special authority has become very powerful in recent releases. You want to limit *IOSYSCFG to only those users who have a need to manage your network configuration and communications.

***SAVSYS**

- Of 84 profiles on your system, 16 users have save system special authority.

*SAVSYS gives the user the authority to save and restore ANY object on the system. *SAVSYS is another powerful capability and should only be given to individuals that you want to have the ability to save your entire system or selected objects. It used to be given out to programmers. This is no longer the case, however, because most programmers are not required to perform system saves or restore objects besides the ones they already have authority to.

***SECADM**

- Of 84 profiles on your system, 12 users have security administration special authority.

*SECADM special authority gives the user the ability to create and manage user profiles and manage access controls within Application Administrator. *SECADM should only be given to users who have the business need to create user profiles.

Return to the description of **Bill of Health** software

***SERVICE**

- Of 84 profiles on your system, 9 users have service special authority.

*SERVICE special authority, allows users to use SSTs (system service tools) which include performing comm traces, configuring ASPs, etc. This is extremely powerful and dangerous. Anyone with this special authority can use service tools to 'flip bits' using the Display/Alter function, run communication traces which include clear text passwords, reload your system and more. Think seriously before you hand out this capability.

***SPLCTL**

- Of 84 profiles on your system, 11 users have spool control special authority.

*SPLCTL special authority allows users to manage ALL spooled files on your system. You cannot control this access. Although some people try, there are always ways around the fences they try to build. *SPLCTL should only be given to users who require the ability to manage every spool file on your system. Users typically do not need this special authority. Rather, based on a combination of having *JOBCTL and the way an output queue is created, you can allow users to manage most spooled files, yet have the ability to keep certain spooled files confidential - that is, only seen and manager by the owner or the spooled file. The book, Experts' Guide to OS/400 and i5/OS Security by Carol Woodbury and Patrick Botz, contains a table listing the attributes of an output queue and how users with *JOBCTL, *SPLCTL and no special authority can access or manage the spooled files in the output queue.

***ALLOBJ**

- Of 84 profiles on your system, 13 users have *ALLOBJ special authority.

The next special authority being reported on is *ALLOBJ special authority and it is in a category of its own. *ALLOBJ gives its users the ability to access any object on the system. This access cannot be prevented. Again, like *SPLCTL, many people try, but it is our opinion that it is not possible. Once you give over *ALLOBJ special authority, you have basically handed over the keys to your system. *ALLOBJ should only be given to very trusted users. In addition, it is very likely that you should audit the commands that *ALLOBJ users enter so that you can monitor their activity.

For a list of users that have each of these special authorities see the QPSECUSR report.

Return to the description of **Bill of Health** software

Powerful Groups

Group profiles are an administrative tool provided by OS/400 to group users who require the same special authorities and need to be authorized to the same things. For example, rather than authorizing 50 users to an order entry application, you can assign them to a group profile and authorize the group to the application. Since the group has authority, the user (or the member of the group) will also have authority.

The same thing applies to special authorities. If a group has special authority, for example *SPLCTL, all members of the group also have *SPLCTL special authority.

- Of 9 profiles that have *AUDIT special authority, 1 profiles are group profiles.
- Of 27 profiles that have *JOBCTL special authority, 1 profiles are group profiles.
- Of 19 profiles that have *IOSYSCFG special authority, 0 profiles are group profiles.
- Of 16 profiles that have *SAVSYS special authority, 1 profiles are group profiles.
- Of 12 profiles that have *SECADM special authority, 1 profiles are group profiles.
- Of 9 profiles that have *SERVICE special authority, 0 profiles are group profiles.
- Of 11 profiles that have *SPLCTL special authority, 1 profiles are group profiles.
- Of 13 profiles that have *ALLOBJ special authority, 1 profiles are group profiles.

Because of the power of *ALLOBJ special authority, if any group profiles have this authority, more investigation is required.

To see what users are in a group, run the Display Authorized Users (DSPAUTUSR) command using the group ordering option on the command.

Groups that Own Objects

Groups that own objects can be a security issue. Every object that a group owns, each user that is a member of the group also owns. This means that every group member can upload, download, modify, replace or even delete every object that the group owns. Obviously this can be quite dangerous. You will find this situation when an application requires application users to be a member of the profile that owns the entire application. This is not a sound security implementation.

The SKYGRPOWN report lists groups that own objects, and the objects they own.

Recommendations:

- If one of these groups owns a third party application, we recommend that you talk to the vendor and determine a different way for these users to get access to run the application
- If a group profile owns the objects of an application that your organization has written, we recommend that you re-work the application authorization scheme to not require users to be a member of the owning profile.

Return to the description of **Bill of Health** software

Use of IBM-Supplied User Profiles

Altered IBM Profiles

Altering IBM-supplied profiles can be dangerous.

Some IBM-supplied profiles have been altered to have more capability than their default setting. This can be a dangerous practice depending on how these profiles are used.

Some IBM-supplied user profiles are shipped with special authorities. The table below indicates what changes, if any, have been made to the special authorities granted to the QPGMR, QSRV, QSRVBAS, QSYSOPR and QUSER IBM-supplied user profiles.

User Profile	Authority	Added or Removed
QSYSOPR	*IOSYSCFG	Added

IBM Profiles with a Password

Allowing IBM Profiles to have passwords can be dangerous. That's because these profiles and passwords are often well-known and many times shared which removes all accountability for the actions of these profiles.

The following IBM-supplied profiles have a password. We recommend that you change these to PASSWORD(*NONE). Only give QSRV and QSRVBAS a password when the IBM representative is on site. Set the password back to *NONE when they leave.

- QSRV

IBM Profiles that are Group Profiles

IBM Profile	No. of members
QPGMR	1

To see the list of users that are members of these profiles, see the SKYGRPUSR report.

By giving users authority to an IBM-supplied profile or by making a user a member of an IBM-supplied profile, you are giving those users additional authorities. OS/400 grants these IBM-supplied profiles private authorities to many commands and programs. To see what these profiles are authorized to, run DSPUSRPRF xxxxx *OBJAUT where xxxxx is the name of the IBM-supplied profile.

To determine what objects these users own, including a list of application objects, you can run DSPUSRPRF xxxxx *OBJOWN where xxxx is the name of the group profile. Please note this report will include objects created by IBM as well as any application objects owned by these profiles. In other words, the report may be quite lengthy.

Recommendations:

- If third-party application objects are owned by an IBM-supplied profile, we recommend that you talk to the vendor and determine a different way for these users to get access to run the application.
- If an application written by your company is owned by an IBM-supplied user profile, we recommend that you re-work the application authorization scheme to not require users to be members of the owning profile. We also recommend that the owning profile be changed to a non-IBM-supplied profile.

Return to the description of **Bill of Health** software

Profiles not *EXCLUDE

The default *PUBLIC authority for profiles is *EXCLUDE. Users that have *USE authority or greater to a profile can submit a job as that profile, use the profile swap, profile token or the UID/GID APIs to change and run their process as that profile, and use a job description that names that profile. This can be a security exposure if the profile is a powerful profile.

The following profiles have *PUBLIC authority NOT set to *EXCLUDE:

- JOHNV

Note. IBM ships a few profiles that are not *PUBLIC(*EXCLUDE). Changing the *PUBLIC authority of these profiles may produce unpredictable results. Do this at your own risk.

- QDBSHR
- QDBSHRDO
- QDOC
- QSPLJOB
- QTMPLPD

*USE Authority to IBM-Supplied Profiles

The table below lists user profiles that have *USE authority or greater to the QPGMR, QSECOFR, QSRV, QSRVBAS, QSYSOPR and QUSER IBM-supplied user profiles.

In addition, the SKYIBMUSRS report provides a list of all IBM-supplied profiles and any users that have been given a private authority to them. You may see some IBM-supplied profiles having authority to other IBM-supplied profiles. It is likely that these authorities were granted during the installation of OS/400 or other IBM product and do not pose an issue. Your focus should be on individual users who have authority to IBM-supplied profiles.

System Profile	Users with *USE Authority
QPGMR	JOEY
QPGMR	LINDAV

Password Expiration Interval

The expiration of passwords can be controlled through the user profile's password expiration interval attribute. This value defaults to use the system value QPWDEXPITV. You might want to set your powerful users' expiration interval to something less than the system value.

The SKYPWDEXPI report lists users whose password expiration interval is not set to *SYSVAL.

Return to the description of **Bill of Health** software

Controlling a User's Environment

Most end users are set up in an environment that takes them directly into an application when they sign onto a system. This is accomplished by specifying an Initial Program in the user's profile. The Initial Menu attribute in the user profile is often set to *SIGNOFF so that when the user exits the application, the session is forced to sign off and the user cannot 'wander' outside of the application - at least not through the 'green screen' interfaces. Also, they are usually prevented from running commands from an OS/400 command line through the use of the limited capability attribute of the user's profile. This method is called 'menu access control'. We recommend this approach for end users. However, this approach is not enough to secure your system. Object authority is also required - more on that issue later.

Limited Capability Users

- Of 84 profiles on the system, 15 users have Limited Capabilities: *YES. This means that they are restricted from running most commands from an OS/400 command line. In addition, they cannot change their initial program, initial menu, current library or attention key program.

- Of 84 profiles on the system, 0 users have Limited Capabilities: *PARTIAL. This means that they cannot change their initial program, current library or attention key program but can enter commands and change their initial menu. In our opinion, there is not much security value in using this particular setting.

Commands for Limited Users

Commands can be configured to allow users - even those with limited capabilities *YES - to run them. The following is a list of commands that can be run by those users:

Command	Library	Text
DSPJOB	QSYS	Display Job
DSPJOBLOG	QSYS	Display Job Log
DSPMSG	QSYS	Display Messages
SIGNOFF	QSYS	Sign Off
SNDMSG	QSYS	Send Message
STRPCO	QIWS	Start PC Organizer
STRPCO	QSYS	Start PC Organizer
WRKENVVAR	QSYS	Work with Environment Var
WRKMSG	QSYS	Work with Messages

Controlling their Green Screen Environment

- Of 4 user profiles that have an initial program specified, 2 do not have *SIGNOFF specified for their initial menu.

It may be ok for these users not to have *SIGNOFF specified, but you will want to examine the list and make sure that it is appropriate for each profile.

To see each user's environment (initial program, initial menu, etc) you can run the Print User Profile (PRTUSRPRF) command.

Return to the description of **Bill of Health** software

Controlling what appears on their PC Desktop.

OS/400 has provided mechanisms to make it fairly easy to control a user's green screen environment. However, controlling the user's environment on a PC is not a trivial task. Two methods exist for managing a user's desktop. Those include Microsoft policies and Application Administration (App Admin). App Admin is an OS/400 feature. App Admin has several features. Using two of these you can control which Operations Navigator and Client Access Express functions a user sees on their desktop.

The SKYADMCLNT report lists the client functions that you can control and shows which, if any, users are having their environments controlled through this mechanism.

WARNING. Do not fool yourself into thinking that if you use these two features of App Admin, you have implemented a robust security scheme. You have not. You should think of these two features as an extension to the green screen 'menu access control'. All you're doing when you use these is controlling what appears on the user's desktop. You are in no way protecting objects on the iSeries system. That said, just as we recommend menu access control for simplifying a user's environment, we recommend using App Admin for the same reason.

A third feature of App Admin does provide a layer of security. That feature controls the use or access of certain OS/400 tasks. The difference is that they are OS/400 tasks - not PC-based tasks. This feature will be discussed in the Object Security section of this Assessment.

DST Users and Passwords

Prior to V5R1 DST users were limited to the three default users shipped from IBM. In V5R1 IBM provided the capability to create your own DST users and give them certain capabilities to be used within service tools. Unfortunately, IBM has provided no interface to allow us to report on those users. You must sign on though DST and manage those yourself.

We encourage you to change the passwords of the IBM-shipped DST users from their defaults.

IBM DST User and Default Passwords

DST Capability	DST User	Default Password
Security Officer	QSECOFR	QSECOFR
Full Capability	22222222	22222222
Basic	11111111	11111111
Service Capability	QSRV	QSRV

We especially encourage you to change the security officer (QSECOFR) DST user password from its default. Change it, write it down and lock it up. It is rare that you will hear us recommending that you write down a password. However, in this case, it needs to be changed from the default, but it is a rarely used password so could easily be forgotten or not needed for months or years. If you lose both the QSECOFR user profile and the QSECOFR DST passwords, you will be forced to re-load your system to recover from this situation. You can lose or forget one or the other. But you have major problems if you forget both of them.

Return to the description of **Bill of Health** software

Validation List Users

Validation list objects are a method OS/400 has provided to allow applications - like a web application - to have a secure method for storing user authentication information. For example, when visiting a web site, the web application may require a user to enter their user name and password. The web application may choose to require the user to have an iSeries user profile and password. Or, in the case of many internet applications, they can use a validation list, define the users there, and not require a real user profile. But they still have the benefit of having a secure method to store the authentication information (typically a password).

Robust management tools for these users do not exist. However, you can manage these users through the *ADMIN instance of the APACHE web server. The IBM Rochester CTC (Custom Technology Center) also has a tool-kit that you can purchase at minimal cost. Or you can write your own tools using the validation list APIs.

We have found that you have the following validation lists on your system:

- GLDVLDL in QUSRDIRDB
- QGLDVLDL in QUSRSYS
- QSASRVID2 in QUSRSYS
- QTOCPTP in QUSRSYS
- QTOVDVPKEY in QUSRSYS
- QTOVDVSKEY in QUSRSYS
- QTOZRADI in QUSRSYS
- TEST in QGPL Test validation list
- TEST in SECBOOK Test Validation List

The SKYVLDLE report lists the validation list entries in each validation list. You may find that your validation lists need to be cleaned up. While this is not necessarily a security exposure, it is a security management task that you should be aware of.

Return to the description of **Bill of Health** software

Section 4: Object Authorities

Most systems do not have a robust object authority scheme in place. Most objects (libraries, files, folders, etc) have the default *PUBLIC authority of *CHANGE. Unfortunately, given today's highly networked environment, *CHANGE authority and even *USE provides too much authority for most objects.

Consider this:

*USE authority allows a user to download a file or to display the contents of a file and cut and paste it into a file on his or her laptop. *USE can be quite powerful given today's technology.

*CHANGE authority allows a user to download a file, modify it and then upload the file. The integrity of data comes into question when *PUBLIC authority is *CHANGE or greater. That's because everyone on the system has the ability to update the file.

*ALL authority allows a user to do whatever they want to the file, including download it, upload it, replace it or delete it. *PUBLIC authority *ALL is quite dangerous.

Let's look specifically at the *PUBLIC authority of libraries and directories.

Libraries

We recommend that most libraries have *PUBLIC authority no greater than *USE. This is to prevent users from creating objects into libraries. Some libraries require *CHANGE authority because objects are supposed to be created into them. One example of this is the library QGPL. However, we do not believe there is any reason for a library to have *PUBLIC authority *ALL. *ALL authority allows anyone to actually delete the entire library - rarely a desired action.

Recommendations:

- The SKYLIBAUT report lists all libraries on the system and their *PUBLIC authority. We recommend you examine all libraries with *PUBLIC authority greater than *USE to determine if any of the libraries can have their authorities reduced.
- Analyze the public authority settings for all libraries. Be careful changing third-party application libraries. You can often reduce their *PUBLIC authority to *EXCLUDE and then you will want to authorize the appropriate users to the applications libraries. But we don't recommend changing the authority to the application objects themselves (such as files) without a thorough analysis. It can be done, but not without some planning.

Return to the description of **Bill of Health** software

Create Authority

One of the attributes of a library is create authority. This value is used when an object, such as a file, is created into the library. Perhaps you have noticed that on most commands, the AUT parameter defaults to *LIBCRTAUT. This means that when a file is created, the *PUBLIC authority for the file will default to whatever the create authority attribute of the library is set to. A library's create authority value defaults to *SYSVAL. This means that, unless the value is changed, the value of the system value QCRTAUT is used for the object's *PUBLIC authority setting. When OS/400 is shipped, QCRTAUT defaults to *CHANGE. So, when most objects are created, their *PUBLIC authority is set to *CHANGE. (See the system value section of this assessment for considerations you will want to make before changing QCRTAUT).

- The QCRTAUT system value is set to *USE on your system.

You may not want objects created into a particular library to default to the QCRTAUT value so you may wish to change the library's create authority (preferably to *USE or *EXCLUDE - we do not recommend *ALL).

The SKYLIBAUT report lists all libraries on your system with their create authority values. Hint: While not always accurate, the library's create authority is an indication of the *PUBLIC authority setting of the objects residing in the library.

Before changing any library's create authority value, make sure that the applications using the objects in the library can accommodate a different security setting. A more restrictive setting than the current setting may prevent some applications from working.

Return to the description of **Bill of Health** software

Directories

Directories are very often ignored, forgotten and discarded as 'not applying to me'. We believe that all system administrators should be concerned with the authorities of the various file systems within the Integrated File System (IFS). That's because IBM and some third party vendors place more and more data in these file systems - in particular, the root ('/') file system each release.

When considering the authority of an object in the IFS, you have to consider two authorities - the data authority and the object authority. By default, OS/400 ships the root or '/' directory with data authority *RWX and object authority *ALL. This is the equivalent of shipping QSYS with *PUBLIC *ALL and create authority *ALL. In most cases, when an object is created into a directory, the object inherits its authorities from the directory it is being created into. This means that most objects being created into the IFS have the equivalent of *PUBLIC *ALL. This means that, by default, anyone can create their own directory or delete an object or subdirectory. This is almost always more access than what is required or desired.

- The *PUBLIC authority of root or '/' on your system is:

  - Data authority *RWX

  - Object authority *NONE

The report, QPSECPVT, lists the authorities of the directories under root. As with libraries, the authorities on the directory often reflect the authorities on the objects within the directories.

Recommendations:

- Set *PUBLIC authority for '/' (root) to Data authority *RX and object authority *NONE. This will allow applications to search through root but not create anything into it. You may be able to set root to Data authority *X, but then the general public would not be able to list any of the subdirectories directly under root. This can be a problem for some environments.
- Set *PUBLIC authority of application directories to no more than Data authority *RX and Object authority *NONE. Often you can set Data authority to only *X, unless the application needs to produce a list of objects within the directory.
- IBM-supplied directories should be ok the way they are shipped. But as a safe-guard, you can check to make sure they are set to data authority *X or *RX and object authority *NONE.
- We don't recommend changing the *PUBLIC authority of QSYS.LIB.

Return to the description of **Bill of Health** software

Getting Started with Object Authorities

You will notice that we have concentrated on the *PUBLIC authority for libraries and directories in this section. That's because when you consider implementing a more stringent object authority model, we recommend that you start at the library or directory level. You may also need to consider tightening the *PUBLIC authority of all the objects in a library, but you will get a great benefit just starting at the library and directory levels.

For example, take an HR application. Only the HR department should have access to this application. By setting *PUBLIC authority *EXCLUDE on the HR application library and granting the HR group the same authority that *PUBLIC used to be set to, you are allowing the appropriate users to run the application and preventing the rest of the company from accessing confidential data.

Object level security is in effect whenever the object, such as a file, is accessed. Whether the object is accessed with a menu-based application or a network interface such as FTP or ODBC or an operator entering a command from a command line or a web application serving enterprise data, object authority is always checked. This is why it is one of the most important aspects of your overall security scheme.

Whether you stop at the library or directory level, we strongly recommend that you implement a more stringent object level authority model if you are currently using the current values as shipped from IBM or if you have changed the defaults to be even less restrictive.

To investigate the authorities of the objects within a library or directory, you can use the Print Private Authorities (PRTPVTAUT) or a Print Public Authorities (PRTPUBAUT) commands to help you in your analysis.

Return to the description of **Bill of Health** software

Authorization Lists

Authorization lists are a management tool that lets you easily give the same authorities to a set of objects. When looking at your object model, do not forget to examine the use of authorization lists.

The following authorization lists exist on your system:

ABC123456	APPLICATION OWNER
APP_DEV	Application development authorization list
APPTEST	Application owner
AR_AUTL	Accounts Receivable authorization list
AUTL	
CHURCH	Application owner
CJW	APPLICATION OWNER
HUNGRY3	Application owner
HUNGRY5	Application owner
HUNGRY6	Application owner
JOEY	Application owner
JOHNV	APPLICATION OWNER
JONATHANA	APPLICATION OWNER
LINDAV	APPLICATION OWNER
MORGANV	APPLICATION OWNER
QIWSADM	Client Access/400 Administrators
QOPTSEC	Default Optical Authorization List
QPWFSERVER	
QSVCDRCTR	
QSYLMTJAVA	
QUSEADPAUT	
QZSRVHTTP	
TEST	
TESTAUTL	
TEST123456	APPLICATION OWNER
TRIAL	Application owner
VIDEO	

To determine what objects are secured by each authorization list, run the Display Authorization List Objects (DSPAUTLOBJ) command.

To determine the authorities users have to the authorization list, run the Display Authorization List (DSPAUTL) command.

Return to the description of **Bill of Health** software

File Shares

File shares are created through iSeries Navigator to allow directories within the IFS to be available via your network. Just because a directory has a file share associated with it does not necessarily mean that everyone with access to the network has access to the directory. After the directory (or path) is made available to the network, OS/400 security takes over. So if a directory has been excluded for the general public, only those users with *ALLOBJ or those that have been given explicit authority to the path can access it. Unfortunately, given the default authorities (that is, wide-open nature) of most of the file systems on OS/400, most directories, once made available on the network are available to everyone.

IBM ships some default shares. To see a list of file shares defined for your system, see the SKYSHARES report.

To manage the file shares defined for your system, you must use iSeries Navigator. Open iSeries Navigator, expand the system name, expand file systems, then click on file shares. We recommend that you review the file shares on the system, keeping in mind the underlying authorities (that is, who can access) on the directories and files being shared.

Application Administration

The Host Application part of Application Administration allows administrators to determine who can perform certain OS/400 tasks such as running a communications trace or administering LPARs.

The SKYADMHOST report shows the host applications defined within Application Administration and the users allowed to use these functions. You will want to monitor App Admin defined functions as you would monitor users' access to sensitive or confidential files.

Return to the description of **Bill of Health** software

Section 5: Exit Points

At various places and times throughout OS/400 processing, IBM gives the opportunity for a user-written program to take over the processing for a while. Sometimes the user-written program has the opportunity to determine whether the process should continue or be terminated. Other times, other work is performed on the data that is passed to the exit program. While the use of exit programs in any form is not inherently bad, we recommend that you monitor the use of exit programs and understand what they do. If you have written them yourself, you should periodically review the source code and monitor who has access to modify it. The following sections focus on the exits that allow you to take action when they are called. Let's examine these exits further.

Network Access Points

Some of the popular uses of exit points are probably the ones associated with the various network servers that are available on OS/400 - For example, FTP, ODBC, iSeries Access for Windows data transfer and so on. You register programs with these exits through two commands - Work with Registration Information (WRKREGINF) and Change Network Attributes (CHGNETA).

Object level security is the most fool-proof way to secure your system. However, most systems do not have a robust object security scheme in place or administrators find that the authority requirements to various files are situational. That is, depending on the interface being used, end-users need some amount of authority coming through one interface, such as a green screen application, and another authority when accessing files using another interface such as Microsoft Excel. Exit programs can provide this function. They also provide added protection against unwanted network access. Exit programs also typically offer additional auditing of the use of these interfaces beyond what OS/400 auditing provides. Therefore, the use of exit programs for the network access points is a requirement for many environments. Many third party solutions are available.

You have two choices when using exit programs - create your own or purchase a third party application. We do not recommend creating your own because of the complexities involved. We recommend that you determine your requirements and then look for a third-party solution that meets your needs. Many third-party solutions are available.

- We have examined the server exit points and found that at least one has an exit program defined. If you have installed a third party exit point solution, make sure that you have it fully implemented.

Trigger Programs

Trigger programs while not dangerous in and of themselves, can be a method by which a disgruntled employee introduces a Trojan horse program to your system. You will want to monitor the use of trigger programs on your system and examine their function to make sure they are not being abused.

- You currently have a number of trigger programs on your system. These are listed in the QPSECTRG report.

Return to the description of **Bill of Health** software

Commands

There are two ways that commands can be compromised on OS/400. First, through defining a validity checker program and/or a prompt override program for the command itself. Second, by using the registration facility and defining an exit program for the QIBM_QCA_CHG_COMMAND exit point. If either of these two methods is used on your system, we recommend that you monitor these programs and understand what they do.

Command Exits

Command exit programs were added in V4R5 to allow third-party vendors to manage when certain commands are run. This allows them to avoid putting their library ahead of QSYS to force their command to run (instead of the OS/400 version of the command). Putting libraries ahead of QSYS can be a security risk in some cases, so using this exit is a good alternative. The point in bringing it to your attention is so that you can monitor its use.

- No command exit programs are registered for your system.

Validity Checker and Prompt Override Programs

- There are some commands with either a prompt override program or a validity checker program defined. These commands are listed in the SKYCMDEXIT report.

Network Attributes

Three network attributes need to be monitored - Network Job Action (JOBACN), Client Request Access (PCSACC) and DDM/DRDA Access (DDMACC). The recommendation is to set each of these to *REJECT if you are not using these functions.

JOBACN:

This attribute is currently set to *SEARCH. If remote systems are submitting jobs through SNADS, set this attribute to *SEARCH to explicitly control the job actions.

PCSACC:

This attribute is currently set to *OBJAUT. If you want to use an exit program to control access to iSeries Access functions, set this attribute to *REGFAC.

DDMACC:

This attribute is currently set to *REJECT. If you use DDM, set this attribute to *OBJAUT to have access be controlled via object authority settings. If you are not using DDM, set this attribute to *REJECT.

Return to the description of **Bill of Health** software

Section 6: TCP/IP Security

TCP/IP provides interesting security challenges. You have some configuration options that help manage the security aspects of each server. These are discussed below. Part of TCP/IP security demands that you monitor the users having *IOSYSCFG special authority. (Configuring and managing TCP/IP requires *IOSYSCFG.) *IOSYSCFG was discussed in the User section of this assessment.

Auto-Start Values

The auto-start value determines which servers are started when the Start TCP/IP (STRTCP) command runs. The table below lists the current setting for each server. Please review this table. If you are not using the application, you should not have the server auto-start. If you don't want one of these servers automatically being started, you can change the auto-start parameter using the appropriate CHGxxxA command, where xxx is the server name. For example, CHGFTPA (Change FTP Attributes).

TCP/IP Server	Auto-Start Value
SNMP Agent	*YES
RouteD	*NO
TFTP	*NO
BOOTP	*NO
DDM TCP	*NO
DHCP	*NO
FTP	*NO
TELNET	*YES
SMTP	*YES
LPD	*NO
HTTP	*NO
POP	*NO
REXEC	*NO

Time-Out Values

Some servers allow you to specify a time-out value for the connection. The idea with time-out values is to set them long enough to let normal activity occur, but short enough so that someone cannot take advantage of a connection left unattended. Review these time-out values to ensure they make sense for your usage requirements.

TCP/IP Server	Time-Out Value
TFTP	30
FTP	300
POP	600
REXEC	300

Return to the description of **Bill of Health** software

Users with Authority to STRTCPSVR Command

The *PUBLIC authority for the STRTCPSVR command on this system is *EXCLUDE.

The following users have private authority to this command:

- ALANY *USE
- QPGMR *USE
- QSRV *USE
- QSRVBAS *USE
- QSYSOPR *USE

Several IBM-supplied profiles have *USE authority to this command. We do not recommend that you remove this authority without knowing what will be affected.

The Start TCP/IP Server (STRTCPSVR) command defaults to starting all TCP/IP servers on your system - regardless of their auto-start value. This means that servers could be started that you don't intend to have started.

We encourage you to monitor who has authority to this command.

If you have not already done so, you may also want to change the command defaults to start a server that you know you always want started (rather than all servers).

Return to the description of **Bill of Health** software

Users with Authority to the QATM* Config Files

Configurations for the TCP/IP servers are kept in the QATM* files. You will want to monitor who has authority to those files because anyone with *CHANGE authority or greater can update those configurations. The current authority settings for these files are:

File	User	Authority
QHTTPSVR/QATMHASFT	*PUBLIC	*USE
QHTTPSVR/QATMHINSTA		Same as QHTTPSVR/QATMHASFT
QHTTPSVR/QATMHINSTC		Same as QHTTPSVR/QATMHASFT
QHTTPSVR/QATMHTTP		Same as QHTTPSVR/QATMHASFT
QHTTPSVR/QATMHTTPC		Same as QHTTPSVR/QATMHASFT
QHTTPSVR/QATMHTTPI	*PUBLIC QTMHHTTP	*EXCLUDE *USE
QTCP/QATMADRLST		Same as QHTTPSVR/QATMHASFT
QTCP/QATMFTP		Same as QHTTPSVR/QATMHASFT
QTCP/QATMFTRLST		Same as QHTTPSVR/QATMHASFT
QTCP/QATMIFCLST		Same as QHTTPSVR/QATMHASFT
QTCP/QATMLPD		Same as QHTTPSVR/QATMHASFT
QTCP/QATMPINC		Same as QHTTPSVR/QATMHASFT
QTCP/QATMPOPA		Same as QHTTPSVR/QATMHASFT
QTCP/QATMRXC		Same as QHTTPSVR/QATMHASFT
QTCP/QATMSMTLA	*PUBLIC	USER DEF
QTCP/QATMSMTP		Same as QHTTPSVR/QATMHASFT
QTCP/QATMSMTPA		Same as QHTTPSVR/QATMHASFT
QTCP/QATMTCPWRK		Same as QHTTPSVR/QATMHASFT
QTCP/QATMTELN		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMADRLST		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMFTP		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMFTRLST		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHASFT		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHELP		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHINSTA		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHINSTC		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHTTP		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHTTPA		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMHTTPC		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMIFCLST		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMLPD		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMPOPA		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMRXC		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMSMTLA		Same as QTCP/QATMSMTLA
QUSRSYS/QATMSMTP		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMSMTPA		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMTELN		Same as QHTTPSVR/QATMHASFT
QUSRSYS/QATMWSG		Same as QHTTPSVR/QATMHASFT

Return to the description of **Bill of Health** software

Port Restrictions

Another approach to controlling what network interfaces are used is to use port restrictions. If you know a port is not going to be used, you can create a temporary profile, secure the port using the Work with TCP/IP Port Restrictions option off the Configure TCP/IP menu and then delete the profile. Or, if you know a sockets program is going to run on a particular port under a specific user profile, you can secure the port and specify that profile. Then all sockets programs coming in on that port will run as that particular user.

Section 7: Adopted Authority

Adopted authority is a way that you can temporarily give authority away. Adopted authority is an attribute of a program - the user profile attribute. When the program is defined as User Profile *OWNER that means that when a user runs that program, the authority checked by OS/400 will be first the authority of the user running the program and then the authority of the owner of the program. Adopted authority gives application owners great flexibility in how to authorize and secure objects owned and accessed by the application. However, this flexibility can also be abused and you need to monitor programs that adopt authority - especially the authority of powerful users.

The SKYADPAUT report lists the objects that adopt *ALLOBJ special authority. The intent of these objects should be understood and monitored to make sure no one is abusing the use of adopted authority.

Return to the description of **Bill of Health** software

Section 8: Miscellaneous Security Topics

Job and Output Queues

The security configuration settings for output and job queues are often overlooked. However, depending on their settings, they can be either secure or wide open. The SKYOUTQAUT report lists output queues and authorities, and the SKYJOBQAUT report lists job queues and authorities. If you are unfamiliar with these settings and what they mean, the book Expert's Guide to OS/400 and i5/OS Security by Carol Woodbury and Patrick Botz has a chapter devoted to the topic along with a table explaining the attribute and whether or not it is affected by whether the user has *JOBCTL or *SPLCTL special authority.

The other considerations for queue security is who has either *JOBCTL or *SPLCTL special authorities. These special authorities can override the queue's security settings. A discussion of these special authorities is in the User section of this assessment.

Job Descriptions

Job descriptions can be configured to name a user profile. When the job description is used, the job runs under the authority of the user named in the job description. This is not inherently "bad" but these should be monitored.

However, if your system is running at security level 30, job descriptions that name a user profile present a major exposure for your system. That's because at security level 20 or 30, a user only needs authority to the job description to use it. Once authorized to the job description any user can submit a job and run it as a powerful profile. At security level 40 and above, the user needs authority to both the job description and the user profile named in the job description. (This is one of the benefits of going to security level 40 and above.)

> Job descriptions exist that name a user profile. These job descriptions are available for public use. They are listed in the SKYJOBDUSR report. If you are at security level 20 or 30, you have a major exposure.

Subsystem Descriptions

Subsystems can be configured to have all jobs run under a particular profile. This is not inherently "bad" but you should be aware that it is happening and decide if it is appropriate.

> You currently have subsystem descriptions that have communication entries that name a user profile. These are listed in the SKYSBSDUSR report.

User Objects in QSYS

When someone with evil intent wants to harm your system, they will sometimes try to "hide" a rogue program or other object in the QSYS library, believing that it will not come under scrutiny because some administrators assume that everything in QSYS comes from IBM. The SKYQSYSUSR report lists the user created objects in QSYS. You will want to review this report to understand these objects and ensure they are appropriate.

Return to the description of **Bill of Health** software

Management Central

Management Central allows you to define commands that run on the target system after certain functions are run. These are called 'post commands'. These commands, along with remote command definitions, are stored in the file QAYPSDFN in library QUSRSYS. You will want to monitor who has authority to this file to ensure it is not inappropriately changed. The current authorities are:

- *PUBLIC *USE
- QSYS *ALL

Unused Products and Libraries

Products and libraries which are no longer in use should be removed from your system. Why take up the storage space with unused objects, but more importantly, why leave unused products and libraries on your system that could pose security exposures or issues? If it resides on your system, you must consider the security issues surrounding it and the security ramifications of its residing on your system. You have too much to do and your time is too valuable to spend time securing something that is not used.

Libraries do not record the last used date, so to determine when a library was last used, you must check the objects in that library. Since changing an object does not always count as using an object, you must find the latest used or changed date from the objects in the library.

Before removing libraries, you may want to do the following:

- Set up object auditing on these libraries. This will show you exactly when and who is using these libraries.
- Set the *PUBLIC authority of these libraries to *EXCLUDE. If someone can't access the library and needs to, they'll call! (Remember that everyone with *ALLOBJ special authority will still be able to access the library even if it is set to *EXCLUDE).
- Save off the old libraries - just in case.
- Finally, delete the libraries if there is no evidence of use.

Check Object Integrity (CHKOBJITG)

We highly recommend that you run this command. The CHKOBJITG command has been available since V3R1 but is rarely used. It will check the integrity of OS/400 and report if any objects have been tampered with - it cannot detect all methods of tampering, but is still worth running. Beginning in V5R1, OS/400 is digitally signed. That way, you can know that OS/400 programs have not been altered since leaving the IBM distribution plant or since receiving a PTF for a program. You can run the CHKOBJITG command to verify OS/400's signatures as well.

We recommend that you run the CHKOBJITG command and at least check all of the objects owned by QSYS. This command can be very long running. We recommend that you run this command when there is the least amount of system activity and the least number of signed on users so that it does no affect the performance of your daily work.

Return to the description of **Bill of Health** software

Section 9: Other Considerations

The security of the iSeries is only one part of an organization's security implementation. The following sections describe other issues that need to be considered.

Security Policy

An organization's security policy is actually the first issue that needs to be addressed - even before securing a particular operating system. If you don't know what your company's overall security policy is, you will not be able to make appropriate decisions regarding the recommendations contained in this document.

Security policies need to be reviewed and updated on a regular basis.

Physical Security

One area that is often implemented, but is often out of date or not enforced, is physical security. This is not meant to be a comprehensive guide for physical security because needs will vary greatly depending on your company's specific requirements.

- Larger iSeries or AS/400 systems come with a key stick. Removing the key from the system affords some amount of security. Assuming that it wasn't removed when the key was in "manual" mode, no one will be able to force DST, force an IPL or load their own tapes. This is quite a lot of protection with a simple removal of a key. Note that not all models come with a key stick and it varies release to release.
- Cipher locks. Often a machine room will be secured with a cipher lock. However, the combinations for those locks are rarely if ever changed. This should be part of security policy.
- Sign-in sheets. Machine rooms often have a sign-in sheet for visitors. However, they are rarely used and even more rarely reviewed. This should also be part of the security policy.
- Laptop computers. These are high theft items. Some organizations recognize this and require them to be locked to some immovable object when left unattended in an office.
- Screen savers. While not fool-proof, a devious person will look for the easiest access method. A screen saver with a password will require the person to guess the password before using the unattended workstation.
- Handheld devices. With the proliferation of handhelds and cell phones and the applications now available for them, you need to consider the security of corporate data residing on these devices. Handhelds are high theft items and are also very easy to misplace.

Disaster Recovery

Another area to investigate is disaster recovery. Here are some questions to ask yourself:

- Are systems backed up?
  - How often?
  - Where is the backup media stored (is it secure)?
- When was the last time the disaster recovery plan was reviewed?
- Has the disaster recovery plan been tested?

Return to the description of **Bill of Health** software

Questions ?

It would be a privilege to answer any technical questions about **Bill of Health** software. Here's Unbeaten Path International's contact information:

Toll free North America: (888) 874-8008
International: +(262) 681-3151
Send us an e-mail (click **here**)

Bill of Health Navigation -- click on purple links

Return to the description of **Bill of Health** software

Look at very detailed **Bill of Health product benefits**

Other **security compliance products** from Unbeaten Path

Index to **IT security requirements**

Unbeaten Path®