



# Best Practices for iSeries Security

## White Paper

March 8, 2003

---

### Contents

<b>Information Is Your Most Valuable Asset .....</b>	<b>1</b>
<b>System-Level Security .....</b>	<b>2</b>
<b>User-Level Security.....</b>	<b>3</b>
<b>Resource-Level Security .....</b>	<b>6</b>
<b>Conclusion .....</b>	<b>9</b>
<b>Best Practice Security Matrix ..</b>	<b>10</b>

Everyone from management to users should be concerned with information security. System security protects the iSeries (AS/400) and sensitive business information from both intentional and unintentional security breaches and threats. In today's computing environment, new security problems emerge on a daily basis. With the basic security issues addressed, you have more time to devote to specific and proactive security improvement endeavors.

This document provides your corporate iSeries security personnel with a basic understanding of OS/400 system security. This document also helps you enhance your overall security plan for ongoing risk reduction and security improvement. Several basic OS/400 best practices can significantly reduce security exposures in all environments. These best practices and basic system security and planning provide a quick and easy path to increasing your peace of mind.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

**© 1995-2003 NetIQ Corporation, all rights reserved.**

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Check Point, FireWall-1, and Provider-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

ActiveAgent, ActiveAnalytics, ActiveAudit, ActiveKnowledge, ActiveReporting, ADcheck, AppAnalyzer, Application Scanner, AppManager, AuditTrack, AutoSync, Chariot, ClusterTrends, CommerceTrends, Configuration Assessor, ConfigurationManager, the cube logo design, DBTrends, DiagnosticManager, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, End2End, Exchange Administrator, Exchange Migrator, Extended Management Pack, FastTrends, File Security Administrator, Firewall Appliance Analyzer, Firewall Reporting Center, Firewall Suite, Ganymede, the Ganymede logo, Ganymede Software, Group Policy Administrator, Intergreat, Knowledge Scripts, Migrate.Monitor.Manage, Mission Critical Software, Mission Critical Software for E-Business, the Mission Critical Software logo, MP3check, NetIQ, the NetIQ logo, the NetIQ Partner Network design, NetWare Migrator, OnePoint, the OnePoint logo, Operations Manager, PentaSafe, PSAudit, PSDetect, PSPasswordManager, PSSecure, Qcheck, RecoveryManager, Security Analyzer, Security Manager, Server Consolidator, SQLcheck, VigilEnt, Visitor Mean Business, Vivinet, W logo, WebTrends, WebTrends Analysis Suite, WebTrends for Content Management Systems, WebTrends Intelligence Suite, WebTrends Live, WebTrends Log Analyzer, WebTrends Network, WebTrends OLAP Manager, WebTrends Report Designer, WebTrends Reporting Center, WebTrends Warehouse, Work Smarter, WWWorld, and XMP are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other jurisdictions. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

---

# Information Is Your Most Valuable Asset

The explosion of information technologies and business-to-business data sharing over the past 10 years has made it increasingly clear that information has become the most valuable asset for corporations today. This asset is more valuable than once thought because it represents a corporation's intellectual property or proprietary secrets, financial transactions, and even their competitive advantage within the market space. As a result of the expansion of internal system connectivity with the Internet, corporate intranets, new client-server technology, and the implementation of heterogeneous distributed systems, information is more at risk than ever before, and the risks continue to increase. Unfortunately, most corporations' information security programs have failed to keep up with this rapid technology evolution and the increased security required to protect this asset.

The protection of information involves both external, or perimeter security controls, and internal access controls. Most companies today are protected from outside threats with firewall technology. However, the security *buck* typically stops there. Even with recent highly publicized security incidents and the costs associated with these breaches, internal security risks continue to receive far less than their fair share of the security budget. Statistics continually show that over 80% of all serious security violations today come from inside the organization. In fact, it is the employee at the desktop who poses, often unwittingly, the greatest security risk. The following list highlights several common examples of internal security risks:

- When someone walks away from their desk and leaves the computer on
- When someone writes a system password on a piece of paper and tapes it to the monitor
- When a user *surfs* the internal network or main application systems

The first two examples are *people* problems that are difficult to reign in and are best addressed by implementing a sound policy and security awareness program. The third example is a *system* problem that can be controlled by implementing system security standards and periodically reviewing those standards across all platforms.

Everyone from management to users should be concerned with information security. System security protects the iSeries (AS/400) and sensitive business information from both intentional and unintentional security breaches and threats. In today's computing environment, new security problems emerge on a daily basis. With the basic security issues addressed, the organization will have more time to devote to more specific and proactive security improvement endeavors. Although OS/400 security within the corporate network is addressed in particular, the best practices outlined in this document must be combined with security best practices for each component (other operating systems, databases, and applications) within the network. Today's business landscape requires that the entire computing environment be secured.

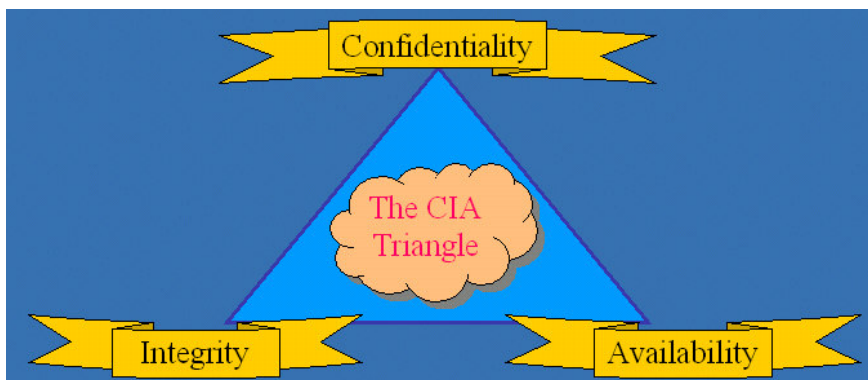
This document provides your key corporate security officers and their staff with a basic understanding of OS/400 system security. This document also helps you enhance your overall security plan for ongoing risk reduction and security improvement. There are many system parameters that can be customized based on different security environment requirements and needs. However, several basic OS/400 best practices can significantly reduce security exposures in all environments. Basic system security and planning provides a quick and easy path to increasing your peace of mind.

---

## System-Level Security

The system security for iSeries is built into the operating system (OS/400) licensed program. IBM designed it this way to take advantage of the architectural enhancements that went into the creation of the OS/400 series of machines. This design gives all the OS/400 functions, such as displays, commands, and terminology, a consistent look and feel. In addition, since the security layer is not a separate software layer, it is much more difficult to bypass, and it has minimal impact on system performance.

The intent of good security for any computing system is to protect the confidentiality, integrity, and availability of the information that is stored within. **Confidentiality** of information ensures that only those users with a legitimate *need-to-know* as part of their job duties can access certain information and that there is minimal risk of disclosure. **Integrity** of information ensures that the information on the system is accurate and has not been manipulated by unauthorized parties. Most companies make major financial and business decisions based upon information extracted from internal systems. Therefore, it is imperative that this information can be trusted to represent what the reports say it represents. **Availability** of information ensures that your systems have been protected from the risk of damage to both the information on the system and to the system itself. Business activity, public reputation, and the financial bottom line can be seriously and adversely impacted if information is rendered unusable by either accidental or deliberate actions.



In OS/400, general security at the system level is controlled by system value settings. The iSeries is shipped with these values set to certain defaults. These defaults need to be reviewed and appropriately modified by an organization prior to bringing the system online in a production environment. There are many system values and many combinations of value settings that can create critical interdependencies not immediately obvious at the outset. System values apply to everyone using the system, unless something more specific, such as a user profile parameter, overrides the system value. Of course, the desired effect when modifying the system values is to increase security without increasing overhead or preventing your users from getting their jobs done. Security staff members must be cautious when attempting to change any of these settings.

## Securing the iSeries at the System Level

The following best practices highlight key ways to secure your iSeries at the system level:

- Ensure that the system is in a climate-controlled environment and that the key lock feature is used. Do not leave the key in the system.
- Maintain a log of personnel movement in and out of the data center.
- Ensure that the system has adequate backup power (UPS) in the event of a power interruption.

- Verify that the system security level is set to a minimum of 40 in order to activate resource security (object authority checking) and integrity checking through the system value (*QSECURITY = 40*).
- Enable system auditing through the system value to record system events and user/object events (*QAUDCTL = \*OBJAUD and \*AUDLVL*).
- Make sure that the system does not shut down if auditing fails, unless the system is C2/DOD regulated (*QAUDENDACN = \*NOTIFY*).
- Set the auditing system value to track security changes, object access, and authority failures (*QAUDLVL = \*AUTFAIL, \*DELETE, \*OBJMGT, \*PGMFAIL, \*SAVRST, and \*SECURITY*).
- Verify the appropriate settings to be sure that new objects do not allow access to all system users by default (*QCRTAUT = \*EXCLUDE*).
- Use the system values to control regular and powerful user access to system sessions and assist in the handling of inactive user sessions (*QLMTDEVSSN, QLMTSECOFR, QINACTITV, and QINACTMSGQ*).
- Properly configure the additional user access system values that include invalid sign-on controls and user password parameter *settings* (*All of the QPWD\* and QMAX\* system values*).
- Ensure that your system is protected from unauthorized remote sessions and system restarts (*QRMTSIGN and QRMTIPL*).

---

## User-Level Security

User security in OS/400 is based upon user profiles. A user profile uniquely identifies each user that accesses the system and also specifies which system objects the user is allowed to access. The user profile also contains information about the objects owned by the user and all of the private authorities for those objects.

The use of individual user profiles is the cornerstone to a proper security strategy. Auditing success requires that you are able to identify system actions and accesses down to the individual object and user who performed the action. OS/400 is very successful at tracking system activity and maintaining the proper audit trail for both users and objects.

The level of success for gathering and reporting this information depends greatly on whether the user data or user naming convention bears meaning. If user profiles are not traceable to a specific individual because they are generic or are in a format that does not uniquely identify the user, the time needed to derive the required information can be greatly increased. However, unique does not imply that the profile should simply be an abstract of the user's actual name, such as JONESR for Robert Jones. Name-based profiles are easily guessed and often just as easy to hack. On the other hand, while using seemingly meaningless profiles like TR85GH4Q decreases the likelihood of profile guessing, the administrative overhead is greatly increased by having to track whom each profile belongs to in a separate file or location. Calls to the Help Desk are likely to increase when users cannot remember their user profile, let alone their password.

The best format for profiles is one that has meaning to the system administrators, is unique to the system, and remains unique even when employee turnover is considered. For example, a multi-office company can begin each profile with an alphabetic character to identify geographic location, followed by two digits to identify status (perm or temp), and then four digits to identify the individual user (employee number). In this scheme, using 00 for permanent employees and 99 for temporary employees, a company with offices in Atlanta, Boston, and Phoenix could have profiles similar to the following examples.

Profile	Employee Description
A000257	Atlanta, permanent, Employee# 0257
B001322	Boston, permanent, Employee# 1322
P990033	Phoenix, temporary, Temp Employee# 0033

Using this scheme, an administrator can quickly identify the location and status of the user. In addition, since most companies do not re-use employee numbers, these profiles remain unique long after an employee leaves the company. In a four-digit employee number scheme, as many as 10,000 employees can *go through the turnstiles* before the risk of repeating an employee number arises. A five-digit employee number yields 100,000 unique combinations.

Regular review of user profiles and their settings is paramount to a pro-active security program. User profiles are one of the first things auditors review when assessing the security health of your systems.

## Securing the iSeries at the User Level

The following best practices highlight key ways to secure your iSeries at the user level:

- Create new profiles based on job function, not by simply copying an existing profile.
- Use a unique password and set it to expire for new profiles. Verify proper password expiration intervals for all profiles on a periodic basis.
- Properly restrict general users by ensuring that profiles are in the correct user class, have class appropriate special authorities, and do not have command-line access.
- Make sure that users access the system through application or in-house menus and not the IBM main menu.
- Verify that the public authority to profile objects in library QSYS is set to \*EXCLUDE.
- Be sure that group profiles for general users do not own production objects.
- All group profiles should have \*NONE for the password since they do not need to sign-on.
- Be sure to use group profiles for authorization instead of individual profiles whenever possible.
- Verify that the passwords for all IBM-supplied user profiles have been changed from their defaults.

## Changing Passwords for Dedicated Service Tools User IDs

Dedicated Service Tools (DST) is a set of tools for performing system tests and service outside the normal operating system. Four levels of DST are available, each with a user ID and password.

- QSECOFR
- QSRV
- 22222222
- 11111111

These user IDs and passwords are shipped with default values and are the same for every iSeries system. It is vital that they are changed to protect the security of the system. You should regularly report on DST password resets to help determine whether they have been changed back to the defaults. This process can also identify potential system abuse.

You cannot change DST user IDs and passwords with the CHGUSRPRF command. You can change them in only two ways:

- Using the Change Dedicated Service Tools (QSYCHGDS) API
- Through the DST function itself

You can change the DST passwords using either the Manual Mode Procedure or the Manual IPL Procedure. The Manual Mode Procedure can be done while the system is operational. This procedure does not require you to IPL the system to change the password. Therefore, you can use this procedure in production environments where the maintenance window is small. For more information about performing the Manual IPL Procedure, see the iSeries Security Reference (SC41-5302-05)

**Note:**

Make sure the DST and QSECOFR user IDs and passwords are confidentially recorded and kept in a safe place. If the QSECOFR profile becomes disabled, you can always sign on with it at the system console, as long as you know the password. However, if both the QSECOFR and DST security user ID passwords are lost or forgotten, you may need to install the operating system again to recover them.

**To change a DST password using the manual mode procedure:**

1. Put the system in manual mode.
2. Enter '21' in the indicator lights and press Enter.
3. Sign-on to the DST sign-on screen at the system console to make the changes.
4. Return the system to normal mode when completed and engage the key lock.

---

## Resource-Level Security

Resource security on the iSeries system provides the ability to define who can access objects and how those objects can be used. This security is provided through authorities.

Authority	Description
Object authority	Provides the ability to access an object. This authority includes several functions, such as changing, saving, or deleting the object. Files, programs, and libraries are the most common objects requiring security protection, but you can define specific authority for any object on the system.
Data authority	Provides the ability to access the contents of an object. This authority includes several actions, such as reading, adding, updating, or deleting records. You can specify detailed data authorities, or you can use the following system-defined subsets of authorities: *ALL, *CHANGE, *USE, and *EXCLUDE.

The most common data authorization scheme is known as *need-to-know*. If a user requires access to a particular object or file in the course of performing his or her job functions, then there is a need to know what that data is.

For maintenance purposes, you should primarily use **group authority** instead of **private authority**. In most cases, many users share the function that requires access to certain files. Managing private authority can quickly become time intensive as the number of users and objects on the system increases. Therefore, you should reserve private authority for special circumstances.

## Object Security Areas to Consider

The basic concepts of object security are presented in the following sections along with the best practice implementation of those concepts. However, resource security is much too involved to permit addressing all the details in this paper. The NetIQ suite of iSeries security products can ease the maintenance and administration nightmare associated with the thousands of objects that exist on the typical iSeries system. The PSAudit and PSSecure products address all areas of object security discussed in the following sections.

### Authorization Lists

You can group users with similar security needs in an authorization list. Authority for objects can then be granted to the list rather than to individual users, most often using group profiles. These lists are very useful for security at the library level. Within the authorization list, individual users can have different authorities. However, the reason for using group profiles is to reduce the management of specific object authorities and private user authorities associated with granting direct user object access.

## Object Ownership

Every object on the system has an owner, and objects can be owned by individual or group profiles. Proper assignment of object ownership helps in the management of applications and data. It is very important to be sure that the QSECOFR profile does not own production objects, since this all-powerful profile should be used only for high-level security maintenance and emergencies. In addition, access to objects owned by QSECOFR requires that general users either have improperly high access or can run programs that adopt QSECOFR authority. A good strategy is one that distributes object ownership between two profiles:

- One profile for production objects and libraries, such as PRODOBJOWN
- One profile for test/development objects and libraries, such as DEVOBJOWN.

The owner of an object has \*ALL authority to that object. Therefore, ownership of an object by a group profile is strongly discouraged.

## Library Authority

Most production systems are configured and grouped by application. Each application has specific programs and files that are vital to its function. These files and programs typically are grouped in libraries because they have similar protection requirements. Restricting access at the library level is often much easier than restricting access to each individual object. For most environments, public authority to libraries should not exceed \*USE.

## Directory Authority

You can manage directory authority in the same manner as library authority. Group objects in a directory and secure the directory rather than securing each individual object.

## Object Authority

In the cases where restricting access at the library or directory level is not specific enough, you can restrict a user's authority to access individual objects at the object level with additional authorization list or user profile entries. However, managing authority at the object level requires more time and resources.

## Public Authority

You can define each object on the system as to what kind of access is available for any system user who does not have any other authority to the object. This access is known as public authority. Public authority (\*PUBLIC) is often the most effective means for securing files and programs and it also provides for good overall system performance since the authority resolution steps are reduced.

## Adopted Authority

Adopted authority adds the authority of a program owner to the authority of the user running the program. Adopted authority can be useful for certain situations, but you should use adopted authority only when required. Programs that are owned by powerful profiles, such as QSECOFR or some other \*ALLOBJ profile, should not be configured to adopt authority. These types of programs should be closely monitored and reviewed on a regular basis.

## Managing the Holes Associated with Exit Points

Today's computing environment is filled with corporate networks that have many different operating systems working in concert to provide a company with the necessary power to use their information to their best possible advantage. However, along with this heterogeneous mix comes an additional security risk that is often overlooked by iSeries administrators and other IT managers: Remote access through exit points.

The iSeries was designed before the ubiquitous local area networks were the staple of corporate computing infrastructures. Since the iSeries was designed as an isolated computing platform, security controls for remote client access tools were not incorporated within the basic OS/400 security methodology. Because of this design, the best way to secure communications and actions within client access is by implementing exit point controls or programs. **Exit points** are the points within a process where OS/400 hands over control of the process to an external function or program, such as when accessing a network information repository like a Windows NT domain or Unix system. Unfortunately, there is still very little discussion of exit points within existing IBM documentation, nor is their readily available information on designing exit point controls.



The biggest risk associated with the lack of exit point control is that a user can often bypass menu and group authorization object controls to access OS/400-resident data directly from a networked PC. Anyone with \*USE authority to an object can potentially access these files and manipulate the data using widely known utilities, such as FTP. The standard OS/400 user controls, such as restricting access to command lines, file management commands, or the client access commands themselves, do not prevent object access through client access. The implementation of exit programs for logging remote system transactions and controlling requests is imperative to adequately secure system resources from common actions, such as file transfers (FTP or Client Access), log on outside of normal channels (Telnet), and the use of remote commands. This aspect of OS/400 security, including the development of exit programs, is very difficult to manage, even for the most seasoned security practitioner or programmer. Fortunately, NetIQ provides the tools to make this important task very easy within the PSSecure product.

## Securing the iSeries at the Resource Level

The following best practices highlight key ways to secure your iSeries at the resource (object) level:

- Use authorization lists whenever possible, preferably with group profile entries instead of individual profiles.
- Verify that QSECOFR does not own any objects and continually monitor for this vulnerability.
- Create object ownership profiles that do nothing more than own production and test objects (such that they cannot even sign-on to the system).
- Whenever possible, restrict access at the library and directory level instead of at the object level. Make sure that the public authority to library and directory objects is no higher than \*USE.

- As with libraries, authorization lists are preferred over individual profile entries for object authorities.
- Whenever possible, rely on \*PUBLIC authority for securing any system object to minimize administrative work, as well as the system authority resolution time.
- Monitor for programs that adopt authority, especially those programs that adopt the authority of powerful users, such as QSECOFR.
- Use exit programs to control remote access to your iSeries systems and information.
- Use WRKREGINF (Work with Registration Info) to control individual exit points through exit programs instead of using one exit program for the PCSACC network attribute.
- Ensure that your exit programs give you the flexibility to be simultaneously broad and specific when managing remote transactions. You should use the object authority approach instead of transaction memorization.

---

## Conclusion

Your organization's information is only as secure as its weakest link. Keeping basic security concepts in mind as the system evolves due to user and application changes will enhance the security for every type of computing environment. Routine check-ups of the security health of the system are vital to maintaining the desired level of protection as changes occur. It is even more important to understand the need to implement basic security practices for *all* systems across the enterprise.

All the necessary auditing and security tasks can be managed with automation tools, such as PSAudit and PSSecure from NetIQ Corporation. These NetIQ products take the guesswork out of OS/400 security administration by providing a user-friendly interface for the management of the many topics and issues discussed in this document. For more information about the VigilEnt Security Agent for iSeries solution, see [www.netiq.com/products/vsa/series.asp](http://www.netiq.com/products/vsa/series.asp).

# Best Practice Security Matrix

The following table provides high-level security and audit best practices. Using this table, you can assess your current procedures against the best practice guidelines and identify several ways NetIQ products can help you secure your iSeries environment.

Best Practice Areas	Self Assessment and Ways NetIQ Can Help
<p><b>System Security – System Values</b></p> <ul style="list-style-type: none"> <li>• Verify that the system security level is set to a minimum of 40.</li> <li>• Turn on system and object level auditing.</li> <li>• Ensure that the system will not shut down if auditing fails.</li> <li>• Verify that the proper audit settings are set to track system security changes, program failures, and authority failures.</li> <li>• Make sure that the default public authority for new system objects is not too lenient.</li> <li>• Ensure that the appropriate parameters are in place for user inactivity monitoring and user password controls.</li> <li>• Verify that the system is protected from unauthorized remote activity.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>The Security Recommendations report in the PSAudit product identifies whether your system values are out of compliance with best practices and/or your custom security thresholds.</p> <p>The Security Check-up Configurator guides you through the process of setting system level security parameters, as well as scheduling security audit reports according to your organizational needs.</p> <p>The PSAudit product provides numerous reports that address all these areas. You can use custom filters to tailor each report for your specific needs.</p>
<p><b>System Security – Physical</b></p> <ul style="list-style-type: none"> <li>• Use appropriate physical and environmental controls.</li> <li>• Log all data center activity.</li> <li>• Ensure that backup power is available.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>Physical security practices cannot be monitored or controlled by software. On-going physical security is up to the people involved in facilities and systems management. However, VigilEnt Policy Center allows you to publish your physical security policies and test personnel to ensure they remain current on your latest policies.</p>

Best Practice Areas	Self Assessment and Ways NetIQ Can Help
<p><b>User Security – Setup Process</b></p> <ul style="list-style-type: none"> <li>• Use an appropriate profile naming scheme to maintain viable user accountability on the system.</li> <li>• Create new user profiles based on job function or <i>need-to-know</i>.</li> <li>• Verify proper initial profile settings, such as the password being set to expire on first use.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>Ultimately, the user profile format is up to the organization. However, the Profile and Password Management module of the PSSecure product can help enforce profile format and creation standards through profile templates.</p> <p>The PSAudit product contains many reports related directly to password security, such as a report that shows when a password itself is the same as the profile.</p>
<p><b>User Security – DST Passwords</b></p> <ul style="list-style-type: none"> <li>• Change the DST (Dedicated Service Tools) passwords to clear out default settings.</li> <li>• Ensure that the new passwords are recorded and kept in a safe place.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>The DST SecOfr Password Reset report in the PSAudit product can show whether the DST passwords were changed. You can schedule this report to run periodically and help ensure that the DST profiles are not modified.</p>
<p><b>Resource Security</b></p> <ul style="list-style-type: none"> <li>• Use authorization lists for securing objects instead of direct individual user authority, especially at the library level.</li> <li>• Ensure that a sound object ownership strategy is in place so that powerful profiles do not own production objects.</li> <li>• Verify that the public authority level for library and directory objects is no higher than *USE.</li> <li>• Monitor for authority adopting programs, especially those that adopt QSECOFR authority.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>The PSAudit product provides multiple reports that present object details, including authority information. You can schedule these reports, as well as use customized report parameters to filter the data for a specific user according to your needs.</p> <p>Object Authority Management in the PSSecure product enables you to create templates that specify object ownership and authorization according to your standards.</p>

Best Practice Areas	Self Assessment and Ways NetIQ Can Help
<p><b>Resource Security – Exit Points</b></p> <ul style="list-style-type: none"> <li>• Use exit point controls (exit programs) to ensure that there are minimal risks associated with remote access to your AS/400.</li> <li>• Implement exit programs through WRKREGINF instead of changing the PCSACC network attribute to *REJECT or attempting to use a single program for all requests.</li> </ul>	<p><b><i>How are you addressing this area today?</i></b></p> <hr/> <p><b><i>How can NetIQ help?</i></b></p> <p>With the exit programs already built-in, the PSSecure product can simplify the job of controlling exit point risks. The menu-driven application simplifies the collection and analysis of exit point-related transactions. Once the desired exit programs are installed, the remote request management (RRM) process is activated and the audit of these transactions is in place for ongoing review, reporting, and continued security updates.</p>