



April 19, 2010

ROSS PHILO
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

THOMAS G. DAY
SENIOR VICE PRESIDENT, INTELLIGENT MAIL AND ADDRESS QUALITY

SUBJECT: Audit Report - Network Security Assessment of the National
Customer Support Center (Report Number IS-AR-10-007)

This report presents the results of our self-initiated network security assessment of the National Customer Support Center (NCSC) (Project Number 09RG030IS000). Our objective was to determine whether network security controls implemented at the NCSC and associated sites adequately provide for the confidentiality, integrity, and availability of U.S. Postal Service information resources. This audit addresses operational risk. See [Appendix A](#) for additional information about this audit.

The NCSC supports the Intelligent Mail program and Address Quality function for the Postal Service. The facility's mission is to support the Postal Service with an address quality database, a change of address system, and customer address products to facilitate the timely and cost-effective coding, sorting, and delivery of the mail.

Conclusion

Network security controls in place at the NCSC may not adequately provide for the confidentiality, integrity, and availability of Postal Service information resources. Management can improve information security by implementing patch and configuration management processes, upgrading and patching database software, and reviewing server configurations to ensure compliance with Postal Service hardening standards. Based on our audit results, management began remediating patch and configuration-related vulnerabilities during the audit.

Operating System and Database Server Vulnerabilities

Administrators did not patch consistently or configure correctly the operating system and database environments. We [REDACTED]

[REDACTED] The operating system vulnerabilities existed, because administrators relied on ineffective vulnerability assessments rather than a

proactive patch and configuration management process to identify and remediate missing patches and configuration issues. The database vulnerabilities existed, because administrators did not upgrade to a version of the Oracle® database software required to apply the patches. [REDACTED]

[REDACTED] See

[Appendix B](#) for our detailed analysis of this topic.

We recommend the senior vice president, Intelligent Mail and Address Quality, direct the manager, Address Management, to:

1. Utilize the Postal Service patch and configuration management processes to identify and remediate missing patches and configuration issues.
2. Upgrade the Oracle database software and remediate the patch-related vulnerabilities.
3. Periodically review server configurations to ensure servers comply with applicable Postal Service hardening standards.

Web Server Vulnerabilities

Administrators did not harden² a publicly accessible web server that supports [REDACTED]. Specifically, we identified one [REDACTED]. Administrators did not identify these vulnerabilities, because they did not configure the vulnerability management software to [REDACTED]. According to Postal Service policy,⁶ information resources supported by networking must be hardened to meet or exceed the requirements documented in Postal Service hardening standards specific to each platform. [REDACTED]

[REDACTED]

¹ [REDACTED]

² Hardening refers to the process of implementing additional software and hardware security controls.

³ The Postal Service and its mailers use MITS. It contains mail-related products and service information as well as a mailer feedback tool.

⁴ [REDACTED]
⁵ [REDACTED]

⁶ Handbook AS-805, *Information Security*, Section 11-3.6, Implementing Hardening Standards, dated November 2009.

⁷ [REDACTED]

⁸ Handbook AS-805, Section 10-3.1 (j), Software Safeguards.

[REDACTED] This data includes information related to [REDACTED]

[REDACTED]. Prompted by our audit, administrators modified the application to remove the [REDACTED]. Therefore, we are not making a recommendation to remediate those specific issues.

We recommend the senior vice president, Intelligent Mail and Address Quality, direct the manager, Address Management, to:

4. Configure existing vulnerability management software to assess [REDACTED] as required.

Management's Comments

Management agreed with the findings and recommendations. In response to recommendations 1 through 3, management will coordinate with the Corporate Information Security Office (CISO) to develop and implement a patch management process and standardize NCSC systems with Postal Service hardening standards. Management implemented a formal patch and configuration review process to ensure all servers continue to comply with Postal Service requirements. This policy is the interim methodology intended to keep NCSC systems at the appropriate revision level and compliant with Postal Service hardening standards. The target completion date for recommendations 1 and 3 is September 30, 2010. The target completion date for recommendation 2 is September 1, 2010.

In response to recommendation 4, management coordinated with the CISO to verify the configuration of the vulnerability management software to ensure it performs web server assessments according to Postal Service policy. Management completed its proposed action and requests closure of this recommendation. See [Appendix C](#) for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and their corrective actions should resolve the issues identified in the report.

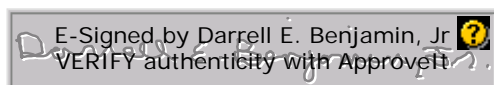
Other Matters – Network Security

We identified [REDACTED] that could allow an unauthorized person to access the NCSC network. When notified, management took corrective action to [REDACTED]

██████████. Management also updated employee departure procedures to reflect the requirement to deactivate network connections when an employee or contractor departs the organization. As a result, we are not making a recommendation to address this network security issue.

The OIG considers recommendation 1 significant and, therefore, requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective action is completed. This recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Frances E. Cain, director, Information Technology, or me at 703-248-2100.



Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: John T. Edgar
Deborah J. Judy
Charles L. McGann
James D. Wilson
Sally K. Haring

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The NCSC, located in [REDACTED], is a customer support and software engineering facility that supports the Intelligent Mail program and Address Quality function for the Postal Service. Specifically, the NCSC supports applications that facilitate the National Change of Address and Address Information System Product Fulfillment systems. The facility's mission is to support the Postal Service with a quality address database, a change of address system, and customer address products to facilitate the timely and cost-effective coding, sorting, and delivery of the mail. In fiscal year 2009, NCSC products and services generated more than \$100 million in revenue for the Postal Service.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether network security controls implemented at the NCSC and associated sites adequately provide for the confidentiality, integrity, and availability of Postal Service information resources. To achieve our objective, we performed network security assessments using industry-accepted automated software tools and manual reviews to identify known high-risk vulnerabilities. In addition, we performed a limited review of physical security.

We performed our assessment from November 30 through December 11, 2009, and limited our review to [REDACTED] residing on eight subnets assigned to the NCSC. We interviewed key officials and reviewed applicable Postal Service policies, standards, and procedures. We used manual and automated techniques to analyze computer-processed data and concluded the data were sufficiently reliable to meet the report objectives. We provided management with detailed results on January 22, 2010.

We conducted this performance audit from September 2009 through April 2010 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusion based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

PRIOR AUDIT COVERAGE

The OIG did not identify any prior audits or reviews related to the objective of this audit.

APPENDIX B: DETAILED ANALYSIS

Operating System and Database Server Vulnerabilities

The Postal Service requires a patch management process to control the deployment and maintenance of software releases and to resolve known security vulnerabilities.¹⁰ Additionally, administrators must manage changes to information resources and configurations to ensure resources are not inadvertently exposed to unnecessary risk and vulnerabilities.¹¹ Further, system administrators must harden hardware and system software to comply with Postal Service information security requirements.¹²

Operating Systems

For the [REDACTED] operating systems included in our review, we identified [REDACTED] as detailed in the following table:

Operating System Environment ¹³	Number Assessed	Systems With At Least One High-Risk Vulnerability	Unique High-Risk Patch Related Vulnerabilities
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Total	[REDACTED]	[REDACTED]	[REDACTED]

We aged each missing operating systems patch according to the date the operating system's vendor made the most recent patch publicly available. As displayed in the following tables, vendors made a patch available to remediate 70 percent of the Windows and 63 percent of the [REDACTED] vulnerabilities at least 1 year before December 15, 2009, the date we completed our automated assessment.

[REDACTED] Patch Aging Schedule		
Age	Number	Percentage
< 30 Days	3	2%
31 – 180 Days	33	18%
181 – 365 Days	19	10%
> 365 Days	131	70%
Total	186¹⁴	100%

¹⁰ Handbook AS-805, Section 8-2.4, Configuration and Change Management.

¹¹ Handbook AS-805, Section 8-2.4.3, Change and Version Control.

¹² Handbook AS-805, Section 8-2.4.2, Configuration Hardening Standards.

¹³ The operating system environment includes operating system and third-party application vulnerabilities.

¹⁴ [REDACTED]

Patch Aging Schedule		
Age	Number	Percentage
< 30 Days	1	1%
31 – 180 Days	23	18%
181 – 365 Days	23	18%
> 365 Days	81	63%
Total	128¹⁵	100%

In addition, we identified:

- Two [redacted] systems with [redacted].
- Five [redacted] systems with [redacted].
- Twenty-six systems [redacted].
- Three [redacted] systems [redacted].
- One [redacted] system [redacted].
- One system [redacted].
- Sixty-two [redacted] operating systems that were [redacted].
- [redacted] operating systems [redacted].
- Five systems allowed [redacted].
- Four [redacted] operating systems [redacted].
- Overall, we identified [redacted] configuration-related vulnerabilities, as shown in the following table.

Operating System	Number Assessed	Unique High-Risk Configuration Related Vulnerabilities
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Total	[redacted]	[redacted]

15 [redacted]
16 [redacted]
17 [redacted]

Databases

We reviewed five Oracle database servers and identified the following [REDACTED] unique high-risk vulnerabilities.

- [REDACTED]
- [REDACTED]

We also identified:

- [REDACTED]
- [REDACTED]
- [REDACTED]

APPENDIX C: MANAGEMENT'S COMMENTS



April 9, 2010

Lucine M. Willis
Director, Audit Operations
Office of Inspector General
1735 N. Lynn Street, Room 11044
Arlington, VA 22209-2020

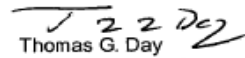
SUBJECT: Transmittal of Draft Audit Report – Network Security Assessment of the National Customer Support Center (Report Number IS-AR-10-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendation 1, 2, 3 and 4 of the report; the response is attached.

The subject report and this response contain information related to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will work with you to determine what portions of this report should be considered as classified and restricted and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding this response please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.


Ross Philo
Executive Vice President
and Chief Information Officer


Thomas G. Day
Senior Vice President
Intelligent Mail and Address Quality

Attachment

cc: audittracking@uspsaig.gov
John T. Edgar
Deborah J. Judy
Charles L. McGann
James D. Wilson
Sally K. Haring

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260

Network Security Assessment of the National Customer Support Center
(Report Number IS-AR-10-FRAFT) Project Number 09RG030IS000

Page 2

We recommend the senior vice president, Intelligent Mail and Address Quality, direct the manager, Address Management, to:

1. Utilize the Postal Service patch and configuration management processes to identify and remediate missing patches and configuration issues.

Management agrees with the recommendation. The NCSC will work closely with the Corporate Information Security Office (CISO) to develop and implement a process to derive all patches, operating system, and database updates directly from the official CISO source and to standardize NCSC systems with all applicable Postal Service hardening standards. This will ensure that NCSC systems maintain the same level of update as used throughout the Postal Service IT environment.

Anticipated completion date: September 30, 2010

2. Upgrade the Oracle database software and remediate the patch-related vulnerabilities.

Management agrees with the recommendation. Two applications are currently remaining on systems that require database patch remediation. One requires a series of system outages to perform that is scheduled to be completed for May 15, 2010 as described in the response to Recommendation 1. The other remaining system is scheduled to be migrated into a new environment on or before September 1, 2010.

All other Oracle database instances within the NCSC are at the current patch levels.

The NCSC will work closely with the Corporate Information Security Office (CISO) to develop and implement a process to derive all patches, operating system, and database updates directly from the official CISO source and to standardize NCSC systems with all applicable Postal Service hardening standards. This will ensure that NCSC systems maintain the same level of update as used throughout the Postal Service IT environment.

Anticipated completion date: September 1, 2010

3. Periodically review server configurations to ensure servers comply with applicable Postal Service hardening standards.

Management agrees with the recommendation. Server configuration issues noted on the audit report have been corrected to comply with USPS hardening standards. Plans have been developed to remediate other configuration and patch management issues concurrent with the migration to new servers. The NCSC has implemented a formal patch and configuration review process to ensure all servers continue to comply with postal requirements. See attachment for the written policy. This policy document is intended as the interim methodology to keep NCSC systems at the appropriate revision level and compliant with Postal Service hardening standards.

The NCSC will work closely with the Corporate Information Security Office (CISO) to develop and implement a process to derive all patches, operating system, and database updates directly from the official CISO source and to standardize NCSC systems with all applicable Postal Service hardening standards. This will ensure that NCSC systems maintain the same level of update as used throughout the Postal Service IT environment.

Anticipated completion date: September 30, 2010

Network Security Assessment of the National Customer Support Center
(Report Number IS-AR-10-FRAFT) Project Number 09RG030IS000

Page 3

4. Configure existing vulnerability management software to assess web server vulnerabilities as required.

Management agrees with the recommendation. The NCSC does not have the access required to configure the scanning software used to perform vulnerability assessments. The NCSC has coordinated with the USPS Corporate Information Security Office to install an updated version of the vulnerability management system. The CISO has verified that the vulnerability management system is configured properly to perform the vulnerability assessments per USPS policy standards. See attached email from CISO contact as reference.

Anticipated completion date: Completed, requesting closure upon receipt of this response.

**NCSC Technology Services
Standards, Procedures, Policies and Guidelines**

NCSC PATCH AND CONFIGURATION MANAGEMENT POLICY

Introduction

The NCSC technology services group acquires systems, hardware, and COTS products from various third-party providers. These technology applications, systems and hardware are periodically updated for performance or to ensure that appropriate security is maintained by identifying known vulnerabilities. Security patches and configuration requirements must be evaluated on a regular basis and installed in a timely manner following established evaluation and implementation processes and must be properly documented in the change management system (Remedy) to ensure that systems are current and compliant with the USPS's information security policies.

Scope of Policy

The NCSC's patch and configuration management process covers all information resources located in the NCSC facilities in [REDACTED] that are administered by NCSC personnel (equipment administered by Engineering, ACE, Raleigh, etc. is outside the scope of this document).

Goal

It is the Technology Services group's responsibility to provide a secure environment for NCSC applications. As part of this goal, it is NCSC'S policy to ensure all computer devices connected to the network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed.

The NCSC's patch and configuration management process was implemented to investigate, prioritize, test, track, control the deployment and maintenance of software releases, USPS security requirements, and resolve known security vulnerabilities. The NCSC understands that patch and configuration management is critical to ensure the integrity and reliability of information resources.

Responsibility

While safeguarding the network is every user's job, Technology Services ensures all known and reasonable defenses are in place to reduce vulnerabilities while keeping the applications functional. The technology services management staff will be notified of the implementation of patches and service packs or changes to hardware operating systems. The systems and database administrators will be responsible for the implementation of security patches/changes for applications, services and hardware. The administrators will maintain appropriate documentation of changes via Remedy (with approvals from impacted users or development groups) made to each application, system and hardware device. The administrators will also perform periodic inventories of application, system and hardware versions.

Scanning

Scanning the entire network and providing information such as service pack level of the machine, missing security patches, key registry entries, weak passwords, users and groups, and more will be done throughout the year by the network support group. Results from the scans will be provided to the [REDACTED] and database management team. Based on the criticality of the scan results a decision will be made as to whether immediate (emergency) patching should be performed or if the patching can be scheduled during the next scheduled upgrade.

Monitoring

In addition to the information found during scanning. Technology Services will review vendor notifications and web sites for the release of new patches. The NCSC uses third-party software to inventory systems and versions and determine that appropriate, licensed versions are in use. Software may also be used to easily obtain and implement required patch information.

Notification and scheduling

Technology Services' management must approve the schedule prior to implementation. Regardless of criticality, each patch release requires the creation and approval of a change request (CR) prior to releasing the patch. Approvals include the technology staff group implementing the change, the application/user groups impacted, and the security group.

[REDACTED]

January 15
June 15

COTS products
January 15
June 15

Quarterly for Oracle

Note: Oracle database Critical Patch Updates (CPU) are distributed every quarter – Jan, Apr, Jul, and Oct and their content may or may not apply to the database.

Mar 15
June 15
Sept 15
Dec 15

Monthly for Windows
15th of each month

Evaluation and Implementation

Technology Services will categorize the criticality of the patch and/or configuration change according to the following:

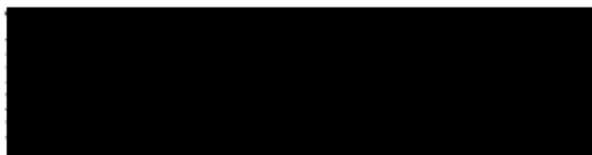
- Emergency — an imminent threat to NCSC'S network
- Critical — targets a security vulnerability
- Not Critical — a standard patch release update
- Not applicable to NCSC'S environment

If Technology Services categorizes a patch or configuration change as an Emergency, the department considers it an imminent threat to NCSC'S network and may immediately release the patch. As Emergency patches pose a dire threat to the network, the release may proceed testing. In this case, the department will perform testing post-implementation. Technology Services will obtain authorization for implementing these emergency patches via an emergency CR with the appropriate approval. The department will implement non-critical patches during regularly scheduled preventive maintenance. Patches deemed Critical or Not Critical will undergo testing for each affected platform before release, if at all possible, for implementation during the next scheduled patch release. In the case that testing is not possible, a complete back out plan must be established prior to implementation which includes backing up the systems about to be patched to be sure that it is possible to return to a working configuration.

Technology Services will assess the effect of a patch or configuration change prior to its deployment. If it is determined that the patch or change can not be implement because software or an application will not function properly with the upgrade, this will be noted and approved by NCSC management and, if appropriate, a remediation plan will be developed.

When possible, patch and configuration management will be done centrally from in order to expedite patching, reduce the costs associated with distribution and management, and automate the repetitive activity associated with rolling out patches.

Finally, following the release of all patches, Technology Services staff will verify the successful installation of the patch and that there have been no adverse effects.



From: [REDACTED]
Sent: Monday, April 05, 2010 1:51 PM
To: [REDACTED]
Cc: [REDACTED]
Subject: RE:

I got your second voicemail. So for the record, yes the Nexpose system is configured to check for vulnerabilities in webservers. It will always get best results when credentials are configured for the sites to be scanned.

|| [REDACTED]