



August 15, 2008

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Access Controls at the [REDACTED]
[REDACTED] Information Technology and Accounting
Service Centers for Fiscal Year 2008 (Report Number IS-AR-08-015)

This report presents the results of our audit of access controls at the [REDACTED]
[REDACTED] Information Technology and
Accounting Service Centers (IT/ASCs) (Project Number 08RD001IS002). The objective
of this audit was to determine whether the U.S. Postal Service has adequate controls
that limit or detect access to its information resources (data, programs, equipment, and
facilities) and protect these resources against unauthorized (accidental or intentional)
modification, loss, damage, or disclosure. We performed this self-initiated review as
part of the fiscal year (FY) 2008 information systems audit of general controls at the
Postal Service's IT/ASCs. Click [here](#) to go to Appendix A for additional information
about this audit.

Conclusion

Overall, physical access controls for IT facilities and logical access controls for
[REDACTED] were in place and functioning
adequately. However, our testing identified opportunities to improve compliance with
these controls. Specifically, management can improve logical access controls by
removing user accounts of terminated and transferred employees from [REDACTED]
[REDACTED]

UNIX Groups

UNIX groups, which are a means of facilitating access to directories and files in the
UNIX operating system, contained user accounts of terminated and transferred
employees. This occurred because UNIX administrators did not remove inactive user
accounts from UNIX groups at the time they were locked, making them inactive and
unusable. Reinstatement of these accounts for transferred or terminated personnel
could result in users inheriting prior permissions. When administrators promptly revoke
access for terminated and transferred personnel, it eliminates the potential for

accidental or intentional modification, loss, damage, or disclosure of computer data. Click [here](#) to go to Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the Manager, Host Computing Services, in Eagan to:

1. Develop an automated procedure to identify and remove user accounts of terminated and transferred employees who no longer need access from UNIX groups.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

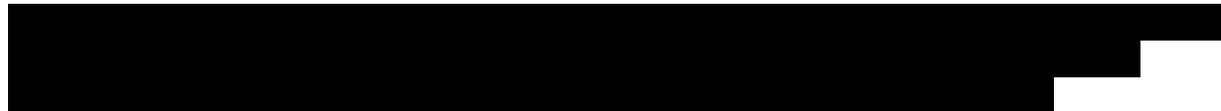
Management's Comments

[REDACTED]

[REDACTED]

¹ [REDACTED]

² Information System Access Controls at the Eagan, Minnesota, and San Mateo, California, Information Technology and Accounting Service Centers (Report Number IS-AR-06-018, dated September 27, 2006).



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.

Oracle Password Verification



Physical Security

We reviewed physical security controls restricting access to computer resources at the [xxxxxx](#) IT/ASCs. Our review verified that management implemented proper physical security controls commensurate with the risks of physical damage or loss to the IT/ASCs.

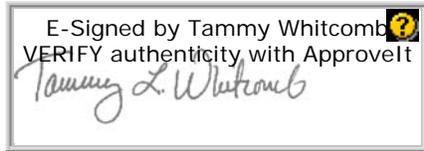
Mainframe and the Windows Environment

We reviewed mainframe users who had access to sensitive payroll files and the EMRS. We also reviewed two applications operating in a Windows environment: the Sales Resource Management (SRM) and Official Mail Accounting System (OMAS). Our review verified that management implemented proper access controls, providing reasonable assurance that data files and application programs are protected against unauthorized modification, disclosure, loss, or impairment. We found no issues associated with the specific applications reviewed for these environments.

³ Handbook AS-805, *Information Security*, Section 9-7.1.1, Password Selection Requirements, dated March 2002 and updated with *Postal Bulletin* revisions through November 23, 2006, details password selection requirements such as upper and lower case alphanumeric, along with numbers and special characters, and a specified minimum password length.

⁴ A black rectangular redaction covering the text of the second footnote.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Gary C. Rippie, Director, Information Systems, or me at (703) 248-2100.



Tammy L. Whitcomb
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Ross Philo
H. Glen Walker
Harold E. Stark
Joseph J. Gabris
Jerome G. Reynolds
Gregory Wallace
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The Postal Service maintains policies and procedures governing logical and physical access controls over information systems that support its business operations.

Logical access controls include the use of computer hardware and software to prevent or detect unauthorized access. For example, users may be required to input user names, passwords, or other identifiers that are linked to predetermined access privileges. It also includes proper system configurations that conform to the concepts of least privilege and need-to-know.

Physical access controls involve restricting physical access to computer resources and protecting these resources from intentional or unintentional loss or impairment. For example, users are required to use a badge to access restricted areas.

Oracle is a relational database management system owned and developed by the Oracle Corporation. [REDACTED]. Oracle controls user access to its databases through the use of profiles. The Database Administrator (DBA) first creates profiles and may subsequently assign privileges directly to a user or to a defined role.

A profile is a collection of resource usage and password-related features that a DBA can assign to users. Profiles set hard limits on scarce database and server resources and parameters used for enforcing password-related security policies. [REDACTED]

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether the Postal Service has adequate controls to limit or detect access to its information resources (data, programs, equipment, and facilities) and protect these resources against unauthorized (accidental or intentional) modification, loss, damage, or disclosure.

The scope of our review included physical access controls over computer resources and logical access controls over systems hosted at the [REDACTED] IT/ASCs; and applications supported by staff at the [REDACTED] Integrated Business Systems Solutions Centers; and the [REDACTED] Information Technology Service Center (ITSC).

The audit covers the following primary platforms the Postal Service uses in its computing environment:

- Mainframe
- UNIX
- Windows
- Databases

We judgmentally selected several applications⁵ for review on these platforms. We used criteria such as production status, financial relevance, sensitivity or criticality, platform, and location to make our selections. Table 1 provides a summary of the applications reviewed.

Table 1: Applications Selected for Review by Platform

Mainframe	OMAS; ChangeMan	EMRS
UNIX	eAwards	EMRS
Windows	OMAS	SRM
Databases	eAwards (Oracle)	EMRS (Oracle)

To validate access controls over system software, we reviewed current policies and procedures to ensure they exist and are up-to-date. We reviewed access to file names associated with critical system software libraries, selected applications, and servers. We verified administrators configured the operating systems to monitor and log access through the security software, use of system management facilities, or system configurations. We interviewed key Postal Service personnel responsible for the platforms under review.

We conducted this performance audit from November 2007 through August 2008 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 conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We used manual and automated techniques to analyze the computer-processed data. Based on the results of these tests and assessments, we generally concluded the data were sufficient and reliable to use in meeting the objective. We discussed our observations and conclusions with management officials during the audit and on July 17, 2008, and included their comments where appropriate.

⁵ We selected the following applications: [REDACTED]

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date	Monetary Impact	Report Results
<p><i>Information Systems Access Controls at Selected Information Technology Facilities for Fiscal Year 2007</i></p>	<p>IS-AR-08-002</p>	<p>November 6, 2007</p>	<p>N/A</p>	<p>Overall, access controls for mainframe, xxxx [REDACTED], and networking platforms were in place and functioning adequately. However, testing identified opportunities to improve compliance with these controls. Specifically, management can improve access controls [REDACTED]</p>
<p><i>Information System Access Controls at the [REDACTED] Information Technology and Accounting Service Centers</i></p>	<p>IS-AR-06-018</p>	<p>September 27, 2006</p>	<p>N/A</p>	<p>Overall, we found access controls were adequate to protect computer and information resources at the data centers against unauthorized modification, loss, and disclosure. However, management could improve the access control environment by developing an automated process for monitoring [REDACTED]</p>

APPENDIX B: DETAILED ANALYSIS

UNIX Groups

[REDACTED]⁶ UNIX group membership gives users special access to files and directories permitted to that group. We found six of the seven groups analyzed on the [REDACTED] server and four of seven groups analyzed on the [REDACTED] server contained user accounts of staff who had changed positions or were no longer with the Postal Service. The user accounts for transferred or terminated employees or contractors were placed in a locked status, making them inactive and unusable.

[REDACTED]
[REDACTED] When administrators promptly revoke access for terminated and transferred personnel, it eliminates the potential for accidental or intentional modification, loss, damage, or disclosure of computer data.

[REDACTED]

[REDACTED]

[REDACTED]⁷

[REDACTED]

⁶ The majority of accounts contained in these UNIX groups consisted of Information Technology personnel such as developers and DBAs.

⁷ See footnote 1.

Oracle Password Verification

[REDACTED]. To determine if the passwords on the Oracle databases followed Postal Service policies for passwords, we changed the password for our Oracle account. [REDACTED]

[REDACTED]. This occurred because Oracle cannot process certain password characteristics⁸ as currently required.

Corrective Actions Taken

During the audit we identified several miscellaneous items that required attention, although we did not consider these items reportable issues. When we brought these items to the attention of management, they took corrective action. We give credit to management for their timely action to resolve the issues.

In the UNIX environment we found situations of improper settings, file ownership, or permissions associated with individual user accounts. For example:

[REDACTED]

- The default security settings applied to objects a user created did not conform to UNIX hardening guidelines.
- A directory had an access mode established as if it were a user account rather than a system account.
- Four files on servers had an invalid ownership association.
- A test account which administrators should have removed remained active after the completion of system testing.
- A user account which administrators were supposed to disable had been inadvertently enabled during system changes.

In the Oracle environment management corrected circumstances of inappropriate security that we identified such as a database connection from the eAwards database to another database being assigned to a developer rather than to a DBA.

⁸ See footnote 4.

In the mainframe environment, we found an employee had access to critical and sensitive datasets in San Mateo but no longer required this access. Eagan mainframe security personnel revoked the employee's access.

APPENDIX C: MANAGEMENT'S COMMENTS

GEORGE W. WRIGHT
VICE PRESIDENT
INFORMATION TECHNOLOGY OPERATIONS



August 11, 2008

Lucine Willis
Director, Audit Operations
1735 North Lynn Street
Arlington, VA 22209-2020

SUBJECT: Transmittal of Draft Audit Report- Access Control Review (Report Number
IS-AR-08-DRAFT)

Thank you for the opportunity to review and comment on the subject draft audit report. We are pleased to provide the attached response to the recommendations provided in the subject audit report. We are in full agreement with recommendation 1 and in partial agreement with recommendation 2.

The subject audit report and this response contain information relating to potential security vulnerabilities that, if released, could possibly be exploited and cause 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 classified and restricted, and exempt from disclosure under the Freedom of Information Act.

If you have any questions or comments regarding our responses and would like to discuss them further, please contact Pete Stark, Manager, Corporate Information Security, at 202-268-7378.

A handwritten signature in black ink, appearing to read "George W. Wright".

George W. Wright

cc: Ross Philo
H. Glenn Walker
Harold E. Stark
Joseph J. Gabris
Katherine S. Banks
Jerome G. Reynolds
Gregory Wallace

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260 1600
202-268-2764
Fax: 202-268-4402
TELEPHONE: 202-268-4402
WWW.EPS.COM

Transmittal of Draft Audit Report-Access Control Review (Report Number IS-AR 08-DRAFT)

We recommend the Vice President, Information Technology Operations, direct the Manager, [REDACTED] to:

Recommendation 1: Develop an automated procedure to identify and remove user accounts of terminated and transferred employees who no longer need access from UNIX groups.

Response: Management agrees with this recommendation. The management of the UNIX group memberships is already being addressed in the SOX efforts. The implementation is dependant on the development of UNIX support within eAccess. This is expected to be fully deployed by the end of March 2009.

Scheduled Completion Date: March 31, 2009

We recommend the Vice President, Information Technology Operations, direct the Manager, Business Data Management, to:

Recommendation 2: Develop an automated procedure to periodically review user accounts [REDACTED]

Response: Management partially agrees with this recommendation. DBSS is developing an automated procedure to periodically review user account profiles. This procedure is being addressed as part of the SOX efforts and is expected to be completed by the end of March 2009.

Scheduled Completion Date: March 31, 2009