March 31, 2010

ROSS PHILO
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

VINCENT DEVITO
VICE PRESIDENT, CONTROLLER

DEBORAH J. JUDY
DIRECTOR, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Fiscal Year 2009 Information Systems General Computer Controls Capping Report (Report Number IS-AR-10-005)

This report summarizes the results of our audit of information systems general controls at the [redacted] Information Technology and Accounting Service Centers (IT/ASC) and the [redacted] Information Technology Service Center (ITSC) for fiscal year (FY) 2009 (Project Number 09RD001IS000). The objectives of the audit were to determine whether general controls for selected applications, data, and computer infrastructure at the IT centers provided reasonable assurance that computer-processed data were complete, validated for accuracy, and secure; and business practices complied with U.S. Postal Service policies, procedures, and standards. We performed this self-initiated audit as part of the FY 2009 financial statements audit. See Appendix A for additional information about this audit.

Conclusion

General computer controls for selected applications, data, and the computer infrastructure at the information data centers provided reasonable assurance that computer-processed data were complete, validated for accuracy, and secure. However, we identified Information Technology (IT) control issues that do not, alone or collectively, represent a significant risk to reliance on general computer controls. We issued five interim audit reports during our FY 2009 audit to assist management in improving information technology operations. See Appendix B for summaries of the audit reports we issued. This report does not contain recommendations; however, four of the interim audit reports provided recommendations to address issues identified during our audit.

The issues were in the areas of:

- Physical security related to semiannual building key surveys and reviews of identification (ID) badge access control lists.
- UNIX access controls related to [redacted].
- Network access controls related [redacted].
- Windows® access controls related to [redacted] not in compliance with the Windows security standards.

While conducting the audit, we identified several additional issues that required management's attention. Management took action to correct each of the issues during the audit; therefore, we did not make recommendations to address them.

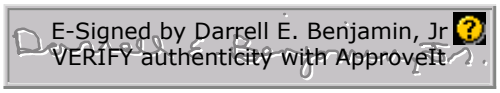
- Repairing a [redacted] facility door that separates processing and distribution center personnel from the IT/ASC.
- Resolving UNIX issues to:
  - Disable [redacted]
  - Add a missing account and missing group.
  - Remove privileged files from a shared directory.
  - Remove an unlocked unnecessary account.
  - Restrict [redacted] to the system console.
  - Disable [redacted].
  - Restrict access to [redacted].
  - Limit access to [redacted]
  - Set appropriate security mode on [redacted][1] [redacted].
  - Correct a primary group ID shared by multiple accounts.
- Modifying Oracle® issues for appropriate application and user profile settings.

[1] [redacted]

We summarized the status of FY 2009 and previous years' recommendations in Appendix C.[2] See Table 1 in Appendix C for a list of open recommendations and Table 2 for a list of recommendations that were closed.

This report does not contain any findings or recommendations. Management concurred with the facts presented in the report. See Appendix D for management's comments, in their entirety.

We appreciate the cooperation and courtesies provided by your staff. If you have 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: Charles L. McGann
Joseph J. Gabris
Gregory D. Larrabee
Sally K. Haring

[2] The recommendations in Appendix C refer to audits of IS general controls only.

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

[redacted] IT/ASCs provide computer processing and accounting services for the Postal Service. [redacted] ITSC provides infrastructure services[3] for over 38,000 Postal Service locations. Each site includes multiple service organizations.

[redacted] IT/ASCs house three parallel service areas:

- Host Computing Services (HCS)
- Integrated Business Systems Solutions Center (IBSSC)
- Accounting Service Center

[redacted] IT/ASC has a similar structure but without a HCS area.

HCS deploys, operates, and supports systems and applications for all business units within the Postal Service. The IBSSCs perform application development, enhancement, and maintenance of systems that enable the Postal Service to achieve its business objectives. The ASCs are responsible for a variety of accounting and finance activities. These activities include accounts payable, banking, and reconciliation issues; domestic and international claims; money orders; daily financial reporting; and payroll and benefits adjustments. All IT-related service centers report to the executive vice president, chief information officer. The ASCs report to the vice president, controller.

To facilitate the delivery of mail worldwide, the IT organization:

- Maintains the Postal Service's computing infrastructure.
- Manages the corporate-wide intranet.
- Runs the systems that connect processing centers and 38,000 post offices nationwide.
- Controls the technology supporting 650 applications for day-to-day Postal Service business, including payroll for approximately 700,000 career employees.
- Determines the strategic direction for the agency's information technology.
- Employs over 1,000 IT employees across the continental U.S.

[3] Infrastructure services are IT functions that support the overall Postal Service enterprise and include such areas as telecommunications, distributed computing, and IT help desk.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of the audit were to determine whether general controls for selected applications, data, and computer infrastructure at the IT centers provided reasonable assurance that computer-processed data were complete, validated for accuracy, and secure; and business practices complied with Postal Service policies, procedures, and standards.

The scope of our audit at the [redacted] IT/ASCs and the [redacted] ITSC included reviews of the following systems and control areas:

- Security management.
- Access controls.
- Configuration management.
- Segregation of duties.
- Follow-up on prior years' recommendations.

In addition, we tested the above controls as they relate to the operating systems and database platforms for the following applications:

[redacted]

To address the audit objectives, we reviewed:

- Password management practices for compliance with Postal Service standards and password settings, including expiration intervals and password complexity for normal and privileged accounts.

- Mainframe and mid-range[4] user access to commands and data to determine consistency with policies and procedures.

- Mainframe and mid-range logon IDs to ensure the IDs were properly managed and employees had access to appropriate Postal Service data and resources.

- System controls by downloading and reviewing the appropriate settings and configuration files (in some cases performing live tests to ensure that

[4] In general, mid-range refers to computers that are more powerful and capable than personal computers but less powerful and capable than mainframe computers.

system controls were effective), interviewing IT personnel, and reviewing vendor documentation.

- Documentation that authorizes access to Postal Service systems and data to verify adequate protection of Postal Service resources.

- Critical mainframe operating system and system software datasets stored on the mainframe and secured by [redacted] and security parameters to ensure the central security system validates user access.

- Physical security procedures and practices to verify that physical access controls were in place to protect Postal Service resources.

- Information system policies and procedures to validate they were implemented, updated, and followed.

- System configuration reports and observed back-up tape handling procedures to verify management backed up critical production files and servers.

- Badge access system and key control procedures at each IT/ASC to ensure managers reviewed badge and key access lists and validated and documented the processes.

To supplement the general computer controls audit, our Vulnerability Assessment Team conducted tests of selected servers and databases that support the [redacted] application.[6] These tests provided management with an evaluation of the quality of security for servers where the selected applications reside.

We interviewed personnel at the various IT/ASCs to obtain relevant information and to corroborate our analyses. We also collected and analyzed documentation on policies and procedures at these locations as they pertained to the specific areas we reviewed. We judgmentally selected applications for review based on financial significance, sensitivity, elapsed time since the last review, and the platforms on which they reside. For example, to facilitate our UNIX testing, we selected finance-related applications residing on UNIX servers.

We used batch and online report tools to extract and display detailed information from the mainframe, such as user access authorizations, security resource rules governing access to application data sets, and system parameter settings. We

[5] The software security tool the Postal Service uses to enforce security policies and procedures in a mainframe environment.
[6] *Database and Network Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-10-001, dated December 14, 2009).

used manual and automated techniques to analyze computer-processed data. Based on those tests and assessments, we concluded these data were sufficiently reliable to meet the audit objectives. We performed all system queries in a controlled environment with management's full knowledge and approval.

We conducted this performance audit from October 2008 through March 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 conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management officials throughout the audit and again on February 24, 2010, and included their comments where appropriate. We used data from various mainframe and distributed systems and financial applications in the course of conducting our audit. We performed limited testing of this information as part of our review.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date Report	Results
Fiscal Year 2008 Information Systems General Controls Capping Report	IS-AR-09-005	March 19, 2009	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas [redacted] The report contained no recommendations.
Fiscal Year 2007 Information Systems General Controls Capping Report	IS-AR-08-007	March 11. 2008	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas of [redacted] The report contained no recommendations.
Fiscal Year 2006 Information Systems General Controls Capping Report	IS-AR-07-009	February 26, 2007	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas of access to [redacted] he report contained no recommendations.

APPENDIX B: SUMMARY OF REPORTS ISSUED

***Physical Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-09-008, dated July 28, 2009).**

This report presented the results of our audit of physical access controls at the Postal Service's IT/ASCs [redacted] The objective of this audit was to determine whether the Postal Service established adequate controls to restrict physical access to information resources at the IT/ASCs. We determined that the Postal Service established adequate controls to restrict physical access to information resources at the IT/ASCs. However, we identified an opportunity to improve compliance with Postal Service policies. Specifically, management could further minimize the risk of unauthorized modification, loss or disclosure of Postal Service information resources by conducting a semiannual survey of all building keys at the IT/ASCs and periodically reviewing the [redacted] IT/ASC ID badge access control list.

We provided recommendations to (1) develop a procedure to track and schedule key inventory surveys at the [redacted] IT/ASCs; (2) conduct a survey of all building keys at the [redacted] IT/ASC; (3) develop a procedure to track and schedule key inventories at the [redacted] IT/ASC; and (4) develop a procedure to track and schedule quarterly ID badge access reviews at the [redacted] IT/ASC. In addition, when brought to their attention, management initiated action to correct three security issues.

***UNIX Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-09-010, dated August 10, 2009).**

The report presented the results of our audit of logical access controls of UNIX information resources [redacted]. The objective of this audit was to determine whether management established adequate logical controls to limit or detect inappropriate access to its UNIX information resources. We determined that management established adequate logical access controls to limit or detect inappropriate access to UNIX information resources. However, we found the Postal Service can further improve logical access controls [redacted]

We provided recommendations to [redacted]

[redacted]

Management took corrective action to initiate ten access control issues we identified during the audit. These access control issues did not, alone or collectively, represent a significant risk to reliance on general computer controls. Therefore, we did not make a recommendation regarding these specific issues.

***Database and Network Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-10-001, dated December 14, 2009).**

The report presented the results of our audit of database and network access controls at the [redacted] IT/ASCs and the [redacted] ITSC. The objective of this audit was to determine whether the Postal Service adequately controls logical access to its database and network information resources to protect these resources against unauthorized (accidental or intentional) modification, loss, damage or disclosure. We determined that database and network logical access controls were generally in place and functioning properly. However, management can improve [redacted] Management corrected these issues during the course of our review, therefore, we did not make a recommendation regarding this issue. Further, management can improve network access controls by improving the management and monitoring of [redacted]

We provided recommendations to (1) develop a process to review and identify appropriate network devices at the [redacted] IT/ASCs to include in the network management software; (2) periodically review and update the [redacted] are categorized appropriately; (3) [redacted] to ensure compliance with applicable hardening standards and adopt industry practices as appropriate; (4) develop procedures to ensure standardized and complete network diagrams are produced; (5) develop a procedure to provide continuous maintenance and monitoring of [redacted][7] and (6) incorporate a test of controls [redacted] to validate the encryption of sensitive information.

[7] A remote authentication protocol used to communicate with an authentication server. [redacted] allows a remote access server to communicate with an authentication server to determine if the user has access to the network.

***Mainframe Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-10-003, dated December 29, 2009).**

The report presented the results of our audit of the mainframe access controls at the [redacted] IT/ASCs. The objective of this audit was to determine whether the Postal Service established adequate logical controls to limit or detect inappropriate access to its mainframe operating environment. We determined that the Postal Service established adequate logical controls to limit or detect inappropriate access to its mainframe [redacted][8] [redacted][10] [redacted] This report did not contain any findings or recommendations.

***Windows Access Controls at the Information Technology and Accounting Service Centers* (Report Number IS-AR-10-006, dated March 24, 2010).**

The report presented the results of our audit of Windows access controls at the [redacted] IT/ASCs and the [redacted] ITSC. Our objective was to determine whether the Postal Service established adequate logical controls to limit or detect inappropriate access to its Windows operating environment. We determined that the Postal Service established adequate logical controls to limit or detect inappropriate access to its Windows operating system [redacted]. However, [redacted]

We provided recommendations to (1) revise security standards for [redacted] to clearly define system administrator responsibilities for [redacted] on a regular basis; (2) review the Windows security standards and update them as appropriate; and (3) perform a comprehensive review of the [redacted] to ensure compliance with applicable Windows security standards.

[8] [redacted]

[9] System software is a set of programs designed to operate and control computer processing activities. Examples of system software include system utilities, program library systems, and file management software.

[10] [redacted]

APPENDIX C: ACTION ON PRIOR YEAR RECOMMENDATIONS

Table 1: Open Recommendations

Report Number	Rec. Number Significant (S)	Description	Responsible Organizations							
			[redacted][11]	[redacted][12]	[redacted][13]	[redacted][14]	[redacted][15]	[redacted][16]	[redacted][17]	[redacted]
IS-AR-07-017[18]	1(S)	Assess the risk to all IT/ASC positions for the purpose of assigning them as sensitive.	X					X	X	X
	2	Require a periodic reassessment of the risk of sensitive positions to determine if they should retain the designation.	X					X	X	X
	3	Establish a central location to maintain an official list of sensitive positions by occupation code, title, and job description.	X					X	X	X

[11] [redacted]
[12] [redacted]
[13] [redacted]
[14] [redacted]
[15] [redacted]
[16] [redacted]
[17] [redacted]
[18] *Separation of Duties* [redacted], dated August 29, 2007.

Report Number	Rec. Number Significant (S)	Description	Responsible Organizations							
			11 [redacted]	12 [redacted]	13 [redacted]	14 [redacted]	15 [redacted]	16	17 [redacted]	[redacted]
4(S)		Notify the Postal Inspection Service when management creates a new IT/ASC position, hires a new employee, or promotes an employee to a new position to make certain management attributes the proper clearance level to the employee.	X					X	X	X
	5	Amend the *Administrative Support Manual*, Issue 13, Chapter 2, Section 272 (Security Clearance), to: ▪ Designate the chief postal inspector as responsible for defining the criteria for identifying sensitive positions. ▪ Specify the criteria for designating a position as sensitive. ▪ Update the list of position types requiring a sensitive clearance.						X		

Report Number	Rec. Number Significant (S)	Description	Responsible Organizations							
			[redacted] 11	12 [redacted]	13 [redacted]	14 [redacted]	15 [redacted]	16	[redacted] 17	[redacted]
IS-AR-08-015[19]	1	Develop an automated procedure to identify and remove user accounts of terminated and transferred employees who no longer need access from UNIX groups.	X	X	X					
IS-AR-09-002[20]	3	Perform risk reassessments on the six applications reviewed during this audit.	X							

[19] *Access Controls* [redacted] dated August 15, 2008.

Security Policies and Procedures (Corporate-Wide) at the Information Technology and Accounting Service Centers for Fiscal Year 2008, dated November 13, 2008.

Table 2: Closed Recommendations

Report Number	Recommendation Number	Responsible Organizations							
		[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
IS-AR-08-009[21]	1(S)	X	X					X	
	2(S)								
	3(S)								
	4								
IS-AR-08-011[22]	1(S)	X	X	X					
	2								
	3								
IS-AR-08-013[23]	1(S)	X	X	X	X	X			
	2								
	3								
	4								
IS-AR-08-015 2		X	X	X					
IS-AR-09-002	1	X					X		
	4								
IS-AR-09-003[24]	1	X		X					
	3								
	4								

[21] *Update Processes for Active Directory and CA-ACF2*, dated March 14, 2008.
[22] *System Software Controls at the* [redacted] *Information Technology and Accounting Service Centers for Fiscal Year 2008*, dated June 3, 2008.
[23] *Protection of Sensitive Equipment at Selected Postal Service Information Technology Facilities*, dated July 9, 2008.
[24] *Service Continuity at the Information Technology and Accounting Service Centers for Fiscal Year 2008,* dated January 20, 2009.

APPENDIX D: MANAGEMENT'S COMMENTS

ROSS PHILO
EXECUTIVE VICE PRESIDENT
CHIEF INFORMATION OFFICER

UNITED STATES POSTAL SERVICE

March 3, 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 – Fiscal Year 2009 Information Systems General Computer Controls Capping Report (Report Number IS-AR-09-XXX), Project Number 09RD001IS000

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with the reported summaries the report contains no recommendations.

[redacted]

If you have any questions regarding our response, and would like to discuss it further, please contact Gerri Wallace at 202-268-6821, Corporate Information Security Office.

Ross Philo

Ross Philo

cc: Vincent DeVito
Debbie J. Judy
Charles L. McGann
Joseph J. Gabris
Gregory D. Larrabee
Sally K. Haring

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-6900
FAX: 202-268-4492
ROSS.PHILO@USPS.GOV
WWW.USPS.COM