OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 19, 2009

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

LYNN MALCOLM
VICE PRESIDENT, CONTROLLER

SUBJECT: Audit Report – Fiscal Year 2008 Information Systems General Computer Controls Capping Report (Report Number IS-AR-09-005)

This report summarizes the results of our audit of information systems (IS) 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) 2008 (Project Number 08RD001IS000). We performed this self-initiated audit as part of the FY 2008 financial statements audit. See Appendix A for additional information about this audit.

Conclusion

Overall, general computer controls over 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 IT audit control issues that do not, alone or collectively, represent a significant risk to reliance on general computer controls. We provided recommendations to address these issues during our review.

These issues were in the areas of:

- [redacted].
  [redacted]® [redacted]
- Security clearance processing.
- Periodic application risk assessments.
- [redacted]
- [redacted] plan updates.

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

- Obsolete criteria in [redacted] hardening standards.
- Improper settings, file ownership, and permissions associated with user accounts in the [redacted] environment.
- Improper access to critical and sensitive datasets in the mainframe environment.

We issued four interim reports during our review in FY 2008 to assist management in improving information technology operations (ITO). See Appendix B for summaries of the reports we issued.

We also summarized the status of FY 2008 and previous years' recommendations in Appendix C.[1] See Table 1 in Appendix C for a list of open recommendations and Table 2 for a list of recommendations we have closed.

This report contains no recommendations. Management agreed with the facts as 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 Systems, or me at (703) 248-2100.

E-Signed by Tammy Whitcomb
VERIFY authenticity with ApproveIt
Tammy L. Whitcomb

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

Attachments

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

cc: Ross Philo
Joseph Corbett
Harold E. Stark
Joseph J. Gabris
G. Dean Larrabee
Jo Ann E. Mitchell
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The [redacted] IT/ASCs provide computer processing and accounting services for the U.S. Postal Service. The [redacted] ITSC provides infrastructure services[2] for over 38,000 Postal Service locations. Each of these sites includes multiple service organizations.

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

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

The [redacted] IT/ASC has a similar structure but without a [redacted]

[redacted] deploys, operates, and supports systems and applications for all business units within the Postal Service. The [redacted] 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 Vice President, Information Technology Operations.[3] The ASCs report to the Vice President, Controller.

Finally, 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 the payroll for approximately 700,000 career employees.

[2] Infrastructure services are those IT functions that support the overall Postal Service enterprise and include such areas as telecommunications, distributed computing, and IT Help Desk.
[3] Prior to February 25, 2008, all information technology-related service centers reported to the Vice President, Chief Technology Officer (CTO). They now report to the Vice President, Information Technology Operations.

- Determines the strategic direction for the agency's information technology.

- Employs over 1,000 IT employees located across the continental U.S.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of the audit were to determine if 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; data integrity controls were in place; and business practices complied with Postal Service policies, procedures, and standards. In addition, we evaluated controls over software, data, personnel, and physical security that affect computer systems.

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

- Security Program Planning and Management
- Access Controls
- Application Software Development and Change Control
- System Software Controls
- Corporate-Wide Security Policies and Procedures
- Segregation of Duties
- Service Continuity
- 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 user access to commands and data to determine consistency with policies and procedures.

- Mainframe and mid-range logon IDs to ensure they 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 system controls were effective) and interviewing IT personnel and reviewing vendor documentation.

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

- [redacted][4] [redacted].

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

- Employee and contractor files to verify that security clearances were current.

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

- Facility, workgroup, and application recovery plans and test documentation to verify that management completed and tested service continuity plans.

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

- The 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].[6] These tests provided

[4] [redacted].

[5] *Security Vulnerability Assessment of the* [redacted] (Report Number IS-AR-08-012, dated June 25, 2008).

[6] *Security Vulnerability Assessment of the* [redacted] (Report Number IS-CS-08-001, dated August 29, 2008).

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. In general, we judgmentally selected applications for review based on financial significance, sensitivity, elapsed time since the last review, and the platforms on which they reside. [redacted]

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 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 2007 through March 2009 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 March 4, 2009, 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	Monetary Impact	Report Results
Fiscal Year 2007 Information Systems General Controls Capping Report	IS-AR-08-007	March 11, 2008	None	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas of [redacted], classification of employees in sensitive positions, [redacted], and key inventory management. This report contained no recommendations.
Fiscal Year 2006 Information Systems General Controls Capping Report	IS-AR-07-009	February 26, 2007	None	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas of access to [redacted]. This report contained no recommendations.
Fiscal Year 2005 Information Systems General Controls Capping Report	IS-AR-06-004	March 6, 2006	None	Overall, general computer controls were in place and working effectively. However, additional controls and actions were needed in the areas of [redacted]. This report contained no recommendations.

APPENDIX B: SUMMARY OF REPORTS ISSUED

System Software Controls at the [redacted] *Information Technology and Accounting Service Centers for FY 2008* (Report Number IS-AR-08-011, dated June 3, 2008).

This report presented the results of our audit of system software controls at the [redacted] [redacted] IT/ASCs. The objective of this audit was to determine if management established a framework and continuing cycle of activity for limiting access to system software, monitoring access to and the use of system software, and controlling system software changes. Overall, management adequately configured data systems and platforms to optimize security and appropriately manage risks for the selected applications that we reviewed. [redacted]

We provided three recommendations to (1) develop procedures to ensure [redacted] administrators review exception reports and timely correct [redacted] server settings deficiencies to comply with hardening standards; (2) update [redacted] hardening standards to add applicable audit features and to specify log review and retention requirements; and (3) implement [redacted] system audit features and log review and retention requirements as specified in the revised hardening standards. In addition, management had corrected, or was in the process of correcting, other minor issues that we identified during the review concerning obsolete criteria in the [redacted] hardening standards, awareness of the existence of the Postal Service's [redacted] hardening standards, and obsolete and outdated information regarding administering and installing software patches in a [redacted] environment.

Access Controls at the xxxxx[redacted] *Information Technology and Accounting Service Centers for Fiscal Year 2008* (Report Number IS-AR-08-015, dated August 15, 2008).

This report presented the results of our audit of access controls at the [redacted] [redacted] IT/ASCs. The objective of this audit was to determine whether the Postal Service had 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. Overall, physical access controls for IT facilities and logical access controls [redacted] [redacted] were in place and functioning adequately. However, our testing identified opportunities to improve compliance with these controls. [redacted]

[redacted]

Security Policies and Procedures (Corporate-Wide) at the Information Technology and Accounting Service Centers for Fiscal Year 2008 (Report Number IS-AR-09-002, dated November 13, 2008).

This report presented the results of our audit of corporate-wide security planning and program management at the Postal Service's IT/ASCs located in [redacted]. The objectives were to determine whether management established a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Overall, management established information security policies and procedures to protect critical and sensitive information resources. These included, but were not limited to, [redacted]

However, our review identified opportunities to improve compliance with these policies and procedures. Specifically, management could improve controls by initiating security clearance processing for all employees occupying sensitive positions. In addition, [redacted] We provided four recommendations to: (1) develop a process to ensure security clearances are initiated for individuals in positions classified as sensitive; (2) provide reports to the Security Control Officer on a semiannual basis to track the security clearance status of employees in sensitive positions at the [redacted] IT/ASCs; (3) perform risk reassessments on the six applications reviewed during this audit; and (4) establish milestones to review all sensitive and critical applications for current risk assessments and complete the reassessments on those applications that are not current. In addition, management took corrective action to initiate nine security clearances we identified as missing during the audit.

Service Continuity at the Information Technology and Accounting Service Centers for Fiscal Year 2008 (Report Number IS-AR-09-003, dated January 20, 2009).

This report presented the results of our audit of service continuity at the [redacted], IT/ASCs. The objective of this audit was to determine whether service continuity controls were in place to minimize the risk when unexpected events occur and to ensure critical operations continue without interruption or can be resumed within a reasonable amount of time. Overall, management adequately developed the infrastructure and service continuity processes and procedures to maximize the availability of critical Postal Service operations while minimizing potential risks for service interruption. The Postal Service was undergoing significant changes in the computing infrastructure, including virtualization and replication. To further minimize the risk of service disruption, management could improve processes [redacted] IT/ASC. We made two recommendations to management that included designating personnel responsible for administering the backup process for the [redacted] Center and implementing procedures to ensure [redacted] backup tapes were stored off-site. Additionally, we made two recommendations to management that included clarifying the responsibility for maintaining, administering, and updating the [redacted] plan for [redacted]

APPENDIX C: ACTION ON PRIOR YEAR RECOMMENDATIONS

Table 1: Open Recommendations

Report Number	Recommendation Number	Description	Responsible Organizations							
			CTO/ ITO[7]	[redacted][8]	[redacted]	[redacted][9]	[redacted][10]	USPIS[11]	ERM[12]	Controller
IS-AR-07-017[13]	1(S)[14]	Assess the risk of all IT/ASC positions (career and non-career) for the purpose of assigning them as sensitive.	x					x	x	x
	2	Establish a requirement to periodically reassess 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
	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 the proper clearance level is attributed to the employee.	x					x	x	x

[7] Vice President, CTO. The Postmaster General replaced the CTO position on February 25, 2008, with the ITO position.
[8] IT/ASC, [redacted]
[9] IT/ASC, [redacted]
[10] ITSC, [redacted]
[11] U,S. Postal Inspection Service.
[12] Employee Resources Management.
[13] *Separation of Duties at the* [redacted] *Information Technology and Accounting Service Centers*, dated August 29, 2007.
[14] (S) = Significant.

Table 1: Open Recommendations (cont.)

Report Number	Recommendation Number	Description	Responsible Organizations							
			CTO/ ITO	[redacted]	[redacted]	[redacted]	[redacted]	USPIS	ERM	Corporate IT Portfolio
IS-AR-07-017 (cont.)	5	Amend the *Administrative Support Manual* to designate the Chief Inspector as responsible for defining the criteria for identifying sensitive positions, to specify the criteria for designating a position as sensitive, and to update the list of position types requiring a sensitive clearance.						x		
IS-AR-08-011[15]	1(S)	Develop procedures to ensure [redacted] deficiencies to comply with hardening standards.	x	x	x					
	2	Update [redacted] hardening standards to add applicable audit features and to specify log review and retention requirements.	x	x	x					
	3	Implement [redacted] system audit features and log review and retention requirements as specified in the revised hardening standards.	x	x	x					

[15] *System Software Controls at the* [redacted] *Information Technology and Accounting Service Centers for Fiscal Year 2008*, dated June 3, 2008.

Table 1: Open Recommendations (cont.)

Report Number	Recommendation Number	Description	Responsible Organizations							
			CTO/ ITO	[redacted]	[redacted]	[redacted]	[redacted]	USPIS	ERM	Corporate IT Portfolio
IS-AR-08-015[16]	1	Develop an [redacted] groups.	x	x						
	2	Develop an automated procedure to periodically review [redacted]	x				x			
IS-AR-09-002[17]	2	Provide reports to the Security Control Officer on a semiannual basis to track the security clearance status of employees in sensitive positions at the [redacted] IT/ASCs.							x	
	3	Perform risk reassessments on the six applications reviewed during this audit.	x							
	4	Establish milestones to review all sensitive and critical applications for current risk assessments and complete the reassessments on those applications that are not current.	x							

[16] *Access Controls at the* [redacted] *Information Technology and Accounting Service Centers for Fiscal Year 2008*, dated August 15, 2008.

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

Table 1: Open Recommendations (cont.)

Report Number	Recommendation Number	Description	Responsible Organizations							
			CTO/ ITO	[redacted]	[redacted]	[redacted]	[redacted]	USPIS	ERM	Corporate IT Portfolio
IS –AR-09-003[18]	1	Designate personnel responsible for administering the [redacted].	x							
	2(S)	Implement procedures to ensure [redacted]	x							
	3	Clarify the responsibility for maintaining and administering the [redacted] IT/ASC.	x							
	4	Update the [redacted] IT/ASC.	x							

[18] *Service Continuity at the Information Technology and Accounting Service Centers for Fiscal Year 2008*, dated January 20, 2009.

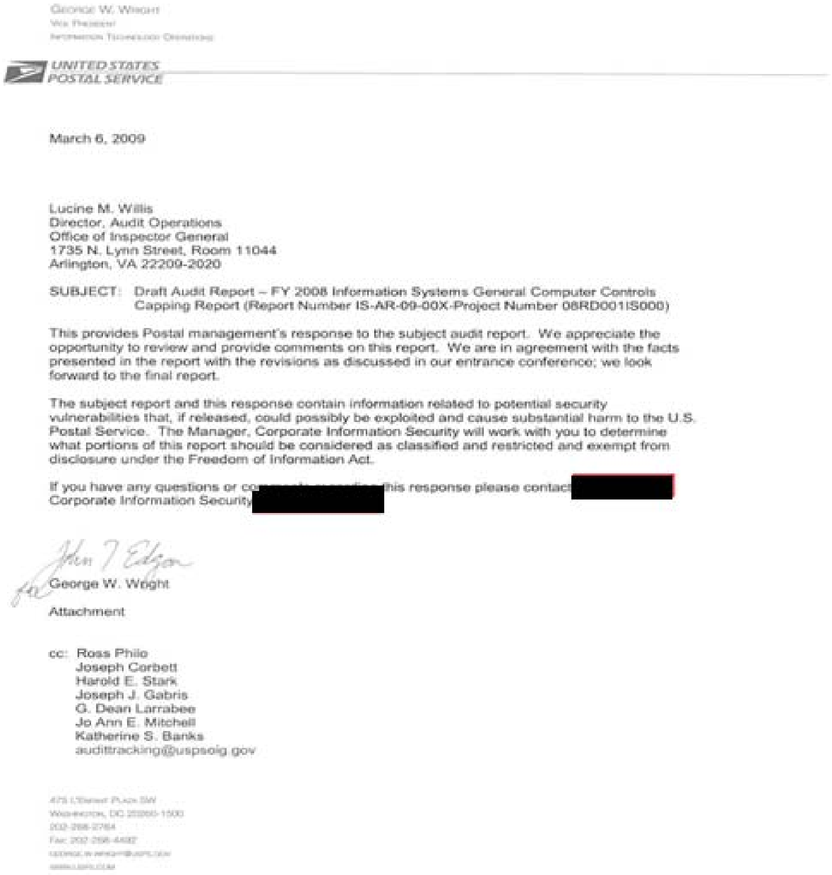
Table 2: Closed Recommendations

Report Number	Recommendation Number	Responsible Organization					
		CTO	[redacted]	[redacted]	[redacted]	[redacted]	ERM
IS-AR-07-018[19]	1	x	x	x			
	3	x	x	x			
IS-AR-08-002[20]	1	x				x	
	2(S)	x			x		
	3	x					
	5(S)	x				x	
IS-AR-09-002	1						x

[19] [redacted] *Information Technology and Accounting Service Centers for Fiscal Year 2007*, dated September 14, 2007.

[20] *Information System Access Controls at Selected Information Technology Facilities for Fiscal Year 2007*, dated November 6, 2007.

APPENDIX D: MANAGEMENT'S COMMENTS



George W. Wright
Vice President
Information Technology Operations

UNITED STATES
POSTAL SERVICE

March 6, 2009

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

SUBJECT: Draft Audit Report – FY 2008 Information Systems General Computer Controls Capping Report (Report Number IS-AR-09-00X-Project Number 08RD001IS000)

This provides Postal management's response to the subject audit report. We appreciate the opportunity to review and provide comments on this report. We are in agreement with the facts presented in the report with the revisions as discussed in our entrance conference; we look forward to the final report.

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 co[redacted]his response please contact[redacted]
Corporate Information Security

John T. Edgar
for George W. Wright

Attachment

cc: Ross Philo
Joseph Corbett
Harold E. Stark
Joseph J. Gabris
G. Dean Larrabee
Jo Ann E. Mitchell
Katherine S. Banks
audittracking@uspsoig.gov

475 L'Enfant Plaza SW
Washington, DC 20260-1500
202-268-2764
Fax: 202-268-4492
george.w.wright@usps.gov
www.usps.com