OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 12, 2011

DEBORAH J. JUDY
DIRECTOR, INFORMATION TECHNOLOGY OPERATIONS

GREGORY D. LARRABEE
MANAGER, RALEIGH INFORMATION TECHNOLOGY SERVICE CENTER

SUBJECT: Audit Report – Fiscal Year 2010 Selected Information Technology General Controls (Report Number IT-AR-11-002)

This report presents the results of our audit of Information Technology (IT) general controls (Project Number 10RD001IT000). We conducted this audit in support of the independent public accounting (IPA) firm's overall audit opinions on the U.S. Postal Service's financial statements and internal controls over financial reporting.[1] Our objective was to evaluate and test infrastructure level internal controls over the information systems at the Postal Service Information Technology and Accounting Service Centers (IT/ASCs) and the [redacted] Information Technology Service Center (ITSC). This report summarizes the results of the nine IT process areas[2] we tested. This audit addresses financial risk. See Appendix A for additional information about this audit.

The Postal Reorganization Act of 1970, as amended, requires annual audits of the Postal Service's financial statements. Also, the U.S. Congress enacted Sarbanes-Oxley (SOX) legislation in calendar year 2002 to strengthen public confidence in the accuracy and reliability of financial reporting. Section 404 of SOX requires management to state its responsibility for establishing and maintaining an adequate internal control structure and make an assertion on the effectiveness of the internal control structure over financial reporting. The Postal Accountability and Enhancement Act of 2006 requires the Postal Service to comply with Section 404 of SOX beginning in fiscal year (FY) 2010. The Board of Governors contracted with the IPA to express an opinion on the Postal Service's financial statements. Beginning in FY 2010, that responsibility was expanded to include an opinion on the Postal Service's internal control over financial reporting.

[1] The IPA maintains overall responsibility for testing and review of all IT controls. The U.S. Postal Service Office of Inspector General (OIG) coordinated audit work with the IPA to ensure adequate coverage.
[2] See Appendix A for additional information about the IT process areas reviewed.

Conclusion

Infrastructure level internal controls in the areas we tested were properly designed and operating effectively. However, by strengthening controls over database and server security settings, management can reduce the risk of a compromise that could negatively affect the confidentiality, integrity, and availability of information resources and data.

Oracle Database Configuration Settings

Management did not properly configure security settings on Oracle databases. Specifically, [redacted] This occurred, because the database administrator did not thoroughly review configuration settings on these databases after installing upgrades or a new operating system.

Properly configured accounts and profiles prevent unauthorized users from gaining access to sensitive information resources and making unauthorized changes to data or programs. The Database Support Services group corrected these issues during the course of our review; therefore, we are not making any recommendations regarding corrective actions. See Appendix B for a detailed analysis of this topic.

The data in [redacted] we reviewed are potentially at risk, which affects information technology. We quantified the costs associated with this risk, using a single database supporting the [redacted] at approximately [redacted] See Appendix C for our calculation of data at risk

Windows Server Management

Security settings on Windows servers were not in compliance with Postal Service policy.[6] While performing our review of [redacted] Windows servers, we identified non-compliant:

- [redacted]
- [redacted].
- [redacted]

[3] [redacted]

Computer software, networks, and data that are vulnerable or at risk of loss because of fraud, inappropriate, or unauthorized disclosure of sensitive data, or disruption of critical Postal Service operations and services.

[6] Handbook AS-805, *Information Security,* Section 9-6.1.12, [redacted] dated February 2010.

The [redacted] occurred, because administrators supporting servers were not always notified when Information Technology Engineering and Architecture updated the [redacted][7] Further, although management performs periodic reviews of Windows software and settings, they did not correct the discrepancies identified during their reviews. As a result, [redacted]

The [redacted] occurred, because configurations o [redacted] were not centrally managed, for example, by using Active Directory.[8]

Properly configuring accounts reduces the risk of unauthorized users gaining access to sensitive information resources and making unauthorized changes to data or programs. Management corrected these discrepancies on the servers we reviewed; however, these conditions could exist on other Windows servers we did not review.[9] See Appendix B for our detailed analysis of this topic.

We recommend the director, Information Technology Operations, direct the manager, [redacted] Information Technology Service Center, to:

1. Develop a procedure to notify administrators supporting Windows servers when [redacted] are available.

2. Correct discrepancies identified by the periodic reviews of all Windows servers, as appropriate.

3. Develop a methodology to centrally manage all [redacted]

Management's Comments

Management agreed with our recommendations. However, management stated they could not validate the accuracy of the information in Appendix C (Other Impacts) and believe the estimated potential cost to the Postal Service reported for data at risk reflects a worst case scenario.

In response to recommendation 1, management stated that all GPO implementations are submitted and approved through the change request process. They will implement an additional notification process with groups responsible for administration of GPOs on the Windows servers. Target completion date is March 31, 2011.

[7] [redacted]

[8] A directory service that provides the means to manage the identities and relationships that make up network environments.

[9] Where we limited our review to 22 Windows servers, there are approximately 300 Windows servers that support the in-scope SOX applications that could also be vulnerable to these conditions.

In response to recommendation 2, management will conduct periodic reviews of Windows baseline configurations in February and August of each year. Within 30 days of the review completion, management will produce an action plan that identifies each discrepancy and the group assigned to correct the problem. The results will be posted in the SOX artifact library. In addition, management will review the baseline standard build annually. Target completion date is September 30, 2011.

To address recommendation 3, management updated Handbook AS-805 to prohibit local accounts listing exceptions of built-in accounts and accounts required by commercial-off-the-shelf applications approved in eAccess. The identification and approval of local accounts will be part of the semiannual review process. Target completion date is September 30, 2011. See Appendix E for management's comments, in their entirety.

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to the recommendations and the actions taken should correct the issues identified in the report. Additionally, we do not believe our other impacts represent a worst case scenario; rather, they represent a historical industry average of the cost associated with the disclosure of personally identifiable information.

The OIG considers all of the recommendations significant and, therefore, requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations 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.

E-Signed by Darrell E. Benjamin, Jr
VERIFY authenticity with ApproveIt

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

Attachments

cc: Ellis A. Burgoyne
Joseph Corbett
Vincent H. Devito
Harold E. Stark
Charles L. McGann, Jr.
Corporate Audit and Response Management

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The Postal Service SOX and Process Improvement office established the IT SOX Compliance Management Office (CMO) to manage the annual documentation, testing, remediation, reporting, and certification requirements to meet and maintain IT SOX compliance. The IT SOX CMO is responsible for developing and implementing internal IT SOX master controls,[10] both general computer and application-specific controls.

The [redacted] and [redacted] IT/ASCs provide computer processing and accounting services for the Postal Service. The [redacted] ITSC provides infrastructure services for approximately [redacted] Postal Service locations. Each site includes multiple service organizations that deploy and support systems and applications; provide accounting and finance activities; and perform application development, enhancement, and maintenance of systems that enable the Postal Service to achieve its business objectives. As of June 2010, these organizations support [redacted] financial[11] applications and [redacted] IT-related applications or infrastructure components.[12]

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to evaluate and test infrastructure level internal controls over the information systems at the Postal Service IT/ASCs and other related IT organizations. Specifically, we reviewed IT master controls designed to mitigate risks associated with [redacted] IT process areas that support in-scope financial applications.[13]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[10] A uniquely named control designed to mitigate risk associated with the infrastructure (for example, database, operating system, and so forth.) supporting in-scope financial applications. Master controls are either general in nature (for example, addressing Active Directory security parameters) or application unique (for example, tailored specifically for the [redacted] .

[11] The IT SOX CMO considers these significant business applications supporting an in-scope business process.

[12] The IT SOX CMO determined that these IT systems have a comprehensive impact on the IT control environment or are relied on by in-scope applications for coverage of controls.

[13] SOX in-scope applications include financial applications supporting in-scope business processes and IT applications that have a pervasive impact on the IT control environment.

[14] An [redacted]

The IT SOX CMO identified [redacted] master controls to cover the IT process areas we reviewed. See Tables 2 and 3 in Appendix D for a detailed list of master controls we reviewed for each IT process area.

To accomplish our objective, we interviewed administrators, observed key processes and procedures, and reviewed applicable Postal Service policies. We selected samples of SOX in-scope applications, servers, and SOX-related notifications for detailed control testing and analysis. We performed all system queries in a controlled environment with management's full knowledge and approval. We conducted our audit at the [redacted] [redacted] and [redacted] IT/ASCs and the [redacted] ITSC.

We conducted this performance audit from October 2009 through January 2011 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 discussed our observations and conclusions with management on December 3, 2010, and included their comments where appropriate.

We assessed the reliability of computer-generated data by reviewing configuration files obtained from the audited systems and interviewing appropriate managers who were knowledgeable about the data. We also reviewed existing information about the data and the operating systems/platforms that produced the data. We determined that the data were sufficiently reliable for the purposes of this report.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date Report	Results
Fiscal Year 2009 Information Systems General Controls Capping Report	IS-AR-10-005	3/31/2010	Overall, general computer controls were in place and working effectively. However, we identified issues in the following areas in four interim audit reports: semiannual building key surveys and reviews of identification badge access control lists; UNIX time-out sessions and unnecessary system and network services; network component management and monitoring, authentication protocols, and data encryption transmissions; and maintaining Windows Active Directory objects and domain controllers not meeting security standards. This capping report contained no additional recommendations, as the issues

			were addressed in separate audit reports issued to management.
Fiscal Year 2008 Information Systems General Controls Capping Report	IS-AR-09-005	3/19/2009	Overall, general computer controls were in place and working effectively. However, four interim audit reports addressed additional controls and actions needed in the areas of UNIX script monitoring, groups management, audit configurations, and log monitoring; Oracle default profiles; security clearance processing; periodic application risk assessments; off-site storage of UNIX tapes; and facility recovery plan updates. This capping report contained no additional recommendations, as the issues were addressed in separate audit reports issued to management.
Fiscal Year 2007 Information Systems General Controls Capping Report	IS-AR-08-007	3/11/2008	Overall, general computer controls were in place and working effectively. However, five interim audit reports addressed additional controls and actions needed in the areas of Oracle database security settings, Windows password settings, classification of employees in sensitive positions, application recovery testing, and key inventory management. This capping report contained no additional recommendations, as the issues were addressed in separate audit reports issued to management.

APPENDIX B: DETAILED ANALYSIS

Oracle Database Configuration Settings

Management did not properly configure security settings on Oracle databases. Specifically, system accounts on [redacted] of the [redacted] databases supporting four in-scope applications still [redacted] In addition, Oracle accounts assigned to the [redacted] had the [redacted] on one database.[15] [redacted]

[redacted]

Postal Service policy[17] requires management to [redacted] to the Postal Service network. Oracle database policy requires management to [redacted] after installation. Properly configuring [redacted] reduces the risk of unauthorized users gaining access or making changes to sensitive information, data or programs.

Windows Server Management

Security settings on Windows servers were not in compliance with Postal Service policy.[19] While performing our review of [redacted] Windows servers, we identified non-compliant:

- [redacted]
- [redacted].
- [redacted]

[15] The [redacted] database supporting the [redacted]

[16] [redacted]

Handbook AS-805, *Information Security,* Sections 9-6.1.11, [redacted] and 9-6.1.12 [redacted] February 2010.

Security Hardening Standards Oracle Databases, Version 2.1, Section 5.8, Enable password management, dated September 3, 2009.

[19] Handbook AS-805, Section 9-6.1.12, [redacted]

Table 1 shows the servers [redacted] setting issues. We identified these issues across [redacted] servers; [redacted] of the [redacted] servers had a [redacted].

Table 1: Password and Account Lockout Settings Issues

Number	Server Name/Application	Password Setting	Account Lockout Setting
1	[redacted]		[redacted]
2	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]
4	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]
6	[redacted]	[redacted]	[redacted]
7	[redacted]	[redacted]	
8	[redacted]	[redacted]	[redacted]

System administrators create domains and use Active Directory to manage security and objects. The Postal Service has multiple domains such as *USA* production, development, secure enclaves, and demilitarized zones (DMZ).[20] During our review, we found that servers outside the [redacted] *domain* did not receive [redacted] [redacted], because administrators supporting these servers were not always notified of the [redacted] Additionally, we found that servers inside the [redacted] *domain* did not receive [redacted], because of software and configuration issues such as ports that were not open. Unless [redacted] are properly applied, management cannot ensure the Windows servers are adequately secured to reduce the risk of unauthorized access to applications and data.

[redacted] on [redacted] of the [redacted] servers had not been updated. The [redacted] is designed primarily for initial logon and configuration of a local computer. The [redacted] to avoid the potential for a computer security breach. Postal Service policy states [redacted] considered sensitive (for example, [redacted] system supervisors, software specialists, system administrators, or vendor-supplied) must be changed at least every 30 days.

[20] Enclaves can be implemented to enforce separate security zones; DMZs are network segments in between intranets, extranets, and the Internet that provide increased security for data transfer between information resources, vendors, and the public.

[21] [redacted] is an infrastructure that allows you to implement specific configurations for users and computers. [redacted] which are linked to Active Directory service containers such as sites, domains, or organizational units.

[22] Handbook AS-805, Section 9-6.1.12, [redacted]

APPENDIX C: OTHER IMPACTS

Data at Risk

The following presents an estimate of the potential costs the Postal Service could incur from the disclosure of personally identifiable information. We based the other impact of [redacted] on an estimate of [redacted] sensitive records stored in two database tables containing sensitive data elements related to the E-Facilities Management System. The calculation assumes each record would contain at least one element of sensitive information.

Cost Category	Costs per Customer Affected as Reported by the Ponemon Institute[23]
Detection and Escalation	
Activities that enable a company to reasonably detect breach of personal data either at high risk (in storage) or in motion; activities necessary to report the breach of protected information to appropriate personnel within a specified period.	[redacted]
Notification	
Activities that enable a company to notify data subjects with a letter, outbound telephone call, e-mail or general notice that personal information was lost or stolen.	[redacted]
Ex-Post Response	
Activities to help victims of a breach communicate with the company to ask additional questions or obtain recommendations to minimize potential harms. Redress activities also include ex-post responses such as a credit report monitoring or reissuance of a new account (or credit card).	[redacted]
Total	[redacted]

[23] Ponemon Institute, LLC, *Fifth Annual US Cost of Data Breach Study*, dated January 2010.

[24] The Ponemon Institute study included a cost category for "lost business" with a cost per customer of [redacted] per record. We have excluded this cost from our calculation, because we do not believe it is a fair representation of the potential cost the Postal Service could incur for this category.

APPENDIX D: TEST RESULTS AND DETAILS

Table 2 shows the level of compliance for the [redacted] Windows and Oracle SOX master controls we tested.

Table 2: IT Master Controls Compliance

IT Master Controls Compliance							
Master Control Number	Master Control	Windows			Oracle		
		Sample Size (Servers)	Number Tested/ Passed	Percentage of Servers Compliant	Sample Size (Databases)	Number Tested/ Passed	Percentage of Databases Compliant
1	Account Suspension	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	Administrative Password Management	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3	Configuration Baseline	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
4	Default Account Password Change	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
5	Separation of Duties	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6	Password Parameter Configuration	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
7	Password Encryption	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
8	Patch Management	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
9	Security Log Monitor Configuration	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
10	Testing Documentation	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted] The IT SOX CMO did not identify the Administrative Password Management master control for Windows operating systems.

[26] We reviewed the results of a separate script for the separation of duties master control. There were [redacted] databases in the universe when we performed our review.

[27] Based on the number of control IDs rather than number of servers.

[28] We did not test Patch Management or Testing Documentation master controls, because management recommended not applying the current patches, which they considered not critical enough to apply across all Oracle databases. Additionally, at the time of our testing, DBSS management had not determined an efficient process to install patches across the scope of all the in-scope Oracle databases. Patch installation requires each of the databases ([redacted] at the time of our testing) to be shut down.

[29] The IT SOX CMO did not identify the Security Log Monitor Configuration master control for Oracle databases.

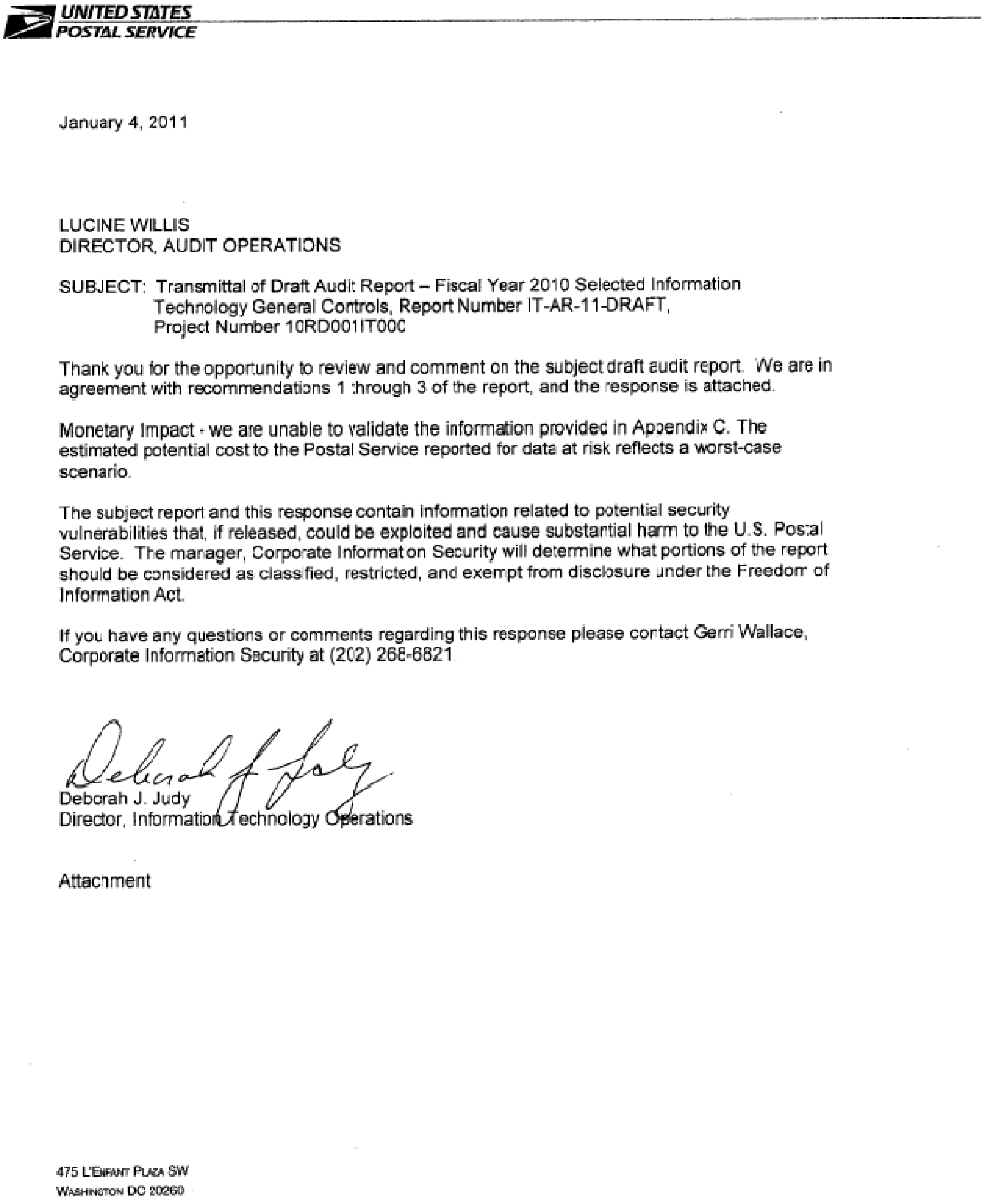
Table 3 presents the master controls the IT SOX CMO identified for the seven remaining IT process areas we tested. The numbers in the table summarize the sampled number of items tested and the number of sampled items passed for each of the master controls identified. The variation in the sample numbers is attributed to the size of the universe, the assessed risk of the area, and consideration of whether expanding the sample would likely conclude that an exception would be more likely.

Table 3: IT Process Areas and Master Controls Tested

Master Controls Identified for Testing	IT Process Areas Tested						
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Account Management Responsibility				[redacted]			
Account Suspension	[redacted]			[redacted]	[redacted]		[redacted]
Administrative Password Management				[redacted]	[redacted]		
Configuration Baseline		[redacted]	[redacted]				[redacted]
Default Account Password Change	[redacted]	[redacted]		[redacted]	[redacted]		
Inactivity Timeout	[redacted]					[redacted]	
Password Encryption	[redacted]			[redacted]	[redacted]		[redacted]
Password Parameter Configuration	[redacted]			[redacted]	[redacted]		[redacted]
Patch Management		[redacted]	[redacted]				
Review Security Logs	[redacted]	[redacted]			[redacted]		
Security Log Monitor Configuration	[redacted]	[redacted]		[redacted]	[redacted]		
Semi-Annual Account Review				[redacted]			
Separation of Duties	[redacted]			[redacted]	[redacted]		[redacted]
Shared Manager Account Provisioning				[redacted]			
Testing		[redacted]	[redacted]				

Master Controls Identified for Testing	IT Process Areas Tested						
	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
Documentation							
UDS Managed Account Suspension							[redacted]
UDS Managed Password Parameter							[redacted]
UDS Managed Password Encryption							[redacted]
Network Connection Authorization						[redacted]	
Firewall Management						[redacted]	
Network Archive Documentation						[redacted]	
Virtual Private Network Access Management						[redacted]	

APPENDIX E: MANAGEMENT'S COMMENTS



UNITED STATES
POSTAL SERVICE

January 4, 2011

LUCINE WILLIS
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Transmittal of Draft Audit Report – Fiscal Year 2010 Selected Information Technology General Controls, Report Number IT-AR-11-DRAFT, Project Number 10RD001IT000

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

Monetary Impact - we are unable to validate the information provided in Appendix C. The estimated potential cost to the Postal Service reported for data at risk reflects a worst-case scenario.

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

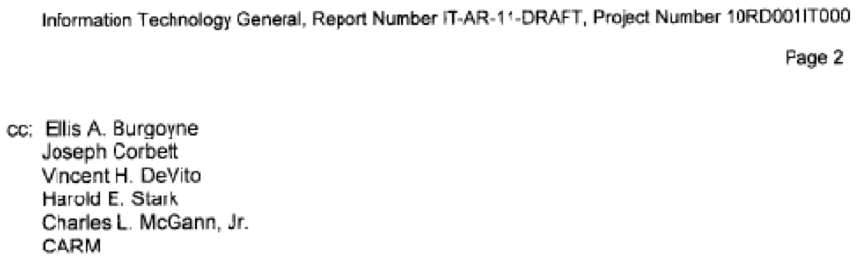
If you have any questions or comments regarding this response please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.

Deborah J Judy

Deborah J. Judy
Director, Information Technology Operations

Attachment

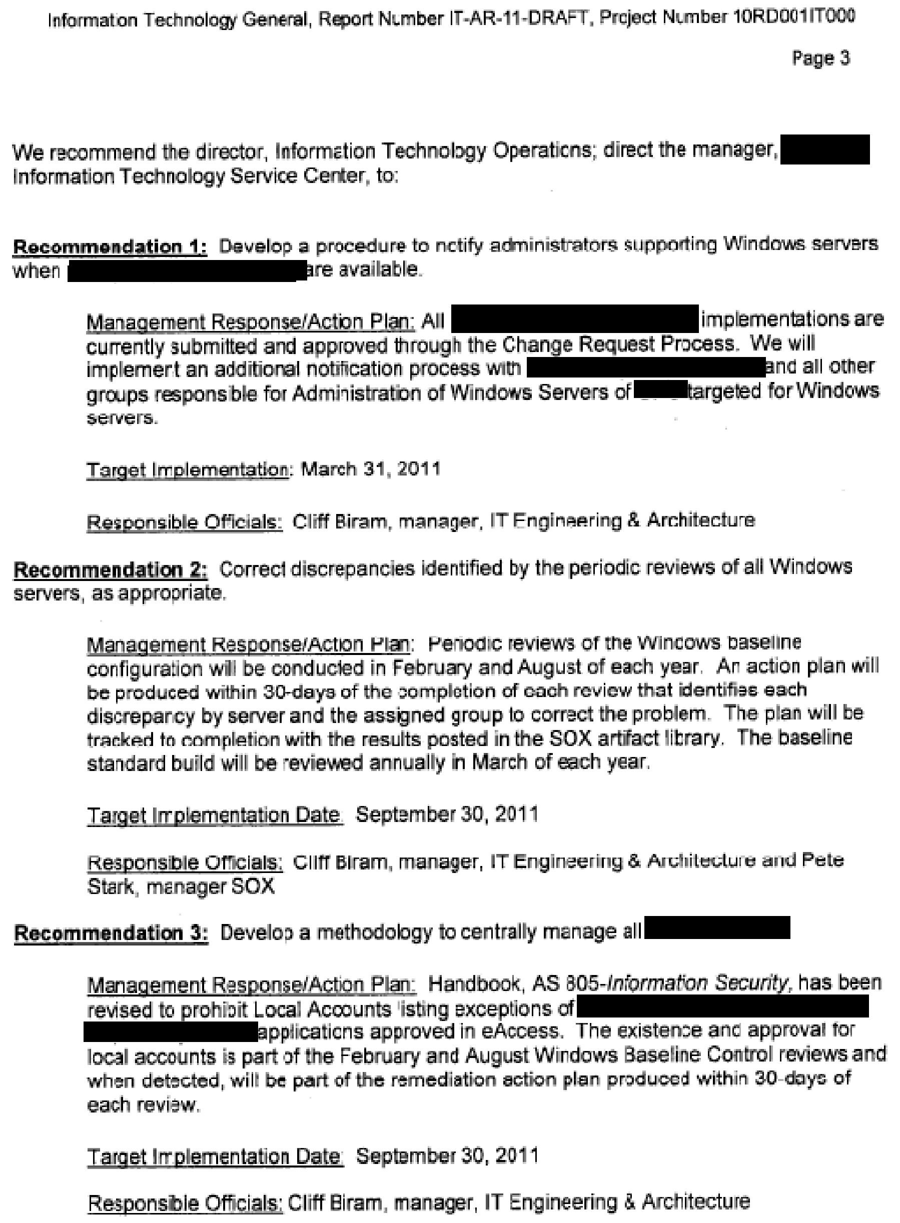
475 L'Enfant Plaza SW
Washington DC 20260



Information Technology General, Report Number IT-AR-11-DRAFT, Project Number 10RD001IT000

Page 2

cc: Ellis A. Burgoyne
Joseph Corbett
Vincent H. DeVito
Harold E. Stark
Charles L. McGann, Jr.
CARM



We recommend the director, Information Technology Operations; direct the manager, [redacted] Information Technology Service Center, to:

Recommendation 1: Develop a procedure to notify administrators supporting Windows servers when [redacted] are available.

Management Response/Action Plan: All [redacted] implementations are currently submitted and approved through the Change Request Process. We will implement an additional notification process with [redacted] and all other groups responsible for Administration of Windows Servers of [redacted] targeted for Windows servers.

Target Implementation: March 31, 2011

Responsible Officials: Cliff Biram, manager, IT Engineering & Architecture

Recommendation 2: Correct discrepancies identified by the periodic reviews of all Windows servers, as appropriate.

Management Response/Action Plan: Periodic reviews of the Windows baseline configuration will be conducted in February and August of each year. An action plan will be produced within 30-days of the completion of each review that identifies each discrepancy by server and the assigned group to correct the problem. The plan will be tracked to completion with the results posted in the SOX artifact library. The baseline standard build will be reviewed annually in March of each year.

Target Implementation Date September 30, 2011

Responsible Officials: Cliff Biram, manager, IT Engineering & Architecture and Pete Stark, manager SOX

Recommendation 3: Develop a methodology to centrally manage all [redacted]

Management Response/Action Plan: Handbook, AS 805-*Information Security*, has been revised to prohibit Local Accounts listing exceptions of [redacted] applications approved in eAccess. The existence and approval for local accounts is part of the February and August Windows Baseline Control reviews and when detected, will be part of the remediation action plan produced within 30-days of each review.

Target Implementation Date: September 30, 2011

Responsible Officials: Cliff Biram, manager, IT Engineering & Architecture