



OFFICE OF **INSPECTOR GENERAL**

UNITED STATES POSTAL SERVICE

Fiscal Year 2014 Information Technology Internal Controls

Audit Report

Report Number
FT-AR-15-005

March 30, 2015





OFFICE OF INSPECTOR GENERAL

UNITED STATES POSTAL SERVICE

Highlights

Our objective was to evaluate and test key financial reporting infrastructure-level internal controls over information systems at Postal Service Information Technology (IT) and Accounting Services and related IT organizations.

Background

The Postal Accountability and Enhancement Act of 2006 required the U.S. Postal Service to begin complying with sections of the Sarbanes-Oxley (SOX) Act in fiscal year (FY) 2010. Specifically, management must assert on the effectiveness of the internal control structure over financial reporting. We conducted this audit to support the independent public accounting firm's overall audit opinions on the Postal Service's financial statements and internal controls over financial reporting.

The information technology (IT) infrastructure-level environment includes processes needed to administer, secure, and monitor key financial reporting systems. Our objective was to evaluate and test key infrastructure-level internal controls over information systems. We limited the scope of our audit in FY 2014 to the primary financial reporting infrastructure-level controls management identified to fully mitigate SOX risks. Further, our audit did not address the entire IT environment but only in-scope, SOX financial reporting systems.

What The OIG Found

We identified opportunities to strengthen certain key financial reporting infrastructure-level internal controls that would reduce the risk of compromised information resources. During our audit, management remediated issues we identified regarding

server management. For security log reviews, management will evaluate the control and procedures due to the recent cyber intrusion incident. We will review these actions as part of future oversight work.

Management also remediated five issues we identified regarding mainframe management approvals, badge access reviews, password policy, server management, and fire suppression inspections. We agreed with the actions taken to address the issues.

Other infrastructure-level internal controls that we tested were properly designed and operating effectively. Specifically, both database password security and account suspension settings and the operating system separation of duties controls properly functioned.

Further, management remediated 12 issues from prior years related to protecting servers against malicious threats and improving job process monitoring. Management is currently remediating eight issues reported during FYs 2011 and 2012 related to managing configuration baselines, and testing patches to operating systems and databases.

The issues identified do not prevent reliance on infrastructure-level controls for accurate and timely financial reporting. Corrective actions should reduce the risk of additional compromises that can harm the confidentiality, integrity, and

availability of information resources, including financial data; and preserve customer confidence in the Postal Service's brand. However, these actions do not entirely mitigate the effects of a recent cyber intrusion incident. Management developed a multiple phase remediation plan and has already implemented one phase for the cyber intrusion incident. They plan to implement subsequent phases in FY 2015.

What The OIG Recommended

We made no recommendations because management has actions planned by June 30, 2015, or took corrective action to resolve the issues noted during the audit.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

March 30, 2015

MEMORANDUM FOR: JOHN T. EDGAR
VICE PRESIDENT, INFORMATION TECHNOLOGY

A rectangular box containing a handwritten signature in black ink that reads "John E. Cihota". A black dot is visible in the top right corner of the box.

FROM: John E. Cihota
Deputy Assistant Inspector General
for Finance and Supply Management

SUBJECT: Audit Report – Fiscal Year 2014 Information
Technology Internal Controls
(Report Number FT-AR-15-005)

This report presents the results of our audit of the Fiscal Year 2014 Information Technology Internal Controls (Project Number 14BM003IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Lorie Nelson, director, Finance, or me at 703-248-2100.

Attachments

cc: Julie S. Moore
Corporate Audit and Response Management

Table of Contents

Cover	
Highlights.....	1
Background.....	1
What The OIG Found.....	1
What The OIG Recommended	2
Transmittal Letter.....	3
Findings.....	5
Introduction	5
Conclusion	5
██████████ Server Management.....	6
██████████ Security Log Reviews.....	7
██████████ Management Approvals	7
Badge Access Reviews.....	8
██████████ Password Policy	8
██████████ Server Management.....	9
Fire Suppression Inspections.....	9
Status of Open Information Technology Issues Reported in Prior Years	10
Recommendations.....	11
Appendices.....	12
Appendix A: Additional Information	13
Background	13
Objective, Scope, and Methodology.....	15
Prior Audit Coverage	17
Appendix B: Prior Years' Information Technology Issues Closed in Fiscal Year 2014	18
Appendix C: Status of Open Information Technology Issues Reported in Prior Years	21
Appendix D: Trademark Information	23
Contact Information.....	24

Findings

We identified opportunities to strengthen certain key financial reporting infrastructure-level internal controls that would reduce the risk of compromised information resources.

Introduction

This report presents the results of our audit of Fiscal Year (FY) 2014 Information Technology Internal Controls (Project Number 14BM003IT000). We conducted this self-initiated 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 key financial reporting infrastructure-level internal controls² over information systems at Postal Service Information Technology (IT) and Accounting Services and related IT organizations. We limited the scope of our audit in FY 2014 to the primary controls management identified to fully mitigate Sarbanes-Oxley (SOX) Act³ risks. Further, our audit did not address the entire IT environment but only in-scope SOX financial reporting systems. During the audit, we met regularly with the IPA firm and Postal Service representatives to report and discuss remediation efforts, testing tools, initial test results, and control deficiencies.⁴ 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. In addition, the SOX Act was enacted to strengthen public confidence in the accuracy and reliability of financial reporting. Section 404 of SOX requires management to state responsibility for establishing and maintaining adequate internal controls over financial reporting. The Postal Accountability and Enhancement Act of 2006⁵ requires the Postal Service to comply with Section 404 of SOX.

The Postal Service's Management Controls and Integration group oversees testing for finance issues and reports to the Office of Controller. The IT Compliance Management Office (CMO) tests and maintains compliance for the IT infrastructure-level controls and reports issues to the vice president, Information Technology. These infrastructure-level controls are referred to as IT SOX master controls,⁶ including both general computer and application-specific controls.

The Postal Service Board of Governors contracted with an IPA firm to express opinions on the Postal Service's financial statements and internal controls over financial reporting. Our audit augments the IPA firm's opinion.

Conclusion

We identified opportunities to strengthen certain key financial reporting⁷ infrastructure-level internal controls that would reduce the risk of compromised information resources.⁸ During our audit, management remediated issues we identified related to [REDACTED] server management. For [REDACTED] security log reviews, management will evaluate the control and procedures due to the recent cyber intrusion incident.⁹ We will validate corrective actions taken or to be taken as part of future oversight work. Management also

-
- 1 The IPA firm maintains overall responsibility for testing and reviewing all IT controls. The U.S. Postal Service Office of Inspector General (OIG) coordinated audit work with the IPA firm to ensure adequate coverage.
 - 2 Infrastructure-level controls are designed to mitigate risk associated with the infrastructure (for example, database, operating system, and so forth) supporting in-scope financial applications. These controls are either general in nature or application unique. A key control is designed to prevent or detect financial statement misstatements.
 - 3 Public Law 107-204, enacted July 30, 2002.
 - 4 A control deficiency exists when the design or operation of a control does not allow management, in the normal course of performing its assigned functions, to prevent or detect and correct misstatements timely.
 - 5 Public Law 109-435, enacted December 20, 2006.
 - 6 A uniquely named control designed to mitigate risks associated with the infrastructure (for example, database, operating system, and so forth) supporting in-scope financial applications. IT SOX master controls are either general in nature (such as addressing security parameters) or application-unique (tailored specifically for the accounting reporting application).
 - 7 Our review did not address the entire IT environment but only SOX in-scope financial reporting systems.
 - 8 Information resources are all Postal Service information assets, including information systems, hardware, software, data, applications, telecommunications networks, computer-controlled mail processing equipment, and related resources and the information they contain.
 - 9 The Postal Service issued a notification on November 10, 2014, that a cyber intrusion had occurred, that compromised employee data, customer care data, and, potentially, workers' compensation claims data. While management has developed a multiple-phase remediation plan and implemented one phase, they plan to implement subsequent phases in FY 2015.

remediated five issues we identified regarding [REDACTED] management approvals, badge access reviews, [REDACTED] password policy, [REDACTED] server management, and fire suppression inspections. We agreed with management's corrective actions to address the five issues.

Other infrastructure-level internal controls that we tested were properly designed and operating effectively. Specifically, [REDACTED] database software controls functioned properly when we tested the password security and account suspension settings. Additionally, the [REDACTED] operating system separation of duties controls properly restricted developer access to the production environment.

Further, management remediated 12 issues from prior years related to protecting servers against malicious threats and improving job process monitoring. Management is currently remediating eight issues reported during FYs 2011 and 2012 related to managing configuration baselines, and testing patches to operating systems and databases.

The issues identified do not prevent reliance on infrastructure-level controls for accurate and timely financial reporting. Corrective actions should reduce the risk of additional compromises that can harm the confidentiality, integrity, and availability of information resources; and preserve customer confidence in the Postal Service brand. However, these actions do not entirely mitigate the effects of a recent cyber intrusion incident. See [Appendix B](#) for corrective actions.

Based on the audit results, we are not making any recommendations. Accordingly, management chose not to formally respond to this report.

[REDACTED] Server Management

A [REDACTED] stand-alone¹⁰ server failed all [REDACTED]. According to management, this occurred because the stand-alone server was built to comply with configuration baseline standards in effect at the time it was built. However, as standards changed, the [REDACTED] were not updated. [REDACTED]

[REDACTED]

[REDACTED] Management addressed this issue in October 2014.

The OIG has not validated the corrective action taken but will test this issue as part of future oversight work. Therefore, we made no recommendation.

[REDACTED]

Security Log Reviews

While the control for [REDACTED]¹⁴ operates properly,¹⁵ the process used to identify suspicious activity during security log reviews for AD needs improvement. To assist their reviews, the [REDACTED]¹⁶ automatically generates a report for the Directory Services and Server Engineering group¹⁷ to determine whether any suspicious activity exists. [REDACTED]

After the [REDACTED] report review, the Directory Services and Server Engineering group executes a separate [REDACTED] management was aware of this issue but did not correct the program. Due to the recent cyber intrusion incident of the Postal Service's information systems and an ongoing investigation, IT CMO management stated they were temporarily discontinuing discussions regarding this process improvement. However, as part of the response to address the cyber intrusion incident, the CMO will completely evaluate the control and procedures and expects to resolve this issue in Quarter 3, FY 2015. The OIG will validate the corrective action as part of future oversight work. Therefore, we made no recommendation.

By continuing to improve controls in these areas, management can reduce the risk of a security compromise and increase the likelihood of timely detection to protect the confidentiality, integrity, and availability of information resources and data.

Management Approvals

System Software Branch (SSB) management did not post [REDACTED] approvals to the IT Procedures Artifact Library (artifact library) timely.²² Specifically, the [REDACTED]

¹⁷ This group provides several IT services, including user authentication and controls to information resources, deployment of software, hardware validation, and server hardening and backup.

[REDACTED] were reset and uploaded to the artifact library²⁷ on October 30, 2013, to await approval. However, management did not meet the control procedures²⁸ requirement to post the baseline approvals annually within 10 days after October 31.²⁹ In these cases, the approvals were not completed until May 22, 2014, and June 11, 2014. This occurred due to recent changes to the control procedures. Instead of approving all baselines on one document, the revised procedures required management to upload a separate approval for each baseline to the artifact library. By the time management understood the new procedures, they had overlooked three of the four approvals. If management does not post mainframe approvals timely, there is no assurance that management is reviewing the configuration baseline changes and recording them according to the change management process. This could lead to security weaknesses in the [REDACTED] or [REDACTED] subsystem.³⁰

Management posted separate approvals for each configuration baseline by the November 10, 2014, deadline. Therefore, we made no recommendation.

Badge Access Reviews

For the April 2014 quarterly badge access review³¹ at Eagan IT and Accounting Services, we determined although the reviews were completed, a management analyst responsible for posting the results to a specified mailbox³² did not ensure one of the responses was posted in a timely manner. [REDACTED]

[REDACTED] Failure to properly maintain a record of access to a controlled area increases the risk of use by unauthorized personnel that could result in physical failure of infrastructure components. Based on our audit, the employee resolved the issue. We retested the July 2014 access review and did not find any issues. Therefore, we made no recommendation.

[REDACTED] Policy

[REDACTED] management did not assign the [REDACTED] to the [REDACTED] group [REDACTED] in the [REDACTED].³⁵ The [REDACTED] overrides the settings for the default [REDACTED].³⁶

[REDACTED] we made no recommendation.

[REDACTED]

²⁷ The IT Procedure Artifacts Library serves as the repository for SOX and non-SOX related IT procedures related to various IT activities, such as mainframe security.

²⁹ The IT CMO maintains the IT Procedure Library.

³² That email is kept in the HCS SOX Artifact Facilities mailbox.

[REDACTED]

Server Management

The Postal Service Engineering Team set the password expiration for the administrator account to the [REDACTED] [REDACTED]³⁷ to 90 days in the [REDACTED]⁸ environment rather than 30 days as required.³⁹ This occurred because management is in the process of converting the operating system from the [REDACTED]⁴² and did not change the settings to meet Postal Service policy when moving the [REDACTED] servers from the test to the production environment. System administrator accounts are more susceptible to a password brute-force attack. A [REDACTED] better protects information resources from accidental or intentional unauthorized use, modification, disclosure, or destruction. As a result of our audit, management set [REDACTED]. Therefore, we made no recommendation.

Fire Suppression Inspections

[REDACTED] IT and Accounting Services management did not conduct fire suppression systems inspections in a timely manner.⁴³ In the [REDACTED],⁴⁴ the last inspection took place in May 2014. The previous inspection took place in October 2012. In the raised floor areas, the last inspections took place in April and October 2013. No inspection took place in April 2014 as required. According to Postal Service procedures,⁴⁵ semi-annual reviews for smoke and heat should take place in April and October. Management stated this occurred due to scheduling conflicts with the vendor conducting the tests. Physical inspections are designed to reduce the risk of physical failure of infrastructure components, and damage from natural or fabricated environmental hazards. During our audit, management conducted inspections with the vendor in June 2014 and October 2014. Therefore, we made no recommendation.

37 [REDACTED] allows a business to establish an online trading community that reliably and securely connects with suppliers, partners, distributors, banks, and service providers across private or public marketplaces of any size.

38 [REDACTED] system designed to provide companies a free or very low-cost [REDACTED] comparable to traditional and usually more expensive [REDACTED]

43 This is not a key control for financial reporting.

44 The [REDACTED] securely stores the [REDACTED].

45 Control procedure, DCTR 03: Reviewing Data Center Environmental Controls Procedure, dated April 22, 2013.

Status of Open Information Technology Issues Reported in Prior Years

During our control tests in FY 2014, we reviewed the status of prior years' open issues. The OIG confirmed the CMO closed 12 issues identified in earlier reports (see [Appendix B](#) for actions taken). Likewise, the CMO continued remediation efforts on eight issues (see [Appendix C](#) for details regarding the remediation efforts on these issues). Table 1 summarizes the status of corrective actions taken in FY 2014 on prior years' issues.

Table 1. Summary of Corrective Actions Taken in FY 2014

Status	Issues Identified by Fiscal Year				Total
	2010	2011	2012	2013	
Remediation in progress	0	4	4	0	8
Issues closed with confirmation from the OIG	2	4	3	3	12
Total	2	8	7	3	20

Source: CMO Integrated Audit Weekly Coordinator Meeting.

Recommendations

Based on the audit results, we are not making any recommendations. Accordingly, management chose not to formally respond to this report.

Appendices

*Click on the appendix title to
the right to navigate to the
section content.*

Appendix A: Additional Information	13
Background	13
Objective, Scope, and Methodology.....	15
Prior Audit Coverage	17
Appendix B: Prior Years' Information Technology Issues Closed in Fiscal Year 2014	18
Appendix C: Status of Open Information Technology Issues Reported in Prior Years	21
Appendix D: Trademark Information	23

Appendix A: Additional Information

Background

The Postal Service's SOX Management Controls and Integration group oversees testing for finance issues and reports to the Office of Controller. The IT CMO tests and maintains compliance for infrastructure-level controls and reports issues to the vice president, Information Technology. These infrastructure controls are referred to as IT SOX master controls, including both general computer and application-specific controls.

The [REDACTED];⁴⁶ IT and Accounting Services provide computer processing and accounting services for the Postal Service. The [REDACTED] Service Center provides infrastructure services for nearly 32,000 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 system maintenance that enable the Postal Service to achieve its business objectives. These organizations currently [REDACTED] [REDACTED] relevant to SOX Section 404 compliance.⁴⁸

The IT SOX master control environment consists of eight process areas:

- Application General
- IT Governance
- Operating System
- Database
- Infrastructure
- Operations
- Application-Unique
- Company-wide

For FY 2014, we were responsible for testing five process areas shown in [Table 2](#).

⁴⁶ We did not test any IT SOX master controls in St. Louis in FY 2014.

⁴⁷ The IT CMO considers these significant business applications supporting a SOX in-scope business process.

⁴⁸ The IT CMO determined these IT systems have a comprehensive impact on the IT control environment or are relied on by SOX in-scope applications for coverage of controls.

Table 2. IT SOX Master Control Process Area

IT Process Area	Description
Operating System	This area is composed of the three types of operating systems that support financial and IT-related applications. [REDACTED]
Database	This area encompasses the numerous database structures that support either financial or infrastructure applications. [REDACTED]
Infrastructure	This area is composed of the individual security software applications that provide centralized user authentication and access to operating systems and standardized job scheduling tools. [REDACTED]
Operations	This area encompasses several functions with broad impact in supporting Postal Service IT functionality. [REDACTED]
Company-wide	This area contains several security monitoring functions, such as those provided by the Corporate Information Security Office (CISO). This includes the Computer Incident Response Team's (CIRT) efforts to monitor and assess security systems and network resources and provide comprehensive responses to computer security incidents.

Source: Postal Service IT SOX Master Control Index Report.

[REDACTED]

Objective, Scope, and Methodology

Our objective was to evaluate and test key financial reporting infrastructure-level internal controls over information systems at Postal Service IT and Accounting Services and related IT organizations. In consultation with the IPA firm, we limited the scope of our audit in FY 2014 to key financial reporting infrastructure-level IT controls.⁵⁷ Our audit did not address the entire IT environment but only SOX in-scope financial reporting systems. After our initial reviews and before final testing was completed, management adjusted the status of several controls. For example, management removed [REDACTED] associated with the IT Operations process area, because the CMO determined that the job scheduling controls were duplicative and reviews were covered through existing eAccess controls.⁵⁸ Additionally, management [REDACTED] of another job scheduling control⁵⁹ by [REDACTED] [REDACTED]⁶⁰ and relying on other control tests,⁶¹ thereby [REDACTED] applications⁶² from the control. Finally, management removed the timeliness criteria to better meet the baseline objective for a data transfer control.⁶³ We concurred with these changes to these infrastructure-level controls and adjusted our work accordingly.

To accomplish our objective, we interviewed administrators, observed master control processes and procedures, and reviewed applicable Postal Service policies. We judgmentally and randomly selected samples of SOX in-scope applications, servers, and SOX-related notifications for detailed control testing and analysis. We reviewed [REDACTED] (37 percent)⁶⁴ IT SOX master controls designed to mitigate risks associated with [REDACTED] IT components. We tested master controls, including those associated with configuration baselines, separation of duties, [REDACTED] configurations, security log monitor configurations, security monitoring, data restoration, and testing documentation. We also monitored corrective action taken on issues open from prior years' reviews and performed assessments as appropriate.

Table 3 shows the number of IT SOX master controls we tested for each infrastructure component to support SOX in-scope financial and infrastructure applications.

57 The primary controls that management has identified to mitigate SOX risks.

[REDACTED]
[REDACTED] and [REDACTED] uses the [REDACTED] and [REDACTED] applications to enable the Postal Service and business partners to exchange and monitor files in a secure, non-platform dependent environment.

63 [REDACTED].

64 By agreement with the IPA firm, the OIG was responsible for 79 of 210 key IT SOX master controls for FY 2014 reporting. However, one control was [REDACTED] [REDACTED], and we could not test one control: CIRT.Review_Sec_Incidents. See footnote 66.

application⁶⁸ to be reliable for reviewing selected controls associated with the [REDACTED], and [REDACTED] systems. We also reviewed the code walkthrough and script validation provided by the IT CMO. This confirmed that the scripts did not contain elements that would manually insert values, and that the scripts would return error messages in the event data from the server could not be read. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

Report Title	Report Number	Final Report Date	Monetary Impact (in millions)
<i>Fiscal Year 2013 Information Technology Internal Controls</i>	IT-AR-14-003	3/26/2014	None
<p>Report Results: The infrastructure-level internal controls we tested were properly designed and generally operating effectively. However, we identified opportunities that would help control owners better manage change management policies and job scheduling procedures for the [REDACTED] application and strengthen administrator access controls for workload scheduling software. In addition to issues identified in FY 2013, we reported on management's corrective actions taken on open issues identified during FY 2013 and reported in FYs 2010 through 2012. Management agreed with the recommendations. We also confirmed management took corrective actions to address 15 prior year issues and was remediating 12 other issues reported during FYs 2010 through 2012.</p>			
<i>Fiscal Year 2012 Information Technology Internal Controls</i>	IT-AR-13-003	1/28/2013	None
<p>Report Results: Many of the infrastructure-level internal controls we tested were properly designed and generally operating effectively. However, we identified opportunities to strengthen certain internal controls over security monitoring of [REDACTED] operating system and database activity, as well as secondary reviews of actions taken in response to database monitoring. In addition to the issues identified in FY 2012, we reported on management's corrective actions taken on open issues identified during FY 2012 and reported in FYs 2010 and 2011. Management agreed with the recommendations, resolved 13 issues associated with five of the recommendations, and was working to complete corrective actions on five issues associated with four of the recommendations.</p>			
<i>Fiscal Year 2011 Information Technology Internal Controls</i>	IT-AR-12-003	1/9/2012	None
<p>Report Results: The infrastructure-level internal controls we tested were properly designed and generally operating effectively. However, we identified opportunities for management to strengthen certain internal controls over operating systems, databases, [REDACTED], job scheduling, and data back-up and restoration operations. In addition to the issues identified in FY 2011, we reported on the status of unresolved issues from the FY 2010 review. Management agreed with the recommendations. Management resolved one issue and was working to complete corrective action on the issues consolidated in the remaining recommendation.</p>			

68 For FY 2014, the IT CMO developed this application to continuously monitor the configuration settings associated with four IT SOX master controls across five platforms (16 controls).

**Appendix B:
Prior Years' Information
Technology Issues
Closed in Fiscal Year 2014**

IT SOX Master Control
(GET⁶⁹ Identification Number)

Description and Action Taken to Close Issue

CMO Tracking Number

Issues Identified in FY 2010

1. [REDACTED] did not perform vulnerability scans on [REDACTED] servers to ensure the [REDACTED] agent is loaded or running. Management implemented a reconciliation process between the [REDACTED]⁷⁰ and the Critical [REDACTED] report on a quarterly basis for all [REDACTED] servers.

[REDACTED]_Compliance_Chk
(2010-774)
FY10.OIG.OE.DCE.07.023

2. ISS relied upon the server listing from the inaccurate [REDACTED] to determine which [REDACTED] and [REDACTED] servers to scan to establish whether the [REDACTED] agent is running. Management implemented a reconciliation process between the [REDACTED] and the [REDACTED] agents report on a quarterly basis for [REDACTED] servers.

[REDACTED]_Compliance_Chk
(2010-827)
FY.10.OIG.OE.DCE.07.036

Issues Identified in FY 2011

3. Semi-annual reviews of access to [REDACTED] resources do not address the control objective because they fail to consider the authorizations granted to the individual user. Instead, the reviews focus only on the authorizations granted via the user's membership in a group. The Production Operations Branch remediated the job scheduling review process and updated the IT Procedure Library. The files provided now show the individual permissions and role assignments in the Privileges and Active tabs.

[REDACTED]_Review_Job_Schd
(2011-341/342)
FY11.OIG.OE.DCE.CTM-EM Job
Schd Review

4. Three [REDACTED] profiles do not comply with the password expiration policy. Management performed a coordinated team effort to reconcile [REDACTED] accounts against accounts registered in [REDACTED]. Subsequent IT CMO testing verified that all accounts met Postal Service password policy.

[REDACTED]_Parm_Config
(2011-433)
FY11.IT_CMO.OE.SOX.07.TRDA
Non Approved Non Expiring PW

5. Management did not create tickets to monitor and track unresolved issues in the [REDACTED] area timely. Management revisited corrective actions taken and worked with the control owner to identify additional procedures to mitigate the risk of not creating tickets in the prescribed timeframe. OIG verified the revised control addressed the issues previously identified.

[REDACTED]_Job_Mntr
(2011-370)
FY11.OIG.OE.DCE.DTS Job
Failure Remedy Ticket Timing

69 Management uses the [REDACTED] to monitor business and IT SOX-related issues. Each issue is assigned a [REDACTED] r. Additionally, the IT CMO maintains records of less significant issues (known as process improvements) the [REDACTED] does not report.

70 The [REDACTED] is a central repository for all server assets in host computing. It is driven by a combination of configuration discovery and data put in by the customer.

71 [REDACTED] offers protection for desktops and servers against malicious behaviors, blended threats, and known and unknown attacks.

Description and Action Taken to Close Issue

CMO Tracking Number

6. Management used a methodology of drawing sample job changes in the change management system⁷² (change requests (CR)), [REDACTED], which may have circumvented their ability to identify any changes made external to the standard change management process. Management updated the methodology for referencing CR tickets in the [REDACTED] system. Management also began providing a report of all job changes, which included the description field to utilize as the source population for testing. Subsequent OIG testing verified that management approval was obtained for all job changes via the referenced CR ticket number; therefore, the control was operating as designed.

[REDACTED]_Chgs_via_CR
(2011-398)
FY11.OIG.DE.DCE.SOX.Job
Schd Chgs via CR

Issues Identified in FY 2012

7. A copy of the [REDACTED] records used to update information in the vulnerability management tool was not retained as required. Management updated procedures to make sure they retained an artifact document of [REDACTED] records and uploaded the artifact to the appropriate library, as stated in the control.

[REDACTED]_Compliance_Chk
(2012-081)
FY12.OIG.OE.DCE.CSP
Compliance Check Retention
of CMDB Extract

8. Twenty-five of 45 SOX in-scope production [REDACTED] servers (on [REDACTED] hardware) were not reporting intrusion detection events to the [REDACTED]⁷³ and were not detected by current monitoring efforts. The [REDACTED] Engineering team implemented changes to their [REDACTED] configuration monitor⁷⁴ for changes to the log configuration files and the [REDACTED] process monitor for sending email alerts to the [REDACTED] Engineering team.

[REDACTED]_Log_Mntr_Config
(2012-094)
FY12.OIG.DEOE.UNIX_Sec_
Log_Mntr_Config.z/linux servers

9. The [REDACTED] script used within the vulnerability scans performed did not confirm whether the intrusion detection software was running or reporting. Management replaced the [REDACTED] script with new [REDACTED] scanning software and instituted a reconciliation process for the [REDACTED] and the [REDACTED] report on a quarterly basis for all servers with [REDACTED] agents installed.

[REDACTED]_Compliance_Chk
(2012-104)
FY12 OIG DE DCE WIND_CSP_
Compliance
Chk Cannot Be Verified

⁷² In a computer system environment, change management refers to a systemic approach to keep track of the detail of the system. For example, what operating system release is running on each computer and which fixes have been applied.

⁷³ [REDACTED] collects and correlates security events from across the network, even though other products, such as antivirus and firewall applications, generate the events.

⁷⁴ [REDACTED] is an open source systems management tool for centralizing and automating configuration management.

⁷⁵ [REDACTED] is a software suite, consisting of a console, intelligent agents, and Knowledge Modules, which system or database administrators can use for security event monitoring.

**Appendix C:
Status of Open Information
Technology Issues Reported
in Prior Years**

Condition of Control per Prior OIG Assessment	IT SOX Master Control (GET Identification Number) CMO Tracking Number	Report and Associated Recommendation Number (Target Completion Date)
Issues Identified in FY 2011		
1. The OIG noted concerns with the method used to determine the universe of databases to be monitored. In FY 2012, management began a remediation effort that clarified the need for an automated discovery tool to identify a complete list of servers in their environment, as well as automated processes to sustain the configuration data within [REDACTED].	[REDACTED]_Log_Mntr_Config (2011-316) FY11.OIG.OE.DCE.SOX. Completeness of [REDACTED] Monitoring	IT-AR-12-003, Recommendation 1 (FY 2015 Q1)
2. Critical patches were not installed for at least 6 months on [REDACTED] databases supporting seven in-scope applications. Management has drafted an [REDACTED] patch policy that incorporates the use of an enterprise tracking system to monitor patches from vendor release to implementation in production. However, management has not determined how to define timeliness for the numerous circumstances that applications requiring database patches encounter.	[REDACTED]_Mgmt (2011-413) FY11.OIG.OE.DCE.SOX [REDACTED] Patch Management	IT-AR-12-003, Recommendation 1 (FY 2015, Q4)
3. Management did not change the password for [REDACTED] on seven sampled servers and had other application and user accounts in the local account environment on 22 sampled servers. Despite remediation of previously found accounts, subsequent testing by management or the OIG disclosed additional accounts that were not properly configured. Management is reviewing the registration process in the account provisioning software and devising a plan to address the systemic problem.	[REDACTED]_Parm_Config (2011-440) FY11.IT.CMO.OE.DCE.SOX [REDACTED] PW Parm Config	IT-AR-12-003, Recommendation 1 (FY 2015, Q2)
4. We identified issues associated with the [REDACTED] patching process, including the absence of documentation provided in patch evaluation assessment, inadequate process and artifacts to ensure that all servers are patched, and absence of test plans and results of testing within the patch management process artifacts. Management is working with the associated parties to revise [REDACTED] patching procedures.	[REDACTED]_Patch_Mgmt (2011-442) FY11.OIG.OE.DCE.SOX [REDACTED] Patching Process	IT-AR-12-003, Recommendation 1 (FY 2015, Q4)

Condition of Control per Prior OIG Assessment	IT SOX Master Control (GET Identification Number) CMO Tracking Number	Report and Associated Recommendation Number (Target Completion Date)
Issues Identified in FY 2012		
<p>5. The current process for [redacted] configuration baseline compliance effectively demonstrates perpetual failure of this SOX control. The control is defined such that SOX production servers should have "configuration baselines [that] meet or exceed the configuration baselines established by management." The decision to equate the [redacted] configuration baseline with hardening standards is problematic because the three hardening standards for [redacted] are inconsistent and may include unnecessary elements or exclude necessary elements for a configuration baseline that supports reliable and timely financial reporting. In addition, elements of the hardening standards duplicate other SOX controls for the [redacted] environment.</p>	<p>[redacted].Config_Baseline (2012-097) FY12.OIG.DE.DCE [redacted] Config Baseline Hardening Standards</p>	<p>IT-AR-13-003, Recommendation 8 (FY 2015, Q1)</p>
<p>6. Management did not include 113 SOX in-scope servers in its review of [redacted] server configurations.</p>	<p>[redacted].Config_Baseline (2012-099) FY12.OIG.OE [redacted].Config Baseline [redacted] Review</p>	<p>IT-AR-13-003, Recommendation 6 (FY 2015, Q2)</p>
<p>7. Management does not follow the required process for documenting baseline discrepancies and remediation plans for [redacted] servers. Specifically, management did not get approval for the remediation plans or correctly identify corrective actions for each discrepancy found and track each discrepancy to completion.</p>	<p>[redacted].Config_Baseline (2012-100) FY12.OIG.OE [redacted].Config Baseline.Execution of Procedure</p>	<p>IT-AR-13-003, Recommendation 6 (FY 2015, Q2)</p>
<p>8. Existing [redacted] patch testing procedures are out of alignment with current Midrange group practices. Both the procedures and current practices require adjustment to improve the patch history of individual servers and provide assurances the control environment is operating effectively.</p>	<p>[redacted]esting_Doc (2012-131) FY12.OIG.OE.DEC.07 [redacted] Testing.Doc Testing and Tracking of Patches</p>	<p>IT-AR-13-003, Recommendation 9 (FY 2015, Q4)</p>

Source: OIG Analysis.

Appendix D: Trademark Information

The following are the trademarks (™) or registered trademarks (®) of their respective owners in the U.S.⁷⁹:

BMC Software, Inc.: [REDACTED] and [REDACTED]

CA Technologies: [REDACTED]

IBM Corporation: [REDACTED]

Microsoft Corporation: [REDACTED]
[REDACTED]

Oracle Corporation: [REDACTED]

[REDACTED]

Symantec Corporation: [REDACTED]

Teradata (Corporation) Operations, Inc.: [REDACTED]

The Attachmate Group, Inc.: [REDACTED]

The Open Group: [REDACTED]

⁷⁹ A trademark (™) is the name or symbol used to identify goods purchased by a particular manufacturer or distributed by a particular dealer and to distinguish them from products associated with competing manufacturers or dealers. A trademark that has been officially registered and is, therefore, legally protected is known as a Registered Trademark (®).



Contact us via our [Hotline](#) and [FOIA](#) forms, follow us on social networks, or call our Hotline at 1-888-877-7644 to report fraud, waste or abuse. Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100