



OFFICE OF  
**INSPECTOR  
GENERAL**  
UNITED STATES POSTAL SERVICE

---

**Fiscal Year 2013  
Information Technology  
Internal Controls**

**Audit Report**

March 26, 2014

---

Report Number IT-AR-14-003



# HIGHLIGHTS

March 26, 2014

## Fiscal Year 2013 Information Technology Internal Controls

Report Number IT-AR-14-003

### **BACKGROUND:**

The Postal Accountability and Enhancement Act of 2006 requires the U.S. Postal Service to comply with the Sarbanes-Oxley Act and make an assertion on the effectiveness of the internal control structure over financial reporting. We conducted this audit in support of 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 system-level environment includes processes needed to administer, secure, and monitor key financial systems. Our objective was to evaluate and test key system-level internal controls over information systems.

### **WHAT THE OIG FOUND:**

The system-level internal controls we tested were properly designed and generally operating effectively. For example, database software controls functioned properly when we tested password security settings and updates. However, we identified opportunities to strengthen certain controls, which would reduce the risk information technology resources would be compromised. Specifically, these improvements would help control owners better manage change management policies and job scheduling procedures for the [REDACTED] and

strengthen administrator access controls for workload scheduling software.

Management also took corrective action to address eight additional issues identified during our audit. We also confirmed management took corrective actions to address 15 prior year issues and is currently remediating 12 other issues reported during fiscal years 2010 through 2012.

We discussed related causes and recommended actions to improve the control environments. The control weaknesses identified, alone or collectively, do not prevent reliance on system-level internal controls for accurate and timely financial reporting.

Corrective actions can reduce the risk of a compromise that could harm the confidentiality, integrity, and availability of information resources.

### **WHAT THE OIG RECOMMENDED:**

We recommended management ensure [REDACTED] administrators follow job control policies and implement a job scheduling procedure. We also recommended management properly document changes to computer command lists and require a password expiration setting for the workload automation software.

[Link to review the entire report](#)



March 26, 2014

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

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

**FROM:** John E. Cihota  
Deputy Assistant Inspector General  
for Financial and Systems Accountability

**SUBJECT:** Audit Report – Fiscal Year 2013 Information  
Technology Internal Controls  
(Report Number IT-AR-14-003)

This report presents the results of our audit of Fiscal Year 2013 Information Technology Internal Controls (Project Number 13BM007IT000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Sean D. Balduff, acting director, Information Technology, or me at 703-248-2100.

Attachment

cc: Julie S. Moore  
Corporate Audit and Response Management

## TABLE OF CONTENTS

|   |    |
|---|----|
| Introduction .....  | 1  |
| Conclusion .....  | 1  |
| Three Open Fiscal Year 2013 Information Technology Issues.....                    | 2  |
| Corrective Actions Taken for Eight Fiscal Year 2013 Issues.....                   | 4  |
| Status of Open Information Technology Issues Reported in Prior Years .....        | 5  |
| Recommendations .....   | 5  |
| Management’s Comments .....   | 6  |
| Evaluation of Management’s Comments.....  | 6  |
| Appendix A: Additional Information .....  | 7  |
| Appendix A: Additional Information .....  | 7  |
| Background .....  | 7  |
| Objective, Scope, and Methodology .....   | 9  |
| Prior Audit Coverage .....  | 11 |
| Appendix B: Open Fiscal Year 2013 Information Technology Issues.....              | 13 |
| Appendix C: Closed Information Technology Issues Reported in Prior Years.....     | 14 |
| Appendix D: Status of Open Information Technology Issues Reported in Prior Years. | 17 |
| Appendix E: Trademark Information.....  | 22 |
| Appendix F: Management’s Comments .....   | 23 |

## Introduction

This report presents the results of our audit of Fiscal Year (FY) 2013 Information Technology (IT) Internal Controls (Project Number 13BM007IT000). 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.<sup>1</sup> Our objective was to evaluate and test key infrastructure-level internal controls over information systems at Postal Service IT and Accounting Service Centers (IT/ASCs) and related IT organizations.<sup>2</sup> During the audit, we met regularly with the IPA firm and Postal Service representatives to report and discuss gaps in controls, initial test results, and control deficiencies.<sup>3</sup> See [Appendix A](#) for additional information about this audit and a description of the IT process areas we reviewed.

The Postal Reorganization Act of 1970, as amended, requires annual audits of the Postal Service's financial statements. Additionally, SOX was enacted in 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. That section also directs management to make an assertion on the effectiveness of the internal control structure over financial reporting. The Postal Accountability and Enhancement Act of 2006 required the Postal Service to begin complying with SOX Section 404 in FY 2010. The Board of Governors contracted with the IPA firm to express opinions on the Postal Service's financial statements and internal controls over financial reporting.

## Conclusion

The infrastructure-level internal controls we tested were properly designed and generally operating effectively. For example, database software controls functioned properly when we tested the password security settings and update process. However, we identified opportunities to strengthen certain controls that would reduce the risk that information resources would be compromised.<sup>4</sup>

---

<sup>1</sup> 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.

<sup>2</sup> Infrastructure-level controls are system controls consisting of processes for managing specific system resources related to either a general support system or a Sarbanes-Oxley Act (SOX) application.

<sup>3</sup> 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.

<sup>4</sup> 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.



As of December 16, 2013, management had open issues requiring corrective action in the following areas:

1. Administrator personnel<sup>9</sup> did not always follow change management policies. Specifically, administrators did not follow the formal version control policy<sup>10</sup> for modifications to the Visual Basic Script (VBScript)<sup>11</sup> used to monitor the critical [REDACTED] CA Workload Automation AE<sup>12</sup> scheduled jobs. Instead, administrators achieved versioning by saving the name of the script prior to making major changes.<sup>13</sup>
2. A job scheduling procedure that documents critical jobs does not exist as required.<sup>14</sup> This occurred because previous management did not develop a scheduling procedure and current management was not aware of the requirement.
3. The password expiration setting for a [REDACTED] administrator was set to 90, rather than 30, days.<sup>15</sup> Management changed the expiration setting back to 30 days after we raised the issue. However, future occurrences may not be detected because the IT master control states Postal Service internal reviewers obtain evidence<sup>16</sup> of password settings from [REDACTED] administrators. These administrators could alter the password settings before or after providing evidence to the reviewers. Internal reviewers could use the [REDACTED] tool to directly review current password settings instead of requesting the evidence from the administrators.

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. See [Appendix B](#) for additional details related to each of the issues identified in FY 2013.

---

<sup>9</sup> Employees and contractors who work at the [REDACTED] (ITSC).

<sup>10</sup> Postal Service Handbook AS-805, *Information Security*, Section [REDACTED], May 2013.

<sup>11</sup> VBScript enables administrators to manage desktop settings and applications.

<sup>12</sup> CA Workload Automation AE is designed to deliver broad-based multiplatform facilities for dynamic service management, event- and policy-driven workload scheduling, resource allocation, automation, and business process optimization. This tool also provides real-time or "on-demand" responses to events, in accordance with business priorities or other policy-based service requirements.

<sup>13</sup> The [REDACTED] team saves script names prior to making major changes in the following format: ChkOne\_YYYYMMDD.vbs.

<sup>14</sup> The [REDACTED] Job Monitoring procedure requires that the "[REDACTED] CA-Autosys – Job Scheduling Procedure" exist for listing critical batch jobs and corresponding [REDACTED] processes and be stored on site by the [REDACTED] team.

Handbook AS-805, Section [REDACTED].

<sup>16</sup> The first test step in the control "[REDACTED]\_PW\_Parm\_Config" recommends the reviewer obtain a screenshot of the "System Parameters" from the [REDACTED] system administrator.

## Corrective Actions Taken for Eight Fiscal Year 2013 Issues

Management took corrective action<sup>17</sup> to address the following eight issues we identified during our FY 2013 audit:

1. Migrate the existing Systems Applications and Products<sup>18</sup> [REDACTED] application<sup>19</sup> from the Advanced Interactive eXecutive (AIX) operating system to the [REDACTED] operating system.
2. Modify security privileges for an [REDACTED]<sup>22</sup> developers group to prevent its access to the production environment.
3. Restrict access to mainframe security datasets from “write” to “read only” for nine [REDACTED] users.
4. Modify a mainframe operating system parameter library<sup>23</sup> to include appropriate corresponding comment lines and change request numbers.
5. Ensure records of monthly mainframe software reviews are placed in an artifact email account.<sup>24</sup>
6. Upload quarterly badge access review documentation to the artifact library.<sup>25</sup>
7. Monitor the email artifact account to verify that all managers have replied to badge access review requests.
8. Correct the list of [REDACTED]<sup>26</sup> users who have administrative access to perimeter firewall appliances.

<sup>17</sup> Management initiated and completed these corrective actions during our audit; therefore, they did not require the IT CMO's participation in the corrective action process.

<sup>18</sup> The original name for the acronym, SAP, was: “Systeme, Anwendungen, Produkte,” meaning Systems Applications and Products (in German).

<sup>19</sup> An enterprise-wide application used to process and manage general personnel records (for example, Postal Service Form 1727, Award Recommendation/Authorization [Quality Step Increase]).

<sup>20</sup> The original [REDACTED] platform consisted of the International Business Machine (IBM) Mainframe version z10 z/OS/DB2 system and xLinux/AIX applications. DB2 is IBM's relational database management system and a formal subsystem of the z/OS mainframe operating system.

<sup>21</sup> The [REDACTED]

The parameter files are part of z/OS, the operating system for Postal Service mainframes, produced by IBM.

<sup>24</sup> As part of the SOX software review (patching) procedures, centralized email accounts (folders/distribution lists) were established in Outlook to archive vendor notifications regarding various software updates. Specifically, on a semiannual basis, the [REDACTED] – under the [REDACTED] manager should review an email account called, “[REDACTED] SOX Artifact [REDACTED]”. This email account serves as an archive for an evaluation by support team members, to determine whether [REDACTED] team members should implement the recommended software updates before the next standard maintenance cycle.

<sup>25</sup> Also known as the [REDACTED], the artifact library serves as the repository for SOX and non-SOX related IT procedures and it contains all artifacts that are not posted in the technology solutions life cycle library.

## Status of Open Information Technology Issues Reported in Prior Years

During our control tests in FY 2013, we reviewed the status of any prior year open issues for which management took or completed corrective action. We found the corrective actions addressed several of these issues and concurred with management's requests to close them. The OIG confirmed that the CMO took corrective action to close 15 issues identified in earlier reports (see [Appendix C](#) for specific actions taken). Likewise, the CMO began remediation efforts on 12 open issues (see [Appendix D](#) for details regarding the remediation efforts on these issues). Table 1 summarizes the status of corrective actions taken this year on prior years' issues.

**Table 1: Summary of Corrective Actions Taken in FY 2013**

| Status                                      | Total Number of Issues Identified by Fiscal Year |          |           | Total Number of Issues by Category |
|---|--|----------|-----------|------------------------------------|
|   | FY 2010  | FY 2011  | FY 2012   |                                    |
| Remediation in Progress                     | 1  | 6        | 5         | 12                                 |
| Issue Closed With Confirmation From the OIG | 1  | 2        | 12        | 15                                 |
| <b>Total</b>                                | <b>2</b>   | <b>8</b> | <b>17</b> | <b>27</b>                          |

## Recommendations

We recommend the vice president, Information Technology, direct the Information Technology Compliance Management Office, in coordination with the manager, [REDACTED], to:

1. Reiterate to [REDACTED] administrators to follow control policies in managing critical jobs and script versions.
2. Implement a job scheduling procedure for the [REDACTED] that documents critical jobs.

We recommend the vice president, Information Technology:

3. Direct the Information Technology Compliance Management Office to require Postal Service internal reviewers to use the [REDACTED] tool to directly obtain evidence of password settings.

<sup>26</sup> Commonly used to provide centralized authentication, authorization, and accounting for dial-up, virtual private network, and, more recently, wireless network access.

<sup>27</sup> The Postal Service maintains perimeter firewalls as a technical, preventive control that limits access and services between networks by accepting or blocking network traffic according to security policy.

## Management's Comments

Management agreed with each of our findings and recommendations and will develop detailed corrective actions in coordination with the particular control owners and in consideration of the OIG's recommendations. Based on a subsequent discussion, the IT CMO plans to review specific corrective actions with the OIG for concurrence and will track the actions to completion. Management plans to complete corrective actions for all three recommendations by June 30, 2014.

See [Appendix F](#) for management's comments in their entirety.

## Evaluation of Management's Comments

The OIG considers management's comments responsive to the recommendations and the planned actions should resolve the issues identified in the report.

The OIG considers all 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.

## Appendix A: Additional Information

### Background

The Postal Service's SOX and Process Improvement Office established the IT SOX CMO to manage annual documentation, testing, remediation, reporting, and certification requirements for meeting and maintaining IT SOX compliance. The IT SOX CMO is responsible for developing and implementing internal IT SOX master controls,<sup>28</sup> including both general computer and application-specific controls. The [REDACTED] IT/ASCs provide computer processing and accounting services for the Postal Service. The [REDACTED] ITSC 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 support [REDACTED] financial<sup>29</sup> applications and [REDACTED] IT-related applications or infrastructure components relevant to SOX Section 404 compliance.<sup>30</sup>

The IT infrastructure environment consists of six process areas:

- Operating System.
- Database.
- Infrastructure.
- Operations.
- Application-Unique.
- Company-wide.

For FY 2013 reporting, we were responsible for testing [REDACTED] IT infrastructure components within the six process areas shown in [Table 2](#).

---

<sup>28</sup> 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. Master controls are either general in nature (such as addressing [REDACTED] security parameters) or application-unique (tailored specifically for the accounting reporting application).

<sup>29</sup> The IT SOX CMO considers these significant business applications supporting an in-scope business process.

<sup>30</sup> The IT SOX CMO determined these IT systems have a comprehensive impact on the IT control environment or are relied on by in-scope applications for coverage of controls.

**Table 2: IT Infrastructure 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. They include z/OS — which functions in a mainframe environment — [REDACTED], and [REDACTED]. The [REDACTED] includes multiple subtypes, including Solaris, [REDACTED] and AIX.  |
| Database           | This area encompasses the numerous database structures that support either financial or infrastructure applications. They include DB2, <sup>32</sup> [REDACTED] Server, [REDACTED], and [REDACTED]. Additionally, the OIG included the [REDACTED] [REDACTED] monitoring tool in this area.  |
| 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. These include [REDACTED], [REDACTED] <sup>35</sup> , [REDACTED] and [REDACTED]. In addition, the area includes the [REDACTED] application used to transmit data between the Postal Service and its trading partners. |
| Operations         | This area encompasses several functions with broad impact in supporting Postal Service IT functionality. They include backup and data restore processes, physical security at IT/ASCs and the ITSC, [REDACTED] and job scheduling.  |
| Application Unique | This area consists of controls designed for individual systems. These applications include [REDACTED] <sup>37</sup> , [REDACTED], and [REDACTED].   |
| Company-wide       | This area contains several security monitoring functions, such as those provided by the [REDACTED]. This includes the [REDACTED].   |

<sup>31</sup> The developing company for a version of the open source UNIX operating system.

<sup>32</sup> DB2 (originally known as Database 2) is IBM's relational database management system and a formal subsystem of the z/OS mainframe operating system.

<sup>33</sup> Formally known as [REDACTED] this software product provides continuous database monitoring to detect or prevent unauthorized or suspicious activity. Management uses [REDACTED] to monitor activity from multiple types of databases that support SOX in-scope systems.

<sup>34</sup> [REDACTED] implemented for [REDACTED] networks, which functions as a [REDACTED] for authentication and authorization of users and computers, assigning and enforcing security policies for all computers and installing or updating software.

<sup>35</sup> IBM implemented [REDACTED] as the mainframe software security product. [REDACTED] provides this security by identifying and verifying users, authorizing users to access protected resources and recording and reporting access attempts.

<sup>36</sup> The software used to monitor and maintain access to the [REDACTED] environment.

<sup>37</sup> [REDACTED] consists of an integrated suite of applications designed to better manage customer relationships, services, financial information, human capital, and projects in a global business environment. Centralized installation of [REDACTED] software at the application level eliminates the need to install and maintain application software on each desktop client computer.

| IT Process Area | Description   |
|-----------------|---|
|                 | <p>efforts to monitor and assess security systems and network resources<sup>38</sup> and provide comprehensive responses to computer security incidents; the approving the connection of systems or networks to the network infrastructure; and the telecommunications team's support of wide- and local-area networks, wireless technologies, telephones, virtual private networks, and the Postal Service's intranet.</p> |

Source: Postal Service *IT SOX Master Control Index Report*.

### Objective, Scope, and Methodology

Our objective was to evaluate and test infrastructure-level internal controls over information systems at Postal Service IT/ASCs and related IT organizations. In agreement with the IPA firm and Postal Service management, we limited the scope of our review in FY 2013 to key controls.<sup>39</sup> After our initial reviews and before final testing was completed, management adjusted the status of several controls. Management removed controls associated with the Integrated Database Management System from the audit scope when the potential financial impact of the supported applications was reduced to an insignificant level for SOX compliance. We concurred with these changes to infrastructure-level controls and adjusted our work accordingly.

To meet 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 97 of <sup>40</sup> IT master controls designed to mitigate risks associated with IT infrastructure components. We tested master controls, including those associated with configuration baselines, separation of duties, password parameter configurations, security log monitor configurations, security monitoring, data restoration, and testing documentation. We also monitored corrective action taken on issues open from prior year reviews and performed assessments as appropriate.

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

<sup>38</sup> Information Systems Security (ISS) specialists perform much of this work.

<sup>39</sup> The primary controls that management has identified to fully mitigate SOX risks.

<sup>40</sup> By agreement with the IPA firm, the OIG was responsible for 97 of key IT master controls for FY 2013 reporting.

**Table 3: Infrastructure Components Tested by IT Process Area**

| IT Process Area    | Infrastructure Components<br>(Number of Master Controls) |   |   |   |   | Subtotal by Area |
|--------------------|--|---|---|---|---|------------------|
| Operating System   | ■  | ■ | ■ |   |   | ■                |
| Database           | ■  | ■ | ■ | ■ | ■ | ■                |
| Infrastructure     | ■  | ■ | ■ | ■ | ■ | ■                |
| Operations         | ■  | ■ | ■ | ■ |   | ■                |
| Application Unique | ■  | ■ | ■ |   |   | ■                |
| Company-wide       | ■  | ■ | ■ | ■ |   | ■                |
| <b>Total</b>       |  |   |   |   |   | <b>97</b>        |

Source: OIG analysis.

We performed all system queries in a controlled environment with management’s full knowledge and approval. We conducted our audit at the [REDACTED].

During the audit, we regularly met with the IPA firm and Postal Service representatives to discuss gaps in controls, initial test results, and control deficiencies. The OIG and IPA firm provided management with specific recommendations for corrective action on each reported issue on weekly IT issues logs. The IPA firm identified other deficiencies affecting the Postal Service’s IT environment that were not in the scope of our audit. Following an internal review, management recorded IT issues on the GET to track progress toward completion of corrective actions.

We conducted this performance audit from October 2012 through March 2014 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 February 11, 2014, and included its 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 them. We determined the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

| Report Title   | Report Number | Final Report Date | Monetary Impact |
|--|---------------|-------------------|-----------------|
| <i>Fiscal Year 2012 Information Technology Internal Controls</i>   | IT-AR-13-003  | 1/28/2013         | None            |
| <p><b>Report Results:</b><br/>                     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 ██████████ 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 12 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><b>Report Results:</b><br/>                     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, ████████ 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>  |               |                   |                 |

| Report Title  | Report Number | Final Report Date | Monetary Impact |
|---|---------------|-------------------|-----------------|
| <i>Testing of Certain Fiscal Year 2010 Sarbanes-Oxley Information Technology Key Infrastructure Controls</i>  | FT-AR-11-007  | 2/16/2011         | None            |
| <p><b>Report Results:</b><br/> Overall, general computer controls were in place and working effectively. However, we identified issues with investigating and resolving computer security incidents in a timely manner; installing and operating an intrusion detection agent in the production [REDACTED] environments; reducing the use of non-standard job scheduling software in the production environment; enhancing the quality of information in daily job logs by documenting the cause and resolution of job failures; and performing thorough semiannual reviews of access to mainframe job scheduling software. This report contained no recommendations as management agreed with our findings and planned corrective actions.</p> |               |                   |                 |

**Appendix B: Open Fiscal Year 2013 Information Technology Issues**

|    | Condition of the Control per<br>OIG Assessment   | Master Control                                 | Report and Associated Recommendation Number |
|----|--|--|---|
| 1. | <p>Administrators did not always follow formal version control policy<sup>41</sup> for modifying the VBScript used to monitor critical CA Workload Automation AE scheduled jobs. Instead, administrators achieved versioning by saving the name of the script prior to major changes. A versioning system must be in place to ensure proper version control is maintained. A fully accountable check-in/check-out process must be operational.</p>   | <p>.Job_Mntr</p>                               | <p>IT-AR-14-DRAFT, Recommendation 1</p>     |
| 2. | <p>A job scheduling procedure that documents critical jobs does not exist as required. This occurred because previous management had not developed a job scheduling procedure and current management was not aware of the requirement.</p>   | <p>.Job_Mntr</p>                               | <p>IT-AR-14-DRAFT, Recommendation 2</p>     |
| 3. | <p>The password expiration setting for the administrator account was set to 90, rather than 30, days. Management changed the expiration setting back to 30 days after we brought it to management's attention. However, future occurrences may not be detected because the IT master control (PW_Param_Config) states that reviewers obtain evidence of password settings from the administrators. These administrators could alter the password settings before or after providing the evidence to the reviewers. Internal reviewers could use the tool to directly review the current password settings.</p> | <p>. Review_Job_Schd;<br/>.PW_Param_Config</p> | <p>IT-AR-14-DRAFT, Recommendation 3</p>     |

Source: OIG analysis.

<sup>41</sup> Handbook AS-805, Section

**Appendix C: Closed Information Technology Issues Reported in Prior Years**

|                                     | Description of Issue   | Master Control<br>(GET Identification<br>Number)             |
|-------------------------------------|--|--|
| <b>Issue identified in FY 2010</b>  |  |  |
| 1.                                  | Management implemented a reconciliation process between the [REDACTED] and the [REDACTED] report on a quarterly basis for all [REDACTED] servers.  | [REDACTED].Compliance_Chk<br>(2010-774)                      |
| <b>Issues identified in FY 2011</b> |  |  |
| 2.                                  | The [REDACTED] remediated the job scheduling review process and updated the [REDACTED]. The files provided now show the individual permissions and role assignments in the Privileges and Active tabs.                 | [REDACTED].Review_Job_Schd<br>(2011-341/342)                 |
| 3.                                  | Management performed a coordinated team effort to reconcile [REDACTED] accounts against accounts registered in eAccess. Subsequent IT CMO testing verified that all accounts met Postal Service password policy.       | [REDACTED].PW_Parm_Config<br>(2011-433)                      |
| <b>Issues identified in FY 2012</b> |  |  |
| 4.                                  | Management implemented a process improvement to periodically review access to the [REDACTED].  | [REDACTED].Review_Sec_Log<br>(None – process<br>improvement) |
| 5.                                  | Management established [REDACTED] account registration within eAccess so that all accounts will go through a formal request, review, and approval process.   | [REDACTED].Sec_Log_Mntr_Config<br>(2012-121)                 |
| 6.                                  | Management added seven key security events to log for [REDACTED].  | [REDACTED].Sec_Log_Mntr_Config<br>(2012-086)                 |
| 7.                                  | Management registered the 13 service accounts in eAccess and removed the terminated account so that accounts in the [REDACTED] and [REDACTED] domains would go through a formal request, review, and approval process. | [REDACTED].IT_SOD<br>(2012-124)                              |

<sup>42</sup> 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.

<sup>43</sup> [REDACTED] offers protection for desktops and servers against malicious behaviors, blended threats, and known and unknown attacks.

<sup>44</sup> Also known as "Linux on System z," Linux always runs in a virtual environment on IBM System z mainframes. Virtualization is handled either via logical partitions or by running under the z/VM hypervisor (virtual machine operating system for creating and running virtual machines).



|     | Description of Issue   | Master Control<br>(GET Identification<br>Number) |
|-----|--|--|
| 15. | 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] installed. | [REDACTED].CSP_Compliance_Chk<br>(2012-104)      |

Source: OIG analysis.

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

|    | <b>Condition of Control per Prior OIG Assessment</b>   | <b>Master Control (GET Identification Number)</b> | <b>Target Completion Date</b> | <b>Report and Associated Recommendation Number</b> |
|----|--|---|-------------------------------|--|
| 1. | Twenty-five of 45 SOX in-scope production [REDACTED] (on mainframe hardware) were not reporting intrusion-detection events to the [REDACTED] and were not detected by current monitoring efforts. Initial problems enabling the necessary intrusion-detection services were attributed to a configuration management tool used for [REDACTED] that was not properly customized for [REDACTED]. However, these 25 servers were identified after the expected fix was installed. | [REDACTED].Sec_Log_Mntr_Config (2012-094)         | FY 2014, Quarter (Q) 2        | IT-AR-13-003, Recommendation 3                     |
| 2. | Management did not include 113 SOX in-scope servers in its review of [REDACTED] r configurations.  | [REDACTED].Config_Baseline (2012-099)             | FY 2014, Q2                   | IT-AR-13-003, Recommendation 6                     |
| 3. | Management does not follow the required process for documenting baseline discrepancies and remediation plans for [REDACTED]. 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.   | [REDACTED].Config_Baseline (2012-100)             | FY 2014, Q2                   | IT-AR-13-003, Recommendation 6                     |

|    | Condition of Control per Prior OIG Assessment  | Master Control (GET Identification Number) | Target Completion Date | Report and Associated Recommendation Number |
|----|--|--|------------------------|---|
| 4. | <p>The current process for █████ 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 █████ configuration baseline with hardening standards is problematic because the three hardening standards for █████ 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 █████ environment.</p> | <p>█████.Config_Baseline (2012-097)</p>    | <p>FY 2014, Q2</p>     | <p>IT-AR-13-003, Recommendation 8</p>       |
| 5. | <p>Existing █████ 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>█████.Testing_Doc (2012-131)</p>        | <p>FY 2014, Q2</p>     | <p>IT-AR-13-003, Recommendation 9</p>       |

|    | Condition of Control per Prior OIG Assessment  | Master Control (GET Identification Number) | Target Completion Date | Report and Associated Recommendation Number |
|----|--|--|------------------------|---|
| 6. | In FY 2010, the OIG reported the use of unreliable inventories of servers to determine which servers should be monitored to confirm that intrusion-detection software is running and reporting questionable activity.  | ████.CSP_Compliance_Chk (2010-827)         | FY 2014, Q2            | IT-AR-12-003, Recommendation 1              |
| 7. | In FY 2011, the OIG also noted concerns with the method used to determine the universe of databases to be monitored. Throughout FY 2012, management implemented 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 █████.   | ████.Sec_Log_Mntr_Config (2011-316)        | FY 2014, Q2            | IT-AR-12-003, Recommendation 1              |
| 8. | Management did not create tickets to monitor and track unresolved issues in the █████ area in a timely manner. Our initial testing and follow-up testing on three occasions in FYs 2011 and 2012 disclosed cases where the tickets were not created in the required time. Management plans to revisit corrective actions taken and work with the control owner to identify additional procedures to mitigate the risk of not creating tickets in the prescribed timeframe. | ████.Job_Mntr (2011-370)                   | FY 2014, Q2            | IT-AR-12-003, Recommendation 1              |

|     | Condition of Control per Prior OIG Assessment  | Master Control (GET Identification Number)       | Target Completion Date | Report and Associated Recommendation Number |
|-----|--|--|------------------------|---|
| 9.  | <p>Management draws its sample of job changes from within the change management system to determine whether all changes have gone through the required process. By employing this source for sampling, management does not have the opportunity to identify changes made to production jobs that may have circumvented the change management system. Management is evaluating the current capabilities of the standard job scheduling tools to generate a population of changes and a proposed approach because system limitations prevent an extract from the job scheduler itself.</p> | <p>████████.Job_Sched_Chgs_via_CR (2011-398)</p> | <p>FY 2014, Q2</p>     | <p>IT-AR-12-003, Recommendation 1</p>       |
| 10. | <p>Critical patches were not installed for at least 6 months on ██████████ supporting seven in-scope applications. Management has drafted an ██████████ patch policy that incorporates the use of an enterprise project 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 ██████████ patches encounter.</p>   | <p>████████.Patch_Mgmt (2011-413)</p>            | <p>FY 2014, Q2</p>     | <p>IT-AR-12-003, Recommendation 1</p>       |

|     | Condition of Control per Prior OIG Assessment  | Master Control (GET Identification Number) | Target Completion Date | Report and Associated Recommendation Number |
|-----|--|--|------------------------|---|
| 11. | Management did not change the password for local administrators' [REDACTED] accounts on seven sampled [REDACTED] 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].PW_Param_Config (2011-440)      | FY 2014, Q2            | IT-AR-12-003, Recommendation 1              |
| 12. | 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)           | FY 2014, Q2            | IT-AR-12-003, Recommendation 1              |

Source: OIG analysis.

## Appendix E: Trademark Information

The following are the trademarks (™) or registered trademarks (®) of their respective owners in the U.S.<sup>47</sup>:

[REDACTED]

**CA Software:** Workload Automation AE™

**IBM Corporation:** IBM®, DB2®, [REDACTED]

**Hewlett-Packard Development Company, L.P.:** [REDACTED]

**Microsoft Corporation:** [REDACTED] Microsoft®, [REDACTED]  
[REDACTED]

**Oracle Corporation:** Oracle™, [REDACTED], and Oracle® [REDACTED]  
[REDACTED]

**Symantec Corporation:** Symantec™ [REDACTED]; Symantec™ [REDACTED]  
[REDACTED]

[REDACTED]

**The Open Group:** [REDACTED]

---

<sup>47</sup> 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 (®).

## Appendix F: Management's Comments

JOHN T. EDGAR  
VICE PRESIDENT  
INFORMATION TECHNOLOGY



March 14, 2014

JUDITH LEONHARDT  
DIRECTOR, AUDIT OPERATIONS

SUBJECT: Draft Audit Report - Fiscal Year 2013 Information Technology Internal Controls (Report Number IT-AR-14-DRAFT)

Thank you for the opportunity to review and comment on the Fiscal Year 2013 Information Technology Internal Controls draft audit report.

Recommendation 1:

Reiterate to [REDACTED] administrators to follow control policies in managing critical jobs and script versions.

Recommendation 2:

Implement a job scheduling procedure for the [REDACTED] that documents critical jobs.

Management Response/Action Plan:

Management agrees with recommendations 1 and 2. Management will update the [REDACTED] Job Monitoring procedure document to clarify processes related to managing critical jobs and the script which monitors job processing.

Target Implementation Date:

June 30, 2014

Responsible Official:

[REDACTED]

Recommendation 3:

Direct the Information Technology Compliance Management Office to require Postal Service internal reviewers to use the [REDACTED] tool to directly obtain evidence of password settings.

Management Response/Action Plan:

Management agrees with recommendation 3. Management will update the suggested testing method of the control, [REDACTED]. The updated testing method will guide testers to directly access [REDACTED]. Manager to obtain

475 L'ENFANT PLAZA SW  
WASHINGTON DC 20260-2100  
202-268-3977  
FAX: 202-268-4492  
[JOHN.T.EDGAR@USPS.GOV](mailto:JOHN.T.EDGAR@USPS.GOV)  
[WWW.USPS.COM](http://WWW.USPS.COM)

- 2 -

the password configuration settings of administrator groups increasing the accountability of the artifacts obtained.

Target Implementation Date:

June 30, 2014

Responsible Official:

[REDACTED]

There are no monetary findings in this report.

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 VP Information Technology, requests that sections Open Fiscal Year 2013 Information Technology Issues (page 2-3), Appendix A: Additional Information, Appendix B: Open Fiscal Year 2013 Information Technology Issues (page 13), and Appendix D: Status of Open Information Technology Issues Reported in Prior Years (page 17-21) of the report should be considered as classified, restricted, and exempt from disclosure under the Freedom of Information Act (FOIA).



---

John T. Edgar  
Vice President, Information Technology

cc: Julie S. Moore  
Sally K. Haring, Manager, Corporate Audit and Response Management