



July 22, 2010

ROSS PHILO  
EXECUTIVE VICE PRESIDENT AND CHIEF INFORMATION OFFICER

DEBORAH J. JUDY  
DIRECTOR, INFORMATION TECHNOLOGY OPERATIONS

CHARLES L. MCGANN, JR.  
MANAGER, CORPORATE INFORMATION SECURITY

SUBJECT: Audit Report – UNIX Operating System Master Controls  
(Report Number IS-AR-10-010)

This report presents the results of our audit of UNIX® operating system master controls (Project Number 10RG005IT000). We conducted this audit in support of the Postal Service's regulatory requirement to comply with section 404, Management's Assessment of Internal Control, of the Sarbanes-Oxley Act of 2002 (SOX). Our objective was to determine whether the Postal Service's UNIX operating system environment, hosting applications supporting the financial statements, complies with Information Technology (IT) SOX master controls.<sup>1</sup> This audit addresses operational risk. See [Appendix A](#) for additional details about this audit.

In December 2006, Congress passed the Postal Accountability and Enhancement Act (the Postal Act) that included significant changes to the way the Postal Service does business. The Postal Act requires the Postal Service to comply with SOX beginning with the fiscal year (FY) 2010 annual report.

## Conclusion

The UNIX operating system environment, hosting applications supporting the financial statements, generally complies with IT SOX master controls. See [Appendix C](#) for a summary of compliance with the [REDACTED] UNIX master controls that we tested. Specifically, we tested [REDACTED] UNIX servers and [REDACTED] UNIX workstations and noted the following:

- All [REDACTED] servers complied with the administrative password management, segregation of duties, and password encryption master controls.

---

<sup>1</sup> Controls designed to mitigate the risk associated with the infrastructure that supports SOX in-scope applications.

- One server did not comply with [REDACTED]
- Two servers did not comply with [REDACTED].
- Three servers did not comply with [REDACTED]
- Six servers did not comply with [REDACTED].
- One workstation did not comply with [REDACTED]

While there was general compliance with the SOX master controls, management can improve preventive and detective security controls and preserve the Postal Service brand by:

- Limiting developer permissions within the production environment.
- Establishing approved baseline security configuration standards.
- Properly configuring account and password settings.
- Adhering to patch management procedures.
- Monitoring modifications to log configuration files and key security events.

Based on our audit results, management began remediating configuration-related vulnerabilities during the audit.

### Developer Access to Production Environment

We identified [REDACTED] developers with privileged access to files across [REDACTED] production servers<sup>2</sup> supporting the [REDACTED]. File permissions provided the developers with the capability to modify or delete [REDACTED] files on [REDACTED] servers. IT SOX controls<sup>4</sup> require developer's access to the production environment be limited to read-only.<sup>5</sup>

According to management, these servers function to stage data for transfer to the [REDACTED] application and developers require access to the servers to review log files when failures occur in the file transfer process. Management submitted a risk mitigation plan<sup>6</sup> (RMP) on October 1, 2009, proposing compensating controls to mitigate the risk of unauthorized deletion of or modification to files by developers.

The SOX and Process Improvement office, the SOX Program Management Office, and the chief information officer are currently reviewing the plan. If they approve the plan,

---

<sup>2</sup> These servers were not included in our sample. However because we identified this issue during our fieldwork, we are including the issue in this report.

<sup>3</sup> Permissions in the UNIX environment determine whether a user can read from, write to, or execute a file.

<sup>4</sup> Master Control 07.UNIX.SOD, version 7, dated December 23, 2009.

<sup>5</sup> The read-only permission allows a user to read a file but restricts the user from modifying or deleting it.

<sup>6</sup> A risk mitigation plan identifies mitigating controls that may act as a substitute for a standard IT master control and includes any residual risk.

the OIG must assess the compensating controls to determine whether they appropriately mitigate the risk.

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

1. Review and update system permissions to ensure developers possess read-only privileges to files in the production environment.

### Configuration Baseline

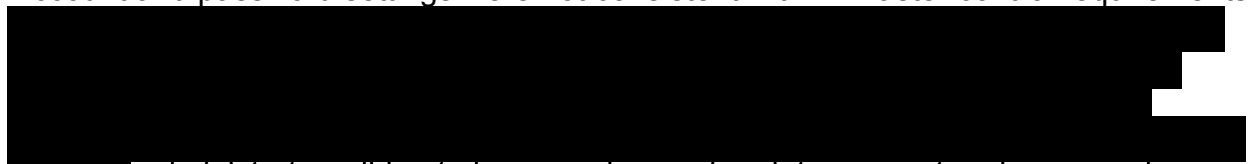
Management has not formally approved UNIX security configuration standards. This is because Information Security Services recently created the International Business Machine Advanced Interactive eXecutive (IBM® AIX®) standards. Information Systems Security is currently working with management to revise and gain approval of the draft AIX standards and existing UNIX standards. Postal Service policy<sup>7</sup> requires management to implement hardening standards specific to each platform. As a result, we could not assess the UNIX environment against the configuration baseline control, as UNIX baseline security configuration standards have not been fully established and approved.<sup>8</sup> The OIG will test this control once management approves all UNIX security configuration standards.

We recommend the manager, Corporate Information Security, coordinate with the director, Information Technology Operations, to:

2. Establish and approve baseline security configuration standards for all UNIX operating system types.

### Account and Password Management

Account and password settings were not consistent with IT master control requirements

 administrators did not always review and update account and password configurations. Improper management of accounts and passwords increases the risk of unauthorized users gaining access to these systems. See [Appendix B](#) for our detailed analysis of this topic.

<sup>7</sup> Handbook AS-805, *Information Security*, dated November 2009, Section 10-2.3.1, Hardening Servers.

<sup>8</sup>IT Master Control 07.UNIX.Config\_Baseline, version 5, dated February 5, 2010, requires management to establish standard operating system security configurations and confirm, semiannually, that production configurations remain consistent with approved standards.

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

3. Review and update UNIX operating system user account and password settings to comply with IT SOX requirements.

### Patch Management

Administrators did not consistently adhere to patch management procedures.

[REDACTED]

[REDACTED] IT SOX controls require administrators to apply recommended patches to production servers. In addition, administrators should document and obtain approval of all patch testing.<sup>11</sup> Missing patches could allow a person or malware<sup>12</sup> to read, change or delete files accidentally or maliciously. In addition, undocumented testing could introduce patches in the environment that may cause system resources to become unavailable to users.

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

4. Install approved patches and document patch testing.

### Log Management

Administrators did not configure the Server Automation Software<sup>13</sup> management utility to monitor modifications to log configuration files [REDACTED]

[REDACTED]

[REDACTED] administrators could not consistently review key security events including log-on failures, elevation of privileges by unapproved personnel, modification of logging settings or the modification

<sup>9</sup> [REDACTED]

<sup>10</sup> IT Master Control 07.UNIX.Patch\_Mgmt, version 6, dated January 15, 2010.

<sup>11</sup> IT Master Control 07.UNIX.Testing\_Doc, version 5, dated January 8, 2010.

<sup>12</sup> Software programs designed to damage or perform unwanted actions on a computer system.

<sup>13</sup> A server management utility that automates operating system provisioning and patch management.

<sup>14</sup> A log management utility that enables organizations to collect, store, and analyze log data.

of log ownership and permissions on these servers as required by IT SOX controls and Postal Service policy.<sup>15</sup>

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

5. Configure the log management utility to monitor modifications to log configuration files.
6. Configure servers to send log events to a centralized log repository.

### Mainframe Servers

Administrators did not correctly configure [REDACTED]. Specifically, [REDACTED]. In addition, they did not consistently comply with the patch management process or follow log management procedures to include monitoring of key security events. [REDACTED]

[REDACTED] Administrators should properly configure and monitor servers to mitigate the risk of unauthorized access or undetected malicious activity occurring on the system. See [Appendix B](#) for our detailed analysis of this topic.

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

7. Review and update Linux operating systems account and password settings to comply with IT SOX requirements.
8. Provide administrators with training addressing configuration, patch, and log management procedures supporting IT SOX requirements.

### Other Matters – Shared User Account

We identified an undocumented, shared local user account on each [REDACTED] [REDACTED] we reviewed. Administrators use the account to access the operating systems when directory services<sup>17</sup> are unavailable. They track use of this account with the [REDACTED] application. However, management did not obtain formal approval for this account as required by policy.<sup>18</sup> When notified, management took corrective action to register the account in eAccess. As a result, we are not making a recommendation to address this issue.

<sup>15</sup> IT Master Control 07.UNIX.Sec\_Log\_Mntr\_Config, version 4, dated March 16, 2010 and Handbook AS-805, Section 9-11.5 Audit Log Reviews.

<sup>16</sup> IT Master Controls 07.UNIX.Sec\_Log\_Mntr\_Config, 07.UNIX.Review\_Sec\_Logs, version 7, dated May 3, 2010, 07.UNIX.Patch\_Mgmt, and 07.UNIX.Testing\_Doc.

<sup>17</sup> Directory Services provides for central authentication and authorization.

<sup>18</sup> Handbook AS-805, Section 9-4.2.4, Shared Accounts.

## Management's Comments

Management agreed with our recommendations. In response to recommendation 1, management completed action on May 30, 2010 for all systems not included in the RMP. Additional UNIX controls were documented in the RMP on May 30, 2010. The appropriate sponsors will pursue approval of the RMP and management will revoke developer access if the plan does not receive approval. The target completion date is September 30, 2010.

In response to recommendation 2, management has approved the IBM-AIX security configuration standards and is seeking final approval of the Solaris and Linux standards. The target completion date is July 31, 2010.

To address recommendation 3, management will review and update configuration settings during their semiannual configuration baseline review. In response to recommendation 4, management completed and documented their patch testing and will install approved patches during their current patch cycle. The target completion date for recommendations 3 and 4 is August 31, 2010.

Management addressed recommendation 5 by converting to Critical System Protection<sup>19</sup> monitoring as of June 25, 2010. Management requested closure of this recommendation upon issuance of the final report.

Management will address recommendations 6, 7, and 8 by configuring servers to send log events to a centralized server, updating Linux operating system account and password settings, and providing administrators with appropriate training. The target completion dates are July 31, 2010 for recommendation 6; August 31, 2010 for recommendation 7; and September 30, 2010 for recommendation 8. See [Appendix D](#) for management's comments in their entirety.

## Evaluation of Management's Comments

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

The OIG considers recommendations 1 and 2 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.

---

<sup>19</sup> Management refers to Critical Site Protector but the product name is actually Critical System Protection.

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.



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

cc: Harold E. Stark  
Susan M. LaChance  
Joseph J. Gabris  
Corporate Audit Response Management

## APPENDIX A: ADDITIONAL INFORMATION

### BACKGROUND

The UNIX server environment includes the [REDACTED] and the IT Corporate Help Desk Organization sections of the Information Technology Computing Services group manage these servers.

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 the development and implementation of internal IT SOX master controls, both general computer and application specific controls. The IT SOX CMO identified [REDACTED] master controls applicable to the UNIX operating system environment.

### OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether the Postal Service UNIX operating system environment, hosting applications supporting the financial statements, complies with IT SOX master controls. We limited our scope to controls applicable to the UNIX operating system environment.

As of March 2010, there were [REDACTED] UNIX servers in the production environment, [REDACTED] of which support [REDACTED] SOX in-scope applications.<sup>20</sup> To achieve our objective, we judgmentally selected a sample of [REDACTED] servers supporting [REDACTED] SOX in-scope applications and reviewed their configuration files. We also judgmentally sampled [REDACTED] applicable UNIX workstations and reviewed their screensaver inactivity timeout settings. In addition, we interviewed administrators, observed key processes and procedures, and reviewed applicable Postal Service policies.

We conducted this performance audit from November 2009 through July 2010 in accordance with generally accepted government auditing standards and included such tests of internal controls, as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient and 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 June 21, 2010, and included their comments


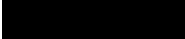



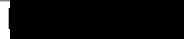
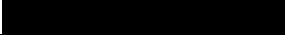
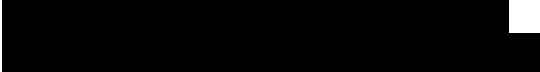
---

<sup>20</sup> 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.



where appropriate. We used manual and automated techniques to analyze the configuration data. Based on the results of these tests and assessments, we concluded the data were sufficient and reliable to use in meeting the objective.

**PRIOR AUDIT COVERAGE**

Report Title	Report Number	Final Report Date	Results
<p><i>UNIX Access Controls at</i>  </p>		<p>8/10/2009</p>	 
<p><i>Access Controls at the</i>    <i>Centers for Fiscal Year 2008</i></p>		<p>8/15/2008</p>	<p>We recommended management develop an automated procedure to identify and remove from                         Management agreed with the finding and recommendation and took action to address the issue in May 2010.</p>

Report Title	Report Number	Final Report Date Report	Results
[REDACTED]	[REDACTED]	6/3/2008	[REDACTED]

## APPENDIX B: DETAILED ANALYSIS

### Account and Password Management

Administrators did not properly configure account and password settings [REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED] did not configure their workstation to lock after 30 minutes of inactivity.

The IT SOX controls<sup>21</sup> require:

- Accounts to lock after six unsuccessful log-on attempts.
- Operating system account passwords to change from their default value.
- UNIX workstations to display a password-protected screensaver after a maximum of 30 minutes of inactivity.
- Passwords changed at least every 45 days for administrative accounts<sup>22</sup> or at least every 90 days for non-administrative accounts.

Management took corrective actions when we brought these issues to their attention.

### Mainframe Servers

- [REDACTED]
- [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]
  - [REDACTED]

<sup>21</sup> Master Controls 07.UNIX.Account\_Suspend, version 11, dated December 23, 2009, 07.UNIX.Default\_Acct\_PW\_Chg, version 8, dated February 22, 2010, 07.UNIX.Inactivity\_Timeout, version 9, dated December 23, 2009; and 07.UNIX.PW\_Parm\_Config, version 4, dated December 23, 2009.

<sup>22</sup> Root is the administrative account on UNIX, Linux, and AIX operating systems.

<sup>23</sup> Master Controls 07.UNIX.Account\_Suspend, and 07.UNIX.PW\_Parm\_Config.

The administrator took action to correct the [REDACTED]  
[REDACTED] when we brought these issues to the administrator's attention.

**APPENDIX C: MASTER CONTROL COMPLIANCE**

The table below shows the level of compliance with the 12 UNIX master controls that were tested.

<b>UNIX Master Controls Compliance</b>				
<b>UNIX Master Control</b>	<b>Sample Size</b>	<b>Number Tested</b>	<b>Number Passed</b>	<b>Percent In Compliance</b>
Configuration Baseline <sup>24</sup>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Administrative Password Management	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Segregation of Duties	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Password Encryption	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Default Account Password Change	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Inactivity Timeout <sup>25</sup>	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Patch Management	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Testing Documentation	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Account Suspension	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Password Parameter Configuration	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Review Security Log	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
Security Log Monitor Configuration	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

<sup>24</sup> We did not test the configuration baseline master control because management had not approved configuration baseline standards for all UNIX operating systems.

<sup>25</sup> We sampled UNIX workstations to test this master control.

**APPENDIX D: MANAGEMENT'S COMMENTS**

ROSS PHILO  
EXECUTIVE VICE PRESIDENT  
CHIEF INFORMATION OFFICER



July 16, 2010

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

SUBJECT: Transmittal of Draft Audit Report – UNIX Operating System Master Controls  
(Report Number IS-AR-10-DRAFT), Project Number 10RG005IT000

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1 through 8 of the report; the response is attached.

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

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

A handwritten signature in black ink that reads "Ross Philo".

Ross Philo  
Executive Vice President  
and Chief Information Officer

Attachment

cc: [audittracking@uspsoig.gov](mailto:audittracking@uspsoig.gov)  
Susan M. LaChance  
Deborah J. Judy  
Charles L. McGann  
Harold E. Stark  
Joseph J. Gabris  
Jamie Gallagher

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

UNIX Operating System Master Controls  
(Report Number IS-AR-10-DRAFT) Project Number 10RG005IT000  
Page #2

We recommend the director, Information Technology Operations, direct the manager, Information Technology Computing Services, to:

1. Review and update system permissions to ensure developers possess read-only privileges to files in the production environment.

**Management agrees with the recommendation.** This action was completed May 30, 2010 for all systems not included in the Risk Mitigation Plan (RMP). The RMP is pending approval and applies to EDW load servers (EIR 1420). Additional UNIX controls documented in the plan were initiated on May 30, 2010. Approval of the RMP will be pursued by the appropriate sponsors. If approval is not granted, the access will be revoked.

Anticipated completion date: September 30, 2010

We recommend the manager, Corporate Information Security, coordinate with the director, Information Technology Operations, to:

2. Establish and approve baseline security configuration standards for all UNIX operating system types.

**Management agrees with the recommendation.** Security configuration standards have been established for all UNIX operating system types; IBM-AIX standards are approved, Solaris standards are out for Jerry Reynolds's signature and Linux operating systems standards are in the final stage of approval and will be ready the week of July 19, 2010.

Anticipated completion date: July 31, 2010

We recommend the director, Information Technology Operations; direct the manager, Information Technology Computing Services, to:

3. Review and update UNIX operating system user account and password settings to comply with IT SOX requirements.

**Management agrees with the recommendation.** This will be validated during our semiannual Configuration Baseline review.

Anticipated completion date: August 31, 2010

4. Install approved patches and document patch testing.

**Management agrees with the recommendation.** This will be completed during the current patch cycle. Patch testing and management review prior to release to Production has been completed for all platforms. Artifacts are available for review on request.

Anticipated completion date: August 31, 2010

5. Configure the log management utility to monitor modifications to log configurations files.

**Management agrees with the recommendation.** The conversion to Critical Site Protector (CSP) based monitoring was completed June 25, 2010. Management request closure is reported, in the final report, for this citing.

UNIX Operating System Master Controls  
(Report Number IS-AR-10-DRAFT) Project Number 10RG005IT000  
Page #3

6. Configure servers to send log events to a centralized log repository.

**Management agrees with the recommendation** and will configure servers to send log events to a centralized log repository.

Anticipated completion date: July 31, 2010.

7. Review and update Linux operating systems account and password settings to comply with IT SOX requirements.

**Management agrees with the recommendation** and will update Linux operating systems account and password settings to comply with IT SOX requirements.

Anticipated completion date: August 31, 2010

8. Provide administrators with training addressing configuration, patch, and log management procedures supporting IT SOX requirements.

**Management agrees with the recommendation** and will provide administrators with training addressing configuration, patch, and log management procedures supporting IT SOX requirements.

Anticipated completion date: September 30, 2010