OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

January 20, 2009

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Service Continuity at the Information Technology and Accounting Service Centers for Fiscal Year 2008
(Report Number IS-AR-09-003)

This report presents the results of our audit of service continuity at the [redacted], Information Technology and Accounting Service Centers (IT/ASC) (Project Number 08RD001IS004). The objective of this audit was to determine whether service continuity procedures are in place to minimize the risk when unexpected events occur and to ensure critical operations continue without unreasonable interruption. We performed this self-initiated review as part of the fiscal year (FY) 2008 information systems audit of general controls at the U.S. Postal Service's IT/ASCs. See Appendix A for additional information about this audit.

## Conclusion

Overall, we believe management adequately developed the infrastructure and service continuity processes and procedures to maximize the availability of critical Postal Service operations. The Postal Service is undergoing significant changes in the computing infrastructure, including virtualization and replication. They have made progress building a replication process between the [redacted] IT/ASCs and have established testing schedules for critical and sensitive applications. To further minimize the risk of service disruption, management could improve processes for [redacted] tapes and procedures for facility recovery program updates at the [redacted] IT/ASC.

### UNIX Tape Off-Site Storage

[redacted] This occurred because management did not assign responsibilities for these procedures after organizational changes. San Mateo personnel believed that [redacted] administered off-site tape storage procedures while the Eagan personnel were unaware of this responsibility. [redacted]. See Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the Manager, Information Technology Computing Services, to:

1. Designate the personnel responsible for administering the backup process for the [redacted] Host Computing Services Center.

2. Implement procedures to ensure [redacted] backup tapes are stored off-site.

## Facility Recovery Plan Update

The Facility Recovery Plan was not current for the [redacted] IT/ASC. This occurred because management did not assign responsibilities for these procedures after organizational changes and [redacted] personnel believed that [redacted] Management Support Service Center was responsible for updates. An updated plan could help avoid confusion during personnel evacuation in an emergency situation and help resume business operations as quickly as possible. See Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the Manager, Information Technology Computing Services, to:

3. Clarify the responsibility for maintaining and administering the Facility Recovery Plan for the [redacted] Information Technology and Accounting Service Center.

4. Update the Facility Recovery Plan for the [redacted] Information Technology and Accounting Service Center.

## Advanced Computing Environment Server Contingency Planning

Audit trails of backup data for [redacted] servers did not clearly show that the data for the servers were stored off-site. Further, applications running on these servers were not tested in a disaster recovery simulation. Specifically, the [redacted] server we selected for review at the [redacted] IT/ASC was backed up locally, but audit trails did not clearly show that the data for the server [redacted] This occurred because the Postal Service is undergoing significant changes from stand-alone physical servers to a virtualization[1] and replication environment. Routinely duplicating or backing up data files to off-site storage prevents or minimizes the damage to automated operations that can occur from

[1] Virtualization is a software technology that lets one computer do the job of multiple computers by sharing the resources of a single computer across multiple environments. Virtual servers and virtual desktops allow hosting of multiple operating systems and multiple applications locally and in remote locations, freeing users from physical and geographical limitations. The benefits include energy savings, lower capital expenses due to more efficient use of hardware resources, high availability of resources, better desktop management, increased security, and improved disaster recovery processes.

unexpected events. Performing periodic testing of application backup data helps ensure application and data recoverability in the event of a disaster. We are not making a recommendation because management is currently deploying a replication process that will address the audit trail issue. In addition, because of our review, management recognized the need for application recovery testing and has re-prioritized resources to meet their testing schedules.

## Management's Comments

Management agreed with all four recommendations. In response to recommendation 1, management stated that the Storage Management group within Host Computing Services is responsible for all backup processes in [redacted]. In addressing recommendation 2, management stated that the offsite storage process was developed in accordance with a Sarbanes-Oxley requirement. Management will provide supporting documentation on the process by March 31, 2009. Further, in response to recommendation 3, management stated the Manager, Management Support Service Center, is responsible for maintaining and administering the [redacted] Facility Recovery Plan. Finally, for recommendation 4, management stated that an updated Facility Recover Plan is currently available. Management considers actions completed on recommendations 1, 3, and 4. See Appendix C for management comments, in their entirety.

## Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General (OIG) considers management's comments responsive to each of the recommendations, and their corrective actions should resolve the issues identified in the report.

The OIG considers recommendation 2 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. This recommendation should not be closed in the follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Frances E. Cain, Acting Director, Information Systems, or me at (703) 248-2100.

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

Tammy L Whitcomb
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: Ross Philo
H. Glen Walker
Harold E. Stark
Joseph J. Gabris
Katherine S. Banks

# APPENDIX A: ADDITIONAL INFORMATION

## BACKGROUND

During FY 2006, management purchased mainframe disaster recovery equipment and upgraded the mainframe operating system at the [redacted] IT/ASCs. The new equipment enabled the [redacted] facilities to electronically send replicated production mainframe files directly to storage devices located at the [redacted], making each site a [redacted] disaster recovery location [redacted]. Application testing followed installation of the mainframe replication process.

Management began deploying a similar replication process for the distributed platforms for [redacted] servers. However, management faced challenges building the infrastructure for these distributed platforms, which resulted in delays in the application disaster testing. As an interim measure, the [redacted] IT/ASCs backed up some production data to tape media and stored it [redacted].

## OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine if service continuity procedures are in place to minimize the risk when unexpected events occur, and to ensure critical operations continue without interruption or can be resumed within a reasonable amount of time.

The scope of our review included reviewing continuity of operations planning and testing for Postal Service facilities. We also reviewed disaster recovery testing for critical Postal Service facilities, workgroups, and computer applications residing on mainframe and distributed platforms, [redacted]

The audit covered the following primary platforms used in the Postal Service's computing environment.

- [redacted][2] [redacted][3] [redacted]
- [redacted][4]

[2] [redacted]™ [redacted]
[3] [redacted]
[4] [redacted]

We judgmentally selected several applications[5] for review on these platforms. Criteria used to make our selections included production status, financial relevance, sensitivity or criticality, platform, and location. Table 1 provides a summary of the applications reviewed.

**Table 1: Applications Selected for Review by Platform**

| [redacted] | [redacted] | [redacted] |
|---|---|---|
| Mainframe | OMAS; ChangeMan | EMRS |
| UNIX | eAwards | EMRS |
| Windows | OMAS | SRM |
| Databases | eAwards (Oracle)<br>ChangeMan (DB2) | EMRS (Oracle)<br>PTS (DB2) |

To accomplish our objective, we interviewed Postal Service facility officials, analyzed Postal Service policies and procedures, and tested related internal controls. To determine if service continuity plans were complete and tested, we reviewed facility, workgroup, and application recovery plans. We also analyzed documentation related to the testing of these plans at each [redacted]. To determine if the Postal Service was backing up critical production files and servers, we reviewed system-generated reports and observed back-up tape handling procedures at the [redacted]

We conducted this audit from April 2008 through January 2009 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We used manual and automated techniques to analyze the computer-processed data. Based on the results of these tests and assessments, we generally concluded the data were sufficient and reliable to use in meeting the objective. We discussed our observations and conclusions with management officials during the audit and on December 10, 2008, and included their comments where appropriate.

[5] We selected the following applications: Official Mail and Accounting System (OMAS), Electronic Awards System (eAwards), Electronic Marketing Reporting System (EMRS), Serena ChangeMan, Sales Resource Management (SRM), and Product Tracking System (PTS).

## PRIOR AUDIT COVERAGE

| Report Title | Report Number | Final Report Date | Monetary Impact | Report Results |
|---|---|---|---|---|
| *Disaster Recovery Testing for Critical Postal Service Applications at the [redacted] California Information Technology and Accounting Service Centers for Fiscal Year 2007* | IS-AR-07-018 | September 14, 2007 | N/A | In general, the Postal Service established and updated continuity plans and procedures relating to essential business functions at the IT/ASCs. However, we provided recommendations for implementing the disaster recovery infrastructure to test all critical midrange applications; developing a schedule documenting when they will conduct full operational recovery tests for critical applications; and prioritizing testing of mainframe disaster recovery infrastructure to complete full operational recovery tests of all critical mainframe applications. Management established the schedule for testing applications; however, actions for the remaining recommendations have not been completed. |
| *Mainframe Service Continuity Planning and Testing at the [redacted] California Information Technology and Accounting Service Centers* | IS-AR-07-002 | November 16, 2006 | N/A | Overall, Postal Service administrators adequately implemented the service continuity programs. However, we recommended testing of the disaster recovery equipment at the Eagan and [redacted] facilities. This recommendation was subsequently completed and closed. |

# APPENDIX B: DETAILED ANALYSIS

## [redacted] Tape Off-Site Storage

[redacted]. Postal Service staff is responsible for ejecting and preparing tape media for storage on a scheduled basis.

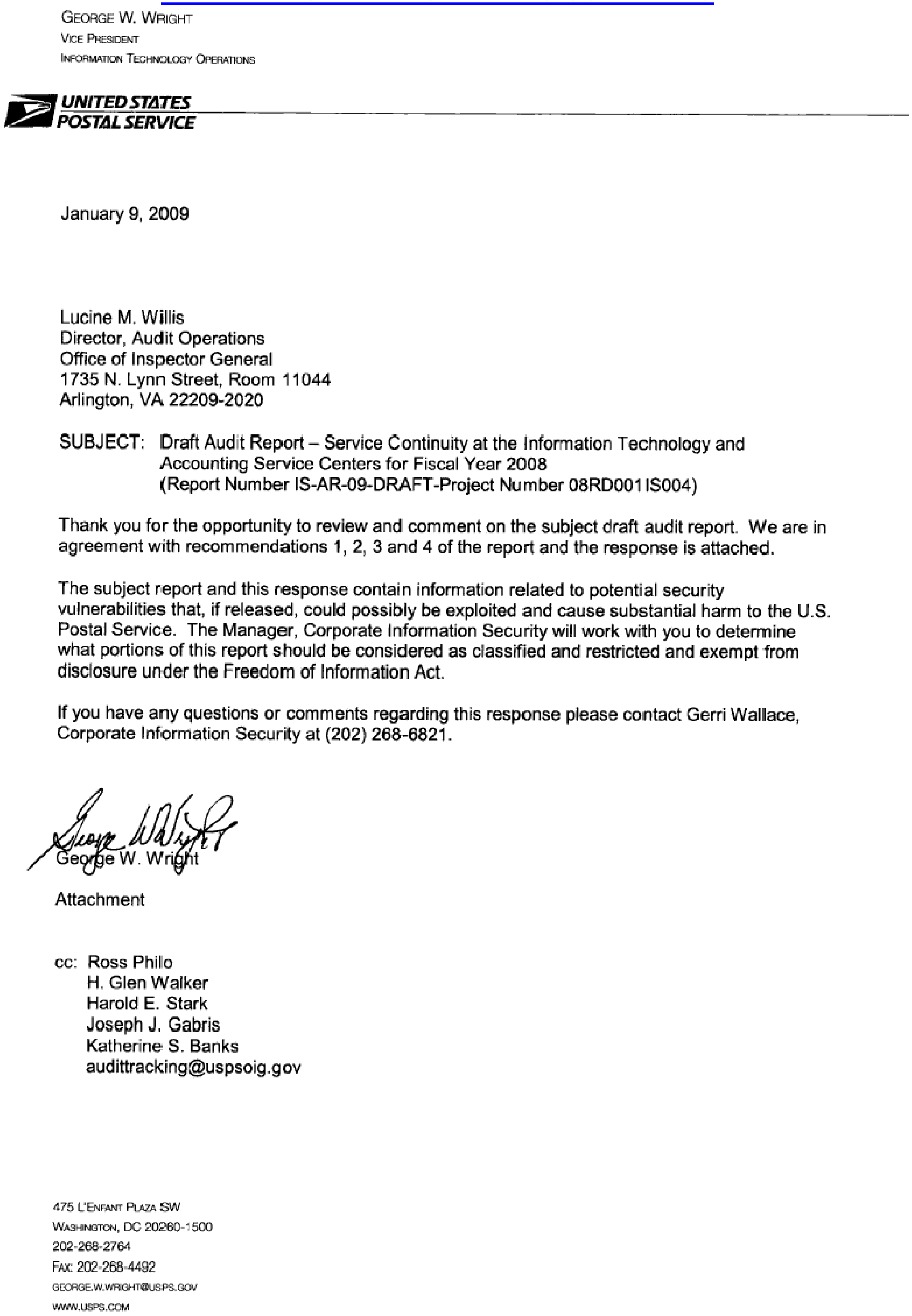
At the [redacted], we sampled an [redacted] application server [redacted] and traced the audit trail to ensure the data was backed up and stored xxxxxxxx. [redacted]. We learned that [redacted]. Postal Service personnel noted there are nearly [redacted] servers at the [redacted] which include some critical applications. Management immediately initiated action to assess the overall backup environment.

## Facility Recovery Plan Update

The [redacted] Facility Recovery Plan (FRP) did not contain current information. We reviewed various documents relating to service continuity and disaster recovery planning. Postal Service policy[6] requires the FRP to include information about the process of restoring a facility to a condition so it meets appropriate personnel, business unit, and safety requirements; and making the facility ready to support business functions and computer programming support. [redacted] FRP included the detailed information in the *Occupant Emergency Plan*. [redacted] did not have the same document, but included similar information in the FRP. However, this document was last updated in February 2006 and contained obsolete information. Management was unable to determine the ownership and responsibility for updating the document.

[6] Handbook AS-805, *Information Security*, Section 12-4.4.2, Facility Recovery Plan, dated March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006).

## APPENDIX C: MANAGEMENT'S COMMENTS



GEORGE W. WRIGHT
VICE PRESIDENT
INFORMATION TECHNOLOGY OPERATIONS

UNITED STATES
POSTAL SERVICE

January 9, 2009

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

SUBJECT: Draft Audit Report – Service Continuity at the Information Technology and Accounting Service Centers for Fiscal Year 2008 (Report Number IS-AR-09-DRAFT-Project Number 08RD001IS004)

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 1, 2, 3 and 4 of the report and 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.

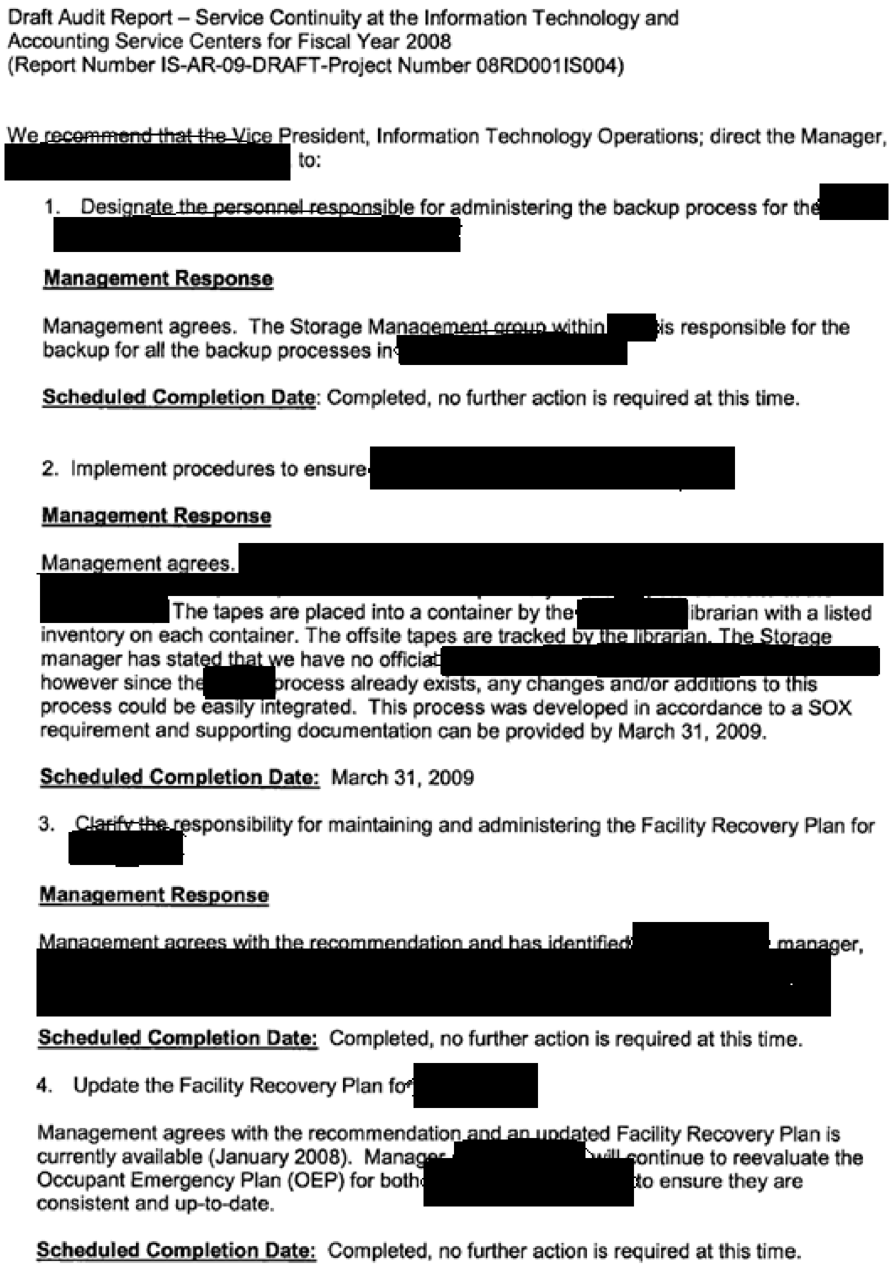
If you have any questions or comments regarding this response please contact Gerri Wallace, Corporate Information Security at (202) 268-6821.

George W. Wright

Attachment

cc: Ross Philo
H. Glen Walker
Harold E. Stark
Joseph J. Gabris
Katherine S. Banks
audittracking@uspsoig.gov

475 L'ENFANT PLAZA SW
WASHINGTON, DC 20260-1500
202-268-2764
FAX: 202-268-4492
GEORGE.W.WRIGHT@USPS.GOV
WWW.USPS.COM



Draft Audit Report – Service Continuity at the Information Technology and
Accounting Service Centers for Fiscal Year 2008
(Report Number IS-AR-09-DRAFT-Project Number 08RD001IS004)

We recommend that the Vice President, Information Technology Operations; direct the Manager, [redacted] to:

1. Designate the personnel responsible for administering the backup process for the [redacted]

**Management Response**

Management agrees. The Storage Management group within [redacted] is responsible for the backup for all the backup processes in [redacted]

**Scheduled Completion Date**: Completed, no further action is required at this time.

2. Implement procedures to ensure [redacted]

**Management Response**

Management agrees. [redacted] The tapes are placed into a container by the [redacted] librarian with a listed inventory on each container. The offsite tapes are tracked by the librarian. The Storage manager has stated that we have no official [redacted] however since the [redacted] process already exists, any changes and/or additions to this process could be easily integrated. This process was developed in accordance to a SOX requirement and supporting documentation can be provided by March 31, 2009.

**Scheduled Completion Date:** March 31, 2009

3. Clarify the responsibility for maintaining and administering the Facility Recovery Plan for [redacted]

**Management Response**

Management agrees with the recommendation and has identified [redacted] manager, [redacted]

**Scheduled Completion Date:** Completed, no further action is required at this time.

4. Update the Facility Recovery Plan for [redacted]

Management agrees with the recommendation and an updated Facility Recovery Plan is currently available (January 2008). Manag [redacted] will continue to reevaluate the Occupant Emergency Plan (OEP) for both [redacted] to ensure they are consistent and up-to-date.

**Scheduled Completion Date:** Completed, no further action is required at this time.