



July 30, 2009

ROSS PHILO  
VICE PRESIDENT, CHIEF INFORMATION OFFICER

ROBERT J. PEDERSEN  
TREASURER

SUBJECT: Audit Report – Disaster Recovery Capabilities of the  
Enterprise Payment Switch (Report Number IS-AR-09-009)

This report presents the results of our audit of the disaster recovery capabilities of the Enterprise Payment Switch (Project Number 09RG012IS000). This is the last in a series of reports issued in response to the October 2005 Value Proposition Agreement between the U.S. Postal Service and the U.S. Postal Service Office of Inspector General (OIG). The OIG audits focused on evaluating the security of the Enterprise Payment Switch solution to verify that routing and storage of customer information are secure within the Postal Service systems. The objective of this audit was to determine whether disaster recovery capabilities of the Enterprise Payment Switch are in place and effective. See [Appendix A](#) for additional information about this audit.

### **Conclusion**

Overall, the disaster recovery capabilities of the Enterprise Payment Switch are in place. However, management can improve its ability to recover the Enterprise Payment Switch by fulfilling requirements consistent with Postal Service policy, developing a comprehensive application disaster recovery plan (ADRP), and performing full operational recovery testing. If management does not address these weaknesses, it cannot assure recovery of the Enterprise Payment Switch in the event of a catastrophic disaster, which could affect the Postal Service brand. We will report the non-monetary impact (preserving the integrity of the Postal Service brand) in our *Semiannual Report to Congress*.

## Disaster Recovery Plan

The Postal Service does not have a comprehensive ADRP in place for the Enterprise Payment Switch as required.<sup>1</sup> This occurred because Business Continuity Management (BCM) accepted the testing strategy document as the disaster recovery plan to reduce the documentation burden on the development community. In addition, management did not provide an ADRP template for the development community to use as a guide. A comprehensive ADRP<sup>2</sup> increases management's ability to recover the application in the event of a catastrophic disaster. See [Appendix B](#) for our detailed analysis of this issue.

We recommend the Manager, Information Technology Computing Services, direct the Manager, Business Continuity Management, to:

1. Develop an application disaster recovery plan template and make it available to the development community.

We recommend the Manager, Business Continuity Management, and the Program Manager, Enterprise Payment Switch, collaborate to:

2. Create a comprehensive application disaster recovery plan for the Enterprise Payment Switch solution.

## Management's Comments

Management agreed with the recommendations, but did not comment on the non-monetary impact (preserving the integrity of the Postal Service brand).

In response to recommendation 1, management stated that the current Handbook AS-805 (dated June 30, 2009) does not require the use of a template or ADRP testing. The Manager, BCM, will review and update the handbook to reflect new documentation requirements and make it available to the development community. The targeted date for completion is December 1, 2009.

In response to recommendation 2, management stated the Manager, BCM, would use the former ADRP template to update the Enterprise Payment Switch solution. The targeted date for completion is September 1, 2009. See [Appendix C](#) for management's comments in their entirety.

---

<sup>1</sup> Handbook AS-805, *Information Security*, dated March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006). Management released a new version of the handbook on June 30, 2009, that significantly reduced the level of disaster recovery requirements.

<sup>2</sup>

## Evaluation of Management's Comments

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

## Full Operational Recovery Testing

Management did not conduct a full operational recovery test for the Enterprise Payment Switch. Although they performed initial Enterprise Payment Switch testing, management delayed full operational recovery testing until after the developers implemented [REDACTED]

[REDACTED] Without comprehensive operational recovery testing, management risks delays in [REDACTED] should disaster recovery become necessary. [REDACTED] could create customer dissatisfaction and negatively affect the Postal Service brand. See [Appendix B](#) for our detailed analysis of this issue.

## Corrective Action Taken

Management performed a full operational recovery test of the Enterprise Payment Switch between April 29 and May 6, 2009 that included tests of the [REDACTED]. We verified management's actions during the audit; therefore, we are not making a recommendation regarding this issue.

The OIG considers recommendation 2 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. The recommendation should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendation can be closed. We will report the non-monetary impact (preserving the integrity of the Postal Service brand) in our *Semiannual Report to Congress*.

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

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

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

Attachments

cc: Robert J. Wolter  
George W. Wright  
Charles L. McGann  
Katherine S. Banks  
William P. Harris

## APPENDIX A: ADDITIONAL INFORMATION

### BACKGROUND

In calendar year 2008, the Postal Service processed more than 323 million debit and credit card transactions totaling more than \$10.8 billion, including transactions originating at traditional post offices, self-service centers, and the Internet; as well as mail and telephone orders. To meet updated performance, reliability, flexibility, and cost objectives associated with debit and credit card transaction processing, the Postal Service developed the Enterprise Payment Switch solution. This solution encompasses new software applications and more than 20 pre-existing Postal Service and vendor systems designed to work together to provide a secure processing environment for nearly all debit and credit card transactions. The Business Impact Assessment classifies the Enterprise Payment Switch as [REDACTED]. The Enterprise Payment Switch supports a broad range of electronic payment types including, but not limited to, credit card, debit card, stored value, checks, and Internet payments.

To address the Value Proposition Agreement objective, we accomplished the project in multiple phases and provided recommendations in four prior audit reports:<sup>3</sup>

- Phase I: Requirements and Design.
- Phase II: Preparation for Security Testing.
- Phase III: Security Testing.

The objective of Phase III included an evaluation of disaster recovery capabilities. However, [REDACTED]

[REDACTED]. As a result, the OIG deferred an audit of disaster recovery capabilities for the Enterprise Payment Switch to provide the Postal Service an opportunity to [REDACTED]. This audit report presents the results of Phase IV of the audit.

### OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether disaster recovery capabilities of the Enterprise Payment Switch are in place and effective. To accomplish our objective we reviewed documentation and applicable policies and procedures, and interviewed key officials assigned to the Information Technology Operations Portfolio and Corporate Treasury functions. We also examined other materials we deemed necessary. In addition, we reviewed the Payment Switch testing strategy,<sup>4</sup> architectural diagram, test plans and results, and other information pertinent to the audit objective.

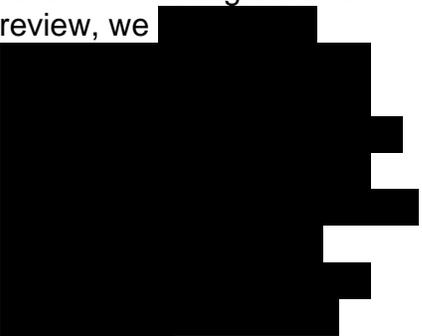
---

<sup>3</sup> See Prior Audit Coverage for details of the reports and results.

<sup>4</sup> Enterprise Payment Switch Security/Failover/Disaster Recovery Testing Strategy, Version 0.19, dated August 2, 2007.

We conducted this performance audit from February through July 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 did not rely on computer-generated data to support our audit findings. We discussed our observations and conclusions with management on July 6, 2009, and included their comments where appropriate.

**PRIOR AUDIT COVERAGE**

Report Title	Report Number	Final Report Date	Report Results
<i>Enterprise Payment Switch Solution Phase I: Requirements and Design</i>	IS-AR-06-017	September 27, 2006	<p>Management was designing and developing the Payment Switch solution with security as a priority. However, we</p>  <p>Management concurred with the findings and recommendations.</p>
<i>National Customer Management System Encryption</i>	IS-AR-07-006	December 26, 2006	<p>While conducting the Phase II review, we</p>  <p>Management concurred with the findings and recommendations.</p>

Report Title	Report Number	Final Report Date	Report Results
<p><i>Enterprise Payment Switch Solution Phase II: Preparation for Security Testing</i></p>	<p>IS-AR-07-007</p>	<p>February 23, 2007</p>	<p>Although the Postal Service was developing the Payment Switch with security as a priority, management [REDACTED] [REDACTED] [REDACTED] We provided three recommendations to [REDACTED] [REDACTED]. Management concurred with the findings and recommendations.</p>
<p><i>Enterprise Payment Switch Solution Phase III: Security Testing</i></p>	<p>IS-AR-08-004</p>	<p>February 6, 2008</p>	<p>Management deployed the Payment Switch solution in limited production [REDACTED] [REDACTED] Management also [REDACTED] [REDACTED] Management concurred with the findings and recommendations.</p>

## APPENDIX B: DETAILED ANALYSIS

### Disaster Recovery Plan

Rather than developing an ADRP for the Enterprise Payment Switch, the BCM and application administrators informally agreed to use the test strategy as the disaster recovery plan.

According to Handbook AS-805 in place at the time we performed the audit fieldwork,<sup>5</sup> a disaster recovery plan must be created for all critical and business controlled criticality information resources. The handbook also states that an ADRP template is available on the Information Technology website. Although we could not confirm whether the template was available when management tested the Payment Switch application, we confirmed that the ADRP template is currently unavailable.

On June 30, 2009, subsequent to our fieldwork, management released a new version of handbook AS-805. Although the handbook no longer requires management to develop an ADRP, we believe doing so is imperative to ensure immediate and full recovery of this critical application in the event of a disaster.<sup>6</sup>

We compared the testing strategy to other Postal Service disaster recovery plans<sup>7</sup> and identified several key attributes that were missing from the testing strategy. While the Payment Switch testing strategy addressed the disaster recovery testing objective, scope, environment, components, and testing approach, it did not include key elements of a comprehensive disaster recovery plan, such as:

1. Roles and responsibilities
  - a) Point of contact list (primary and secondary)
  - b) Recovery assessment team
2. Service restoration requirements
  - a) Disaster recovery components
  - b) Additional disaster recovery requirements
3. Recovery consideration
  - a) Level of emergency
  - b) Timing of event
  - c) Priority recovery listing

---

<sup>5</sup> Chapter 12, Disaster Recovery Planning, Section 12-5.1.

<sup>6</sup> We plan to incorporate a review of the updated version of Handbook AS-805 in a future audit.

<sup>7</sup> *Host Computing Services Disaster Recovery Plan*, Section 4.2.2 Procedures Mainframe – [REDACTED] Version 1.0, dated September 12, 2008 and *Business Information Systems Disaster Recovery Plan*, Version 1.0, dated October 1, 2007

4. Plan maintenance history
5. Reporting and documentation
  - a) Disaster recovery status report
  - b) Assessment and lessons learned report
6. Checklist for disaster recovery configurations

### Full Operational Recovery Testing

Management did not perform a full operational recovery test of the Enterprise Payment Switch application. According to Handbook AS-805,<sup>8</sup> management must test the ADRP for critical and business-controlled criticality applications within 180 days of placing an application into production. In addition, management must perform a full operational recovery test of the disaster recovery plan for critical applications every 18 months. However, management [REDACTED]

[REDACTED] the Payment Switch.

In the testing strategy, management [REDACTED]  
[REDACTED]. We confirmed these servers are now installed and functioning at the [REDACTED]. Although the BCM intended to test the [REDACTED], our review prompted the BCM to expedite full operational recovery testing of the Enterprise Payment Switch application. In May 2009, the BCM and application administrators completed a full operational test. The application passed the testing requirements.

---

<sup>8</sup> Chapter 12, Section 12-5-2.1 (c) and (d).

**APPENDIX C: MANAGEMENT'S COMMENTS**

ROSS PHILO  
Executive Vice President  
Chief Information Officer



July 17, 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 – Disaster Recovery Capabilities of the Enterprise Payment  
Switch (Report Number IS-AR-09-DRAFT) Project Number 09RG012IS000

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

A handwritten signature in cursive script that reads "Ross Philo".

Ross Philo

Attachment

cc: George W. Wright  
Robert J. Wolter  
Charles L. McGann  
Harold E. Stark  
Joseph Gabris  
Jeannie Thomas  
Katherine S. Banks  
audittracking@uspsaig.gov

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

Disaster Recovery Capabilities of the Enterprise Payment Switch - Report Number IS-AR-09-  
DRAFT (Project Number 09RG012IS000)

We recommend the Manager, Information Technology Computing Services; direct the Manager,  
Business Continuity Management to:

1. Develop an application disaster recovery plan template and make it available to the  
development community.

**Management Response**

Management agrees, however today's AS-805 (posted June 30, 2009) does not require  
the use of an application disaster recovery plan template nor any disaster recovery  
testing (application or full operational recovery test).

Manager, Business Continuity Management will review and update the AS-805 to  
reflect the new documentation requirements and make that available to the development  
community.

**Scheduled Completion Date:** December 1, 2009

2. Update the disaster recovery plan for the Enterprise Payment Switch solution.

**Management Response**

Management agrees. Manager, Business Continuity Management will use the old  
application disaster recovery plan template to update the Enterprise Payment Switch  
solution.

**Scheduled Completion Date:** September 1, 2009