



February 12, 2008

GEORGE W. WRIGHT
ACTING VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

SUSAN M. PLONKEY
VICE PRESIDENT, CUSTOMER SERVICE

PAUL VOGEL
MANAGING DIRECTOR, GLOBAL BUSINESS AND SENIOR VICE PRESIDENT

SUBJECT: Audit Report – Security Review of the Electronic Verification System
(Report Number CRR-AR-08-002)

This report presents the interim results of our security review of the Electronic Verification System (eVS) (Project Number 07RG011IS000), which is part of a series of reviews of the PostalOne! System.¹ Our objectives were to determine if the U.S. Postal Service is adequately securing the data and system and whether there were any security issues management should address in the proposed re-engineering of the eVS.

In addition to this audit, on August 7, 2007, we started a project to conduct security scans of eVS using automated tools. We suspended that project on September 14, 2007, due to planned eVS infrastructure upgrades, but will continue our security scans in this area once upgrades are completed. Our audit findings in this report are focused on two security issues management should address in the re-engineering of eVS.

First, the primary external file transfer method used to receive electronic manifests from major mailers is not secure. Secondly, [REDACTED]

[REDACTED] We recommended employing secure methods and relying on the expertise of the Data Transport Services professionals in ensuring the file transfer method employed by eVS is secure. Management agreed with recommendations 1 and 2 and has initiatives in progress, completed, or planned to address the issue in this report. We also recommended [REDACTED]

[REDACTED] and indicated they would accept

¹ We have another project in process entitled Review of Application Controls of Postal Service's PostalOne! System (Project Number 07RG006IS000).

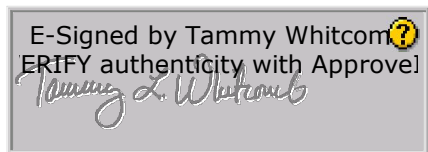
the residual risk. Accordingly, we do not plan to pursue these recommendations through the formal audit resolution process.

During the audit, we informed Information Technology management that a default account was in the production database. When told of this issue, management promptly removed the account from the customer acceptance test and production databases.

Business mailers forwarded about 66.7 million records to the Postal Service during fiscal year (FY) 2007 using an insecure file transfer method. Implementing recommendations 1 through 4 would result in stronger controls over eVS production data, which would help preserve the integrity of the business-sensitive data at risk in this application, safeguard customer goodwill, and protect the Postal Service brand. Management did not comment on the potential non-monetary benefits described in this report. We will report these non-monetary impacts in our *Semiannual Report to Congress*.

The U.S. Postal Service Office of Inspector General (OIG) considers recommendation 2 significant, and therefore, requires OIG concurrence before closure. The OIG requests written confirmation when corrective actions are completed for recommendation 2. 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 during the audit. If you have any questions, or need additional information, please contact Paul Kuennen, Director, Cost, Revenue, and Rates, or me at (703) 248-2100.

An e-signature block with a grey background. It contains the text "E-Signed by Tammy Whitcomb" followed by a yellow question mark icon. Below this is the text "VERIFY authenticity with Approve!". At the bottom of the block is a handwritten signature in cursive that reads "Tammy L. Whitcomb".

Tammy L. Whitcomb
Deputy Assistant Inspector General
for Revenue and Systems

cc: H. Glen Walker
Harold E. Stark
Katherine S. Banks

INTRODUCTION

Background

The Electronic Verification System (eVS) is a key component of the PostalOne! System. eVS allows high-volume package mailers and package consolidators to document and pay postage using electronic manifest files rather than paper forms. Manifest files are transmitted to the U.S. Postal Service network via either File Transfer Protocol (FTP) or Electronic Data Interchange over the Internet (EDI/INT). An Oracle database stores the eVS data.

There are 36 Postal Service distribution facilities that accept eVS mailings at their business mail entry units (BMEUs). The eVS mailers are permitted to drop shipments at any destination delivery unit (DDU). The mailers present eVS mailings to the distribution facility or DDU that is scheduled via the Facility Access and Shipment Tracking System. Facilities accept the scheduled mailings without verification of postage. BMEU technicians use Intelligent Mail Devices (IMD) to scan eVS labels during random samplings of 100 packages per customer, per week. At DDUs, statistical data collectors scan eVS mail they come across for sampling. The eVS information system compares the sampling data to the electronic manifests and adjusts postage based on established business rules.

A Business Impact Assessment (BIA) completed November 1, 2005, defined eVS as a critical system with business-controlled sensitivity.² On March 29, 2007, the Postal Service included eVS as a sub-module³ of the PostalOne! System and management began to re-engineer eVS.

In addition to this audit, on August 7, 2007, we started a project to conduct security scans of eVS using automated tools. However, we had to suspend the project September 14, 2007, due to planned eVS infrastructure upgrades. We will continue our security scans in this area once upgrades are completed.

² Systems classified as critical could have a significant negative impact on operations and/or cash flow if the system or its data becomes unavailable. Business-controlled sensitive systems contain information requiring restrictions on access within the Postal Service or disclosure outside of the Postal Service. Both classifications require a greater degree of protection and controls, as identified in Handbook AS-805-A, *Application Information Security Assurance (ISA)*, which explains the application certification and accreditation (C&A) process.

³ Prior to March 29, 2007, eVS was a "module" of PostalOne!, and subject to the ISA process documented in the Enterprise Information Repository for systems. As a "sub-module," eVS will be evaluated in the C&A of PostalOne!.

Objectives, Scope, and Methodology

Our objectives were to determine if the Postal Service was adequately securing the data and system and whether there were any security issues management should address in the proposed re-engineering of the eVS.

To accomplish our objectives, we researched security information from the Postal Service and industry and academia resources. We interviewed key officials within Information Technology (IT) Sales and Marketing Business Systems Portfolio; IT Network Operations Business Systems Portfolio; Corporate Information Security Office (CISO); Data Transport Services (DTS); Database Support Services (DBSS); and Intelligent Mail Address Quality.

The audit team obtained technical documentation of the eVS system and created a diagram of the data flow to confirm our understanding. The audit team reviewed comparisons of file transfer methods and available services.

We evaluated the output from Oracle data dictionary views related to security. We also reviewed Facility Security Database reports available for the eVS acceptance facilities, not including DDU's. We concluded the automated outputs presented an accurate representation of the data and were sufficiently reliable to support the audit objectives.

The audit team observed BMEU eVS sampling operations and physical security controls at three Postal Service facilities. We witnessed the logon procedure for the IMD and observed the sampling performed at a customer site.

We conducted this performance audit from June 2007 through February 2008 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management officials on November 26, 2007, and included their comments where appropriate.

Prior Audit Coverage We did not identify any prior audits or reviews related to the objectives of this audit.

AUDIT RESULTS

Physical security over IMD devices at the three facilities we visited was adequate. Key Oracle database views we reviewed were also generally acceptable. Due to the suspension of the related vulnerability assessment project, we are not assessing the adequacy of eVS security in its entirety.

However, we are reporting two security findings, which management should address in the re-engineering of eVS. First, the primary external file transfer method used to receive electronic manifests from major mailers is not secure. [REDACTED]

The insecure file transfer method [REDACTED] place the confidentiality, integrity, and availability of about 66.7 million data records at risk. Strengthening controls over business-sensitive financial information would assist in preserving customer goodwill and the Postal Service brand.

File Transfer Method

FTP, which most eVS mailers use to transmit the manifest files, does not meet the security requirements that the BIA prescribes. The eVS data is initiated at the major mailer in the form of an electronic manifest file and is primarily transmitted to the Postal Service network via FTP. With FTP, data is sent over the Internet unencrypted in clear text. These eVS manifests enter the Postal Service network at the FTP-IN server – a server which DTS professionals do not support. The data is then transferred within the Postal Service network using Assured File Transfer, which is a secure, internal Postal Service proprietary transfer method DTS manages. Mailers could use a variety of secure

transmission options, which are available through collaboration with DTS.

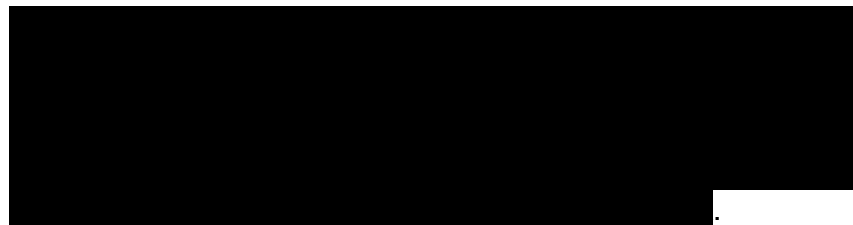
Although alternative file transfer methods exist, the Postal Service is not using the DTS group to implement secure data transmission for the majority of eVS mailers. Publication 91,⁴ updated September 2004, contains the Postal Service's official guidelines for electronic data and file transmission methods for mailers to qualify for discounted rates. This publication does not require a secure method for data and file transmission.

According to its BIA, eVS is a critical system with business-controlled sensitive data. Section 4 of *Information Security Requirements To Be Implemented* requires eVS management to:

- 9-1: Protect data from modification or deletion by unauthorized users.
- 9-8: Encrypt appropriate information transmitted over an untrusted network based on Postal Service encryption and key recovery policies.

According to the BIA, unencrypted information sent via untrusted networks has moderate potential to be used for financial gain through fraud or manipulation. Business partner information⁵ may become exposed, placing the data at risk. This could negatively impact customer goodwill and the Postal Service brand.

Network Access



⁴ Publication 91, *Confirmation Services Technical Guide*, updated September 2004.

⁵ Manifests transmitted from business partners contain unique company identification codes, postage and package information. About 66.7 million records were transmitted via FTP during FY 2007.

6 [Redacted]

44 [Redacted]

[Redacted]

[Redacted]

7 [Redacted]

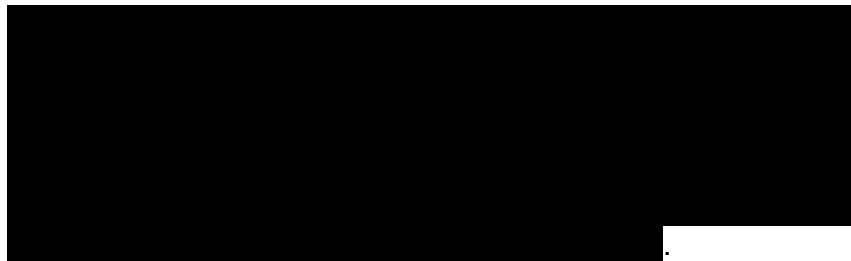
[Redacted]

⁶ *Information Security*, March 2002, updated through September 28, 2006.

⁷ A stylus is provided, however, to mitigate unintended keystrokes by IMD users.



Corrective Actions Taken



Recommendation

We recommend the Vice President, Customer Service, direct the Manager, Marketing Technology and Channel Management, to:

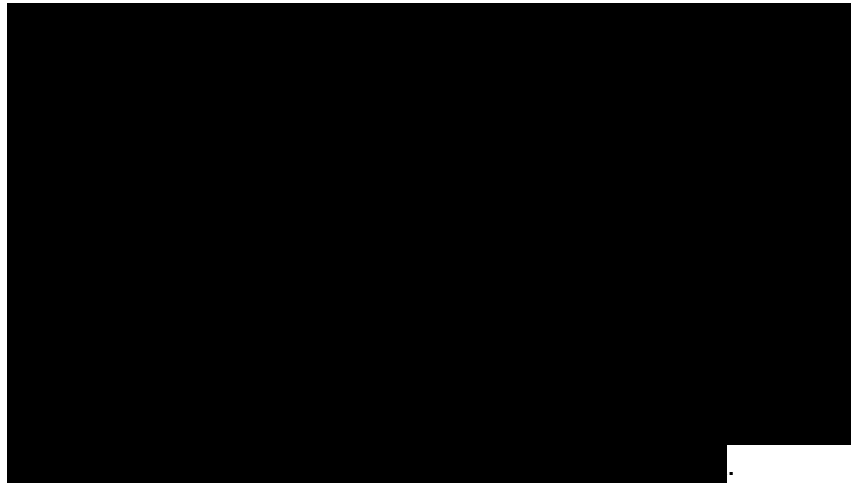
1. Coordinate with the Manager, Information Platform Sales and Marketing Business Systems Portfolio, to facilitate secure external Electronic Verification System file transfer methods.

Management's Comments

Management agreed with the recommendation and stated that, while they believe the risk of using FTP is low, and there have been no issues reported since its initial rollout, they agree that it is in the best interests of the Postal Service and its customers to use secure file transmission protocols. Marketing Technology and Channel Management (MTCM), Product Information Requirements and Information Technology will coordinate with new and existing eVS mailers to convert to a secure transmission protocol during the next 24 months. Management stated that both the Postal Service and mailers must make changes to convert to a secure protocol. A phased-in approach will be used to allow internal and external stakeholders time to plan, coordinate, develop, test and deploy a secure transmission protocol. Management stated this lead time is necessary as many mailers use third party products tailored to meet

existing Publication 205 requirements (e.g., FTP) which may not currently support a secure transmission method. Management's comments, in their entirety, are included in the Appendix to this report.

Evaluation of Management's Comments	Management's comments are responsive to the recommendation, and when fully implemented, should correct the issue identified in the finding.
Recommendation	<p>We recommend the Vice President, Customer Service, direct the Manager, Marketing Technology and Channel Management, to:</p> <ol style="list-style-type: none"> 2. Revise Publication 91 in consultation with the Manager, Corporate Information Security, to require mailers to utilize a secure file transfer method when transmitting manifests for electronic verification to the Postal Service.
Management's Comments	<p>Management agreed with the intent of the recommendation, but proposed an alternative corrective action. Management stated that Publication 91 covers a broader scope than eVS. Management plans to update Publication 205, <i>eVS Business and Technical Guide</i>, to require eVS mailers to use a secure transfer method. The MTCM Group, in consultation with manager, Corporate Information Security and the manager, Product Information Requirements, is already in the process of updating the whole Publication 205. The requirement for secure file transfer will be incorporated in this update, which is scheduled to be completed by September 30, 2008.</p>
Evaluation of Management's Comments	Management's comments are responsive to the recommendation, and when fully implemented, should correct the issue identified in the finding.
Recommendation	<p>We recommend the Acting Vice President, Chief Technology Officer, direct the Manager, Corporate Information Security, to:</p> <ol style="list-style-type: none"> 3. [REDACTED]
Management's Comments	[REDACTED]




Evaluation of Management's Comments

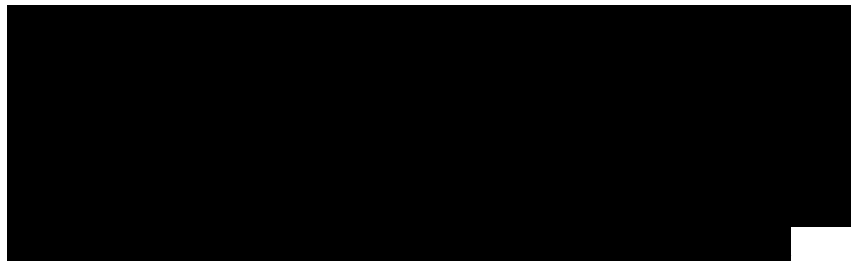
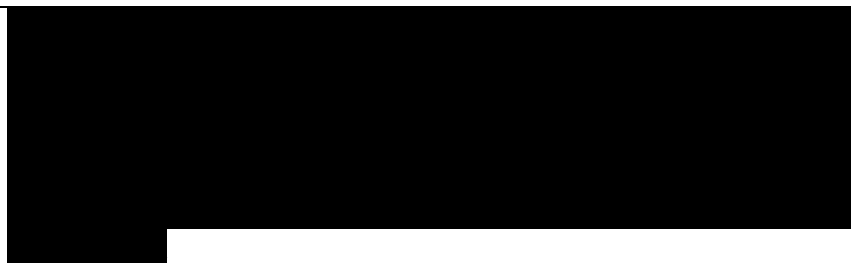
Although management's comments to recommendation 3 indicated disagreement with the recommendation, management chose to accept the risk and has obtained a waiver from the requirements. Thus, we do not plan to pursue the recommendation through the formal audit resolution process.

Recommendation

We recommend the Managing Director, Global Business and Senior Vice President, direct the Director, Global Systems Management, to:

4. 

Management's Comments



[REDACTED]

[REDACTED]

Evaluation of Management's Comments

Although management's comments to recommendation 4 disagreed with the actions recommended, they cited several mitigating factors [REDACTED] and indicated they would accept the residual risk. Thus, we do not plan to pursue the recommendation through the formal audit resolution process.

APPENDIX. MANAGEMENT'S COMMENTS



January 18, 2008

Lucine M. Willis
Acting Director, Audit Operations
1735 North Lynn Street
Arlington, Virginia 22209-2020

SUBJECT: Security Review of the Electronic Verification System (Report Number CRR-AR-08-DRAFT)

This is in response to the Security Review of the Electronic Verification System (Report Number CRR-AR-08-DRAFT). Overall we agree with the accuracy of the findings. However the finding cites Publication 91 as the Postal Service's official guidelines for electronic data and file transmission methods when in fact for eVS, the reference should be Publication 205, eVS Business and Technical Guide.

The Security Review contains four recommendations to the Postal Service. The first two recommendations are addressed by the Vice President, Customer Service; the third recommendation is addressed by the Acting Vice President, Chief Technology Officer and the fourth recommendation by the Managing Director Global Business & Senior Vice President.

Recommendation #1:

Coordinate with the Manager, Information Platform Sales and Marketing Business Systems Portfolio, to facilitate secure external Electronic Verification System file transfer methods.

Response:

Marketing Technology & Channel Management agrees with this recommendation. While we believe the risk of using FTP is low, and there have been no issues reported since its initial roll-out, we agree that it is in the best interest of the Postal Service and our customers to utilize secure transmission protocols. The Marketing Technology & Channel Management (MTCM), Product Information Requirements (PIR), and Information Technology (IT) teams will coordinate with new and existing eVS mailers to convert to a secure protocol over the next twenty-four months. This phased-in approach will allow our mailers, internal business organizations and information technology teams the time to plan, communicate, coordinate with external partners, develop, test and deploy. Both the USPS and mailers must make changes to switch to a secure protocol. This lead time is necessary as many mailers use third party products tailored to meet existing Publication 205 requirements (e.g. FTP), which may not currently support a secure transfer method. The MTCM, PIR, and IT organizations are in the process of contacting existing eVS users to assess the impact of migration to a secure transfer method.

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260

- 2 -

Recommendation #2:

Revise Publication 91 in consultation with the Manager, Corporate Information Security, to require mailers to utilize a secure file transfer method when transmitting manifests for electronic verification to the Postal Service.

Response:

As noted in the opening paragraph, we believe it is Publication 205, eVS Business and Technical Guide, that should be updated to require eVS mailers to use a secure file transfer method. Publication 91 covers a broader scope than eVS. The MTCM Group in consultation with the Manager, Corporate Information Security and the Manager, PIR is already in the process of updating the whole Publication 205. The requirement for secure file transfer will be incorporated in this update which is scheduled to be complete by 09/30/08.

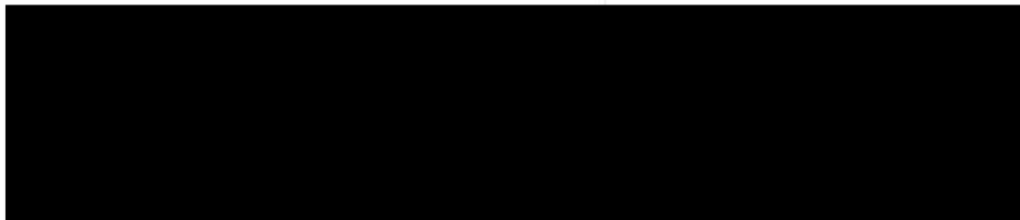
[Redacted]


[Redacted]

[Redacted]

[Redacted]

- 3 -





Susan Plonkey
VP Customer Service

FOR  (PRANAB SHAH)

Paul Vogel
Managing Director Global Business & Senior VP



George W. Wright
Acting Vice President, Chief Technology Officer

Attachment:

- cc: Pritha Mehra, Manager, Mailing Technology & Channel Management
- Pranab Shah, Executive Director Global Business Strategy & Technology
- Harold E. "Pete" Stark, Manager, Corporate Information Security
- Mark A. Mittelman, Manager, Sales & Marketing Portfolio
- John T. Edgar, Manager, Network Operations Portfolio
- Mark J. Stepongzi, Program Manager Information Technology, CISO
- Lily Yee, Information Security Specialist, CISO
- Frances Byrd, Program Manager Sales & Marketing Portfolio
- Melody McGee, Manager Mailer Enterprise Integration
- Katherine Banks, Manager Corporate Response & Audit

Restricted Information



December 03, 2007

OFFICIAL RECORD

SUBJECT: RISK ACKNOWLEDGEMENT/POLICY EXCEPTION - [REDACTED]

Surface Visibility (SV), EIR# 3330.00, has been classified as Non-Sensitive/Non-Critical. The objective of SV is to collect data at the handling unit level (sacks, trays, and tubs) in order to track mail through the site as well as the entire surface transportation network. Handling units are tracked from the time of the initial breakdown (bullpen), through the plant via containers, and on or off trailers.

The SV application utilizes an Intelligent Mail Device (IMD) that runs Windows CE, which refers to the Motorola handheld device running Windows CE .NET version 4.2. The IMD has a small 2 1/4" x 2 3/4" display screen. The IMD is essentially a device that hosts multiple mobile applications including the Electronic Verification Systems (eVS) is one of the applications that utilize the device. [REDACTED]

During the development phase for SV, in 2005, several meetings were held with Corporate Information Security Office (CISO) [REDACTED]

1. [REDACTED]
2. [REDACTED]
3. [REDACTED]
4. [REDACTED]
5. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Restricted Information

OFFICIAL RECORD – Page 2

SUBJECT: RISK ACKNOWLEDGEMENT/POLICY EXCEPTION – [REDACTED]

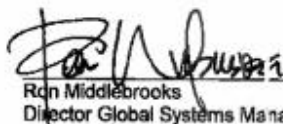
[REDACTED]

[REDACTED]

Mitigating Factors:

[REDACTED]

As the Executive Sponsor for SV, I acknowledge the application is not in compliance with Postal security policy as stated in the AS-805, and accept all security risks involved in operating SV and authorize it to remain in the production environment, effective 10-11-2007.


Ron Middlebrooks
Director Global Systems Management

12/7/07
Date

I approve this exception to policy in IT Security Handbook, AS-805 section 9.7-10 Authentication Requirements


George W. Wright
Acting Vice President, Chief Technology

12/13/2007
Date

- cc: Harold E. "Pete" Stark, Manager, Corporate Information Security
- Mark A. Mittelman, Manager, Sales & Marketing Portfolio
- John T. Edgar, Manager, Network Operations Portfolio
- Mark J. Stepongzi, Program Manager Information Technology, CISO
- Phillip R. Nicholson, Information Systems Security Specialist, CISO
- Gregory N. Dudley, Program Manager Network Operation Portfolio
- Frances A. Byrd, Program Manager Sales & Marketing Portfolio