



August 6, 2007

ROBERT L. OTTO
VICE PRESIDENT, CHIEF TECHNOLOGY OFFICER

SUBJECT: Management Advisory – State of Information Technology Within the
Postal Service (Report Number IS-MA-07-001)

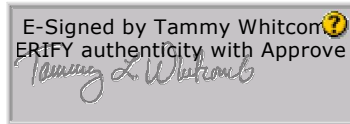
This report presents the results of our review of the state of information technology (IT) within the U.S. Postal Service (Project Number 07BG004IS000). We initiated this review to assess the progress the Chief Technology Office (CTO) has made with the Postal Service's IT program. The Postal Service presented three strategies for its IT program in its 2002 *Transformation Plan*.

Overall, CTO management has made notable progress towards enhancing the Postal Service's information security program, upgrading its computing infrastructure, and achieving universal computing connectivity. We conducted 75 audits and assessments of the IT program from October 2003 through June 2007. Overall, our audits showed that the IT program is well-managed and supports overarching Postal Service needs. When these audits noted opportunities where the Postal Service could make improvements in its IT program, management undertook initiatives to address these issues. Consequently, we believe the Postal Service's information resources provide an adequate level of security, reliability, and value.

The U.S. Postal Service Office of Inspector General (OIG) works closely with management in identifying potential audits and program oversight activities. This includes Value Proposition Agreements for special audit work suggested by CTO management. For example, our work on the Human Capital Enterprise SAP system and the Payment Switch development projects assessed those efforts during their development cycles and identified potential concerns, which management promptly addressed. These and other audits assisted IT project sponsors in deploying, securing, and managing emerging technologies and implementing corrective actions during development.

OIG's partnership with the CTO organization leverages management resources by extending oversight to the widest possible corporate view. These joint efforts assist corporate managers in being proactive agents of transformational change in increasing productivity and reducing support costs while ensuring continuity of critical operations.

This report contains no recommendations. Management agreed with the facts as presented in the report and their comments are included in the report. We appreciate the cooperation and courtesies provided by your staff during the review. If you have any questions or need additional information, please contact Gary Rippie, Director, Information Systems, or me at (703) 248-2100.



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

Attachments

cc: H. Glen Walker
Harold E. Stark
Joseph J. Gabris
G. Dean. Larrabee

INTRODUCTION

Background

The scope of information technology (IT) within the U.S. Postal Service involves the third largest technology infrastructure¹ in the world. The Vice President, Chief Technology Officer, leads the Postal Service's IT activities. The Chief Technology Office's (CTO) mission is to develop, implement, and maintain cost-effective electronic communication, data, and automated solutions that support customer, corporate, business, and security needs.

In support of that mission, CTO management:

- Maintains an eBusiness systems infrastructure that supports gross sales of over \$270 million annually.
- Supports nearly 700,000 employees.
- Controls the technology supporting about 650 applications for day-to-day Postal Service business, including payroll for its 700,000 employees.
- Manages the world's largest intranet.
- Runs the systems that connect processing centers and about 38,000 post offices nationwide.
- Processes over 14 million emails per day.

To safeguard the Postal Service's infrastructure and data, CTO management employs a defense-in-depth model. (See Figure 1.)

¹ Infrastructure includes hardware, applications, service, and support.

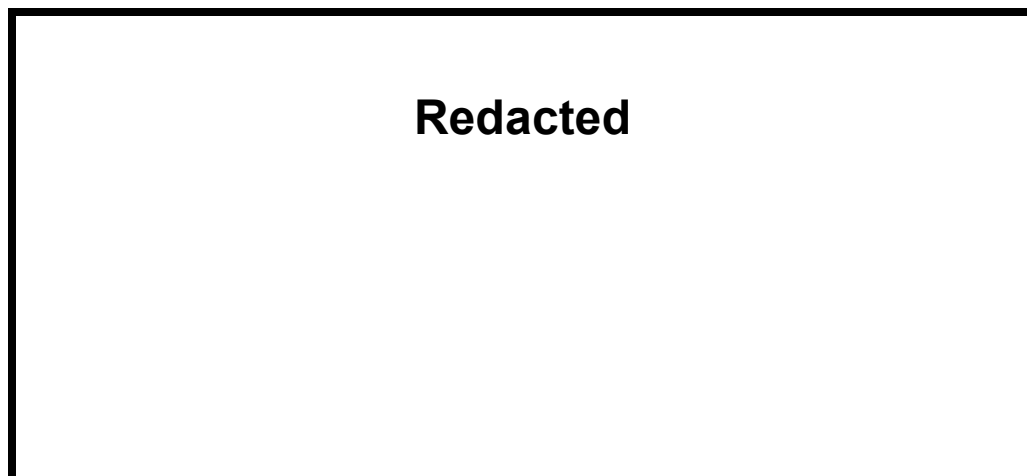


Figure 1. Defense-in-Depth Model

This model:

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

In April 2002, the Postal Service submitted to the President and Congress a *Transformation Plan*³ analyzing both the challenges facing the Postal Service and its future. The Postal Service defined strategies it was pursuing to meet its commitment to its customers to increase the value of its products and services, improve operational

² [REDACTED]

³ The *Transformation Plan* has served as the blueprint for every aspect of Postal Service business.

efficiency, and foster a performance-based culture. For IT, these strategies are:

- Enhanced security
- Upgraded infrastructure
- Universal computing connectivity

In developing its annual audit plan, the U.S. Postal Service Office of Inspector General (OIG) coordinates with CTO management to ensure that management priorities are included in our proposed work plans. For example, we have used Value Proposition Agreements to address specific audit objectives and deliverables for the Payment Switch and the SAP Human Capital Enterprise initiatives, and vulnerability assessments of legacy mainframe systems.

Objective, Scope, and Methodology

The objective of our review was to assess the progress CTO management has made with the Postal Service's IT program. To assess the progress of the Postal Service's IT program, we reviewed IT strategies delineated in the Postal Service's 2002 *Transformation Plan*. We used the overall objective of each strategy as the foundation against which to assess progress in implementing each strategy. We reviewed accomplishments CTO management reported and results we published in information systems audit reports from fiscal year (FY) 2004 to the present. In addition, we interviewed various CTO management and staff.

We conducted this review from December 2006 through August 2007 in accordance with the President's Council on Integrity and Efficiency, *Quality Standards for Inspections*. We discussed our observations and conclusions with management officials on May 21, 2007, and included their comments where appropriate.

Prior Audit Coverage

The OIG completed numerous audits and security assessments from October 2003 through July 2007 regarding IT resources under the Vice President, Chief Technology Officer's purview. These included audits that address computing and network infrastructure security within the Postal Service. We identify each specific audit report and the area it addresses in Appendix A.

RESULTS

Overall, CTO management has made notable progress towards enhancing the Postal Service's information security program, upgrading its computing infrastructure, and achieving universal computing connectivity. We conducted 75 audits and assessments of the IT program from October 2003 through June 2007. Overall, our audits showed that the IT program is well-managed and supports overarching Postal Service needs. When these audits noted opportunities where the Postal Service could make improvements in its IT program, management undertook initiatives to address these issues. Consequently, we believe the Postal Service's information resources provide an adequate level of security, reliability, and value. Management's comments, in their entirety, are included in Appendix B of this report.

Enhanced Security

CTO management has made notable progress toward enhancing the Postal Service's information security program. CTO management has reported on achievements of the information security program as evidence of this progress. Most of the information security-related audits we conducted from the beginning of FY 2004 to the present demonstrate the overall adequacy of the Postal Service's information security program. In addition, our audits have helped enhance the program.

CTO management's overall strategy for enhancing the Postal Service's information security program is to avoid disruptions to critical operations and protect sensitive information from unauthorized disclosure or modification. The strategy aims to protect data entrusted to the Postal Service by contractors, business partners, and customers, to ensure the continuity of its business infrastructure, and to preserve the Postal Service's investment in technologies and information.

To achieve enhanced security, CTO management established goals and initiatives to address five categories: education and training, the certification process,

contingency planning, intrusion protection, and automated monitoring. Following are some of the information security program achievements⁴ CTO management has reported:

- Emphasized security awareness throughout the Postal Service via annual security awareness forums, numerous internal newsletter articles, and an “eLearning” website.
- Inventoried, classified, accredited, and certified 74 percent of the Postal Service’s national applications covered under the information security assurance process. CTO management indicated it is in the process of certifying an additional 13 percent of the applications.⁵
- [REDACTED]⁶
- Reorganized its disaster recovery methodology and established compliant recovery plans for 66 percent of critical Postal Service applications.⁷
- Established a certificate authority⁸ to enable access to government sites.

CTO management also reported it upgraded 100 percent of the Postal Service’s workstations and 95 percent of the servers to new intrusion detection software or other compensating controls and deployed intrusion prevention software to protect against viruses. Each month, the security software has enabled CTO management to:

⁴ Our reviews directly support most of these achievements or CTO management’s efforts toward these achievements.

⁵ [REDACTED]

⁸ A certificate authority is an authority in a network that issues and manages security credentials and public keys for message encryption and decryption.

- Scan more than 170 million internal and 13 million external e-mail messages for viruses.
- Block over 21,000 e-mail messages due to viruses and over 110,000 email messages due to content.
- Block more than 5 million attempts to access non-business or inappropriate websites and block, on average, 222 million external threats at the network perimeter.

Furthermore, CTO management implemented an initiative to secure sensitive corporate and personal data using encryption technology. This initiative should help mitigate the Postal Service's risk of losing sensitive customer or employee personal data that has recently plagued other federal agencies.

Sixty-nine of the 75 audits and assessments we conducted from the beginning of FY 2004 to the present addressed the Postal Service's information security program. (See Appendix A.) During most of these audits, we identified areas where the Postal Service could further strengthen its security program. The Postal Service planned or took corrective action to address these areas. For example, we determined:

- In April 2005, the Postal Service had made progress in completing activities in each of the five *Transformation Plan* information security categories. In addition, the Postal Service's information security program addressed the key recommended elements promulgated by federal guidelines and met the criteria to be categorized as successful as measured by specifications outlined in the President's Management Agenda.⁹
- During its certification and accreditation process in FY 2006, the Postal Service did not complete certain information security assurance processes and related documentation for some production applications. During our audit, the Postal Service completed the

⁹ The President's Management Agenda — announced in 2001 — is an aggressive strategy for improving the management of the federal government. It focuses on key areas of management weakness across the government.

appropriate missing documentation.

- [REDACTED]
- [REDACTED]
- The Postal Service provided adequate security and control over the configuration and use of key mainframe and mid-range software. However:
 - [REDACTED]
 - [REDACTED]
- [REDACTED]




CTO management's sustained efforts to enhance security and our ongoing security audits should help ensure the continuity of critical Postal Service operations and protect sensitive information from unauthorized disclosure or modification.

Upgraded Infrastructure

CTO management has made substantial progress in upgrading the Postal Service's computing infrastructure. CTO management has reported on achievements that highlight this progress. In addition, several Postal Service initiatives we reviewed from the beginning of FY 2004 to the present support this progress.

To upgrade the Postal Service's infrastructure, CTO management's strategy is to leverage technological advances and business partnerships to support current and new business requirements. To pursue this strategy, CTO management established goals and initiatives to address upgraded distributed, mainframe, and mid-range computing infrastructures; technical shared services; and corporate shared services. To highlight progress, CTO management reported it has:

- ¹⁰
¹¹
:
- 

¹⁰¹¹

- Remove about 12,400 servers from over 11,000 field sites and replace them with less than 1,300 servers at fewer than 600 field sites.
- [REDACTED]
- [REDACTED].
- [REDACTED]¹²
[REDACTED]¹³
- Replaced mainframe laser printers with faster, more reliable high-speed laser printers.
- Replaced Check and Earnings Statement Mailing equipment for faster dispatch of checks and earnings statements.
- [REDACTED]¹⁴.

From the beginning of FY 2004 to the present, 55 of the 75 audits we conducted involved the Postal Service's computing infrastructure. (See Appendix A.) Following are examples of audits we conducted on initiatives that support the progress CTO management has made toward achieving its upgraded computing infrastructure objectives:

- We produced two reports on the Postal Service's Payment Switch Solution implementation in conjunction with an October 2005 Value Proposition Agreement between the OIG, the CTO, and the Treasurer. This solution supports a broad range of

¹²¹³¹⁴

electronic payment types to provide the Postal Service with an integrated and more efficient payment solution. We identified areas for improvement to further enhance the security of the system and prepare it for compliance with Payment Card Industry requirements. Management agreed with 12 of our 13 recommendations and has planned or completed actions to address our concerns.

- We reviewed the Postal Service's Automated Postal Centers (APC), which are self-service kiosks that offer customers a broad range of products, services, and information through a smart vending platform that is available 24 hours a day, 7 days a week.¹⁵ We identified a number of areas where management could improve security over the APC kiosks and servers. Management agreed with our recommendations and had initiatives in progress or planned to address our issues.
- We conducted two audits involving the Facilities Database (FDB). The Postal Service established the FDB to serve as the single corporate-wide source for facilities-related information to meet the needs of the Postal Service and its customers. During our review the Postal Service significantly decreased the number of data discrepancies within the FDB. We determined management could make additional improvements in the timeliness, completeness, and accuracy of FDB data. Management agreed with our recommendations and had initiatives in progress and corrective actions planned to address our issues.
- We reviewed the mainframe service continuity controls at the Egan, Minnesota, and San Mateo, California IT/ASCs. During FY 2006, management made a significant investment in new technology to purchase and upgrade mainframe equipment (including the purchase of faster mainframe processors and mainframe data storage equipment) and to make upgrades to the mainframe operating system. We also determined the Postal Service

¹⁵ [REDACTED]

needed to complete testing of mainframe disaster recovery equipment at the San Mateo and Eagan IT/ASCs. Management agreed with our recommendation and completed testing of the mainframe equipment.

Continued infrastructure improvements by CTO management should help the Postal Service's efforts to increase revenue, efficiency and productivity, and reduce support costs.

Universal Computing Connectivity

CTO management has made noteworthy progress towards achieving universal computing connectivity (network connectivity) within its network infrastructure. CTO management has reported accomplishments that illustrate the progress toward network connectivity objectives. In addition, some of our audits support and have contributed to efforts CTO management has made toward achieving these objectives.

CTO management's strategy for network connectivity is to expand its network infrastructure (for example, the core/backbone, wide area network, and local area networks) to provide:

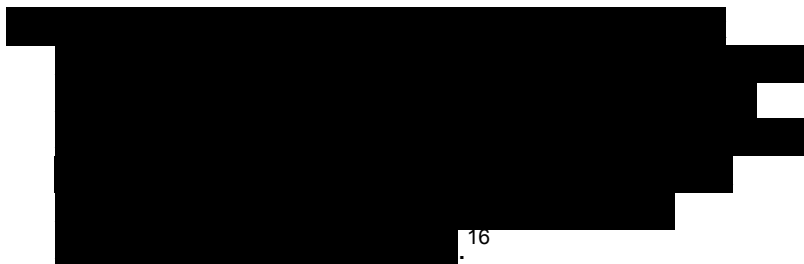
- A means of reducing the Postal Service's operational, training, travel, and other expenses by leveraging the network.
- A highly reliable and secure network — for voice, data, and video transmissions — available 24 hours a day, 7 days a week.

To achieve these objectives, the Postal Service established network connectivity goals and initiatives for a consolidated voice, data, and video network; and wireless technology solutions. Despite having to forgo one of its key initiatives under this strategy — the Universal Computing Connectivity contract — the Postal Service reported the following steps taken toward achieving universal computing connectivity:

- Transitioned critical sites to the Postal Service's high-speed data connections.

- Upgraded bandwidth to 384 kilobits per second at over 19,000 sites.
- Installed 2,650 access points on wireless local area networks at 166 sites.
- Increased BlackBerryTM deployment to 6,400 users, including Continuity of Operations team members. The BlackBerry service includes eApprover, eBuy, eTravel, and eAccess functionality. In addition, the BlackBerry provides the capability to erase data on the device if it is lost.

Thirteen of the 75 audits we conducted from the beginning of FY 2004 to the present addressed the Postal Service's network infrastructure-related objectives. (See Appendix A.) For example:



We performed several audits which identified opportunities to capture savings by eliminating unnecessary telecommunications services and devices such as telephone lines, cellular phones, BlackBerry devices, pagers, and cellular broadband cards, with a total projected cost savings of \$17.2 million. Because of our audit work and collaborative relationship, the Postal Service proactively terminated other unnecessary telephone lines, resulting in an additional cost savings of \$721,000. Furthermore, in October 2006, the Postal Service reported estimated annual savings of \$5.7 million as a result of our national voice audit. Recently, management stated it has eliminated inactive cellular devices resulting in savings of over \$100,000 per month.

As CTO management continues to pursue its network connectivity strategy, the Postal Service will be better able to take full operational advantage of its high-speed network. Maintaining and monitoring a modern information systems environment according to sound system administration practices can assist in protecting the confidentiality, integrity, and availability of corporate and customer data.

**The Future of
Information
Technology at the
Postal Service**

In its *Strategic Transformation Plan 2006–2010*, the Postal Service commits to making further advances in service, productivity, and employee engagement. To optimize its IT infrastructure, the Postal Service established the following goals:

- Accelerate centralization of technology functions and realign IT support functions in the field.
- Reduce the use of high-cost IT contractors by transitioning knowledge to career employees.
- Expand the capabilities of the existing Enterprise Data Warehouse to allow full cross-functional analysis and decision-making by 2008.
- Standardize printers, scanners, photocopiers, and other equipment.

In addition, over the next 3 years, IT will play a key role in ensuring the Postal Service is able to meet the financial management goals of the Sarbanes-Oxley (SOX) Act.¹⁷ CTO management has already started some major efforts that will support the Postal Service's move toward compliance. Specifically, CTO management:

- Created the SOX/Postal Reform Portfolio responsible for overseeing all technology issues related to SOX and other postal reform matters.

¹⁷ The Postal Accountability and Enhancement Act requires the Postal Service to comply with the SOX Act. By 2010, the Postal Service must be fully compliant with SOX, which means it must establish controls and testing for financial reporting, as well as report any changes in financial conditions or operations.

- Initiated efforts to assess the Postal Service's current systems and make any necessary upgrades to bring them in line with SOX requirements for documentation and reporting.

As the Postal Service continues to pursue improvements in its IT program, the OIG will continue to work closely with CTO management to assess appropriate elements of the program.

APPENDIX A. PRIOR AUDIT COVERAGE

October 2003 through June 2007

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-04-001	<i>FY 2003 Information Systems Controls, Eagan, San Mateo, and St. Louis Information Technology and Accounting Service Centers</i>	12/2/03	X	X	
IS-AR-04-002	<i>Advanced Computing Environment – Vulnerability Assessment</i>	1/6/04	X	X	
IS-AR-04-003	<i>Controls Over Wireless Communications Within the Postal Service</i>	1/13/04	X		X
IS-AR-04-004	<i>Information Systems Disaster Recovery Process</i>	3/10/04	X		
IS-CS-04-002	<i>Security Vulnerability Assessment at the Host Computing Services, San Mateo, California</i>	3/24/04	X	X	
IS-AR-04-005	<i>Online Payroll Application Access Controls</i>	3/31/04	X	X	
IS-CS-04-003	<i>Security Vulnerability Assessment of Selected Windows Servers at the Host Computing Services, Eagan, Minnesota</i>	5/21/04	X	X	X
IS-AR-04-006	<i>Follow-up of the Network Security and Security Testing of Load Balancers at the San Mateo Host Computing Services</i>	6/8/04	X	X	
IS-AR-04-007	<i>Postal Service's Advanced Computing Environment Program Management</i>	6/16/04	X	X	
IS-CS-04-004	<i>Oracle Database Testing at the Host Computing Services, Eagan, Minnesota</i>	6/16/04	X	X	

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-04-008	<i>Audit of Serena ChangeMan ZMF Implementation</i>	6/17/04		X	
IS-AR-04-009	<i>Computer Incident Detection and Response Capabilities</i>	6/18/04	X		
IS-CS-04-005	<i>Security Vulnerability Assessment of Selected UNIX Servers at Host Computing Services, Eagan, Minnesota</i>	7/12/04	X	X	X
IS-AR-04-010	<i>Business Continuity Planning and Testing at the Eagan, San Mateo, and St. Louis Information Technology and Accounting Service Centers</i>	7/14/04	X		
IS-AR-04-011	<i>Personnel Security Controls at the Eagan, San Mateo, and St. Louis Information Technology and Accounting Service Centers</i>	9/8/04	X		
IS-AR-04-012	<i>Click-N-Ship Application Controls Review – Access to Nonproduction Systems</i>	9/28/04	X	X	
IS-AR-04-013	<i>Electronic Data Interchange at the San Mateo Information Technology and Accounting Service Center</i>	9/29/04	X	X	
IS-AR-04-014	<i>Postal Service's Business Partner Connectivity</i>	9/30/04	X		
IS-AR-05-001	<i>Reports Distribution</i>	10/25/04		X	

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-05-002	<i>Oracle Security Environment at the Eagan and San Mateo Information Technology and Accounting Service Centers</i>	11/10/04	X	X	
IS-AR-05-003	<i>Windows Server Security at the Eagan, Minnesota, and San Mateo, California, Information Technology and Accounting Service Centers</i>	11/17/04	X	X	
IS-CS-05-001	<i>Security Assessment (PhoneSweep) of PBX Site Event Buffers</i>	12/8/04	X		X
IS-CS-05-002	<i>Click-N-Ship Security Vulnerability Assessment</i>	1/13/05	X	X	X
IS-AR-05-004	<i>FY 2004 Information Systems Controls Capping Report</i>	1/28/05	X	X	
IS-AR-05-005	<i>Click-N-Ship Applications Control Review</i>	2/22/05	X	X	
IS-AR-05-006	<i>Postal Service's Business Partner Connectivity-Firewall Permissions</i>	3/24/05	X		
IS-AR-05-007	<i>Security Controls in Voice Systems</i>	4/18/05	X		
IS-MA-05-001	<i>Information Security Program</i>	4/25/05	X		
IS-AR-05-008	<i>Integrated Database Management System Controls at the Eagan, Minnesota Information Technology and Accounting Service Center</i>	5/12/05	X	X	
IS-CS-05-003	<i>Security Vulnerability Assessment of the Advanced Computing Environment Phase II</i>	5/20/05	X	X	

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-05-009	<i>Software Monitor Controls at the Eagan, Minnesota, and San Mateo, California Information Technology and Accounting Service Centers</i>	5/31/05	X	X	
IS-AR-05-010	<i>Security Assessment Summary Report</i>	6/3/05	X	X	
IS-AR-05-012	<i>Physical Security Controls at the Eagan, Minnesota; San Mateo, California; and St. Louis, Missouri Information Technology and Accounting Service Centers</i>	6/12/05	X		
IS-AR-05-011	<i>Assessment of Patch Management Practices</i>	6/30/05	X	X	
IS-AR-05-013	<i>Mainframe and Midrange Software Controls at the Eagan, Minnesota and San Mateo, California Information Technology and Accounting Service Centers</i>	8/17/05	X	X	
IS-AR-05-014	<i>CA-ACF2 Controls at the Eagan, Minnesota, and San Mateo, California Information Technology and Accounting Service Centers</i>	8/17/05	X	X	
IS-CS-05-004	<i>Security Vulnerability Assessment of Selected Financial Systems at the Host Computing Services Eagan, Minnesota</i>	8/17/05	X	X	
IS-AR-05-015	<i>Human Capital Enterprise SAP Human Resources Project</i>	9/15/05	X	X	
IS-CS-05-005	<i>Security Vulnerability Assessment of Automated Postal Centers</i>	9/23/05	X	X	X

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-06-001	<i>Data Communications Software Controls at the Eagan, Minnesota and San Mateo, California Information Technology and Accounting Service Centers</i>	10/19/05	X	X	
IS-MA-06-001	<i>Security Over Sensitive Customer Data on Automated Postal Center Kiosks</i>	12/23/05	X	X	
IS-AR-06-003	<i>Security Vulnerability Assessment and Audit of Automated Postal Center Systems</i>	2/10/06	X	X	
IS-CS-06-001	<i>Security Vulnerability Assessment at the Engineering Research and Development Center, Merrifield, Virginia</i>	2/10/06	X	X	X
IS-AR-06-002	<i>Controls Over Sensitive Production Data Within the Test Environment for the Human Capital Enterprise SAP Human Resources Project</i>	2/13/06	X	X	
IS-AR-06-004	<i>Fiscal Year 2005 Information Systems General Controls Capping Report</i>	3/6/06	X	X	
IS-AR-06-006	<i>Data Input Validation for the Facilities Database</i>	3/30/06		X	
IS-AR-06-007	<i>Observation of the Certificate Authority-Public Key Infrastructure External Environment at the Eagan, Minnesota Information Technology and Accounting Service Center</i>	3/31/06	X	X	

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-06-008	<i>Human Capital Enterprise SAP Human Resources Project – System Controls Over Roles and Separation of Duties</i>	5/2/06	X	X	
IS-AR-06-009	<i>Information Security Assurance Process</i>	5/4/06	X		
IS-AR-06-011	<i>Router and Switch Controls at Selected Postal Service Information Technology Centers</i>	5/25/06	X		X
IS-AR-06-012	<i>Status of Follow-up Audit of Certificate Authority Public Key Infrastructure Compliance</i>	6/8/06	X	X	
IS-CS-06-002	<i>Security Assessment Audit of Telephone Lines and Modems (PhoneSweep) at Eagan, Minnesota Host Computing Services</i>	6/9/06	X		X
IS-AR-06-013	<i>Change of Address – Application Control Review</i>	7/17/06	X	X	
IS-AR-06-014	<i>Information System Policy and Procedure Controls</i>	8/14/06	X	X	
IS-CS-06-003	<i>Security Assessment Audit of Telephone Lines and Modems (PhoneSweep) at San Mateo, California Host Computing Services</i>	8/18/06	X		X
IS-CS-06-004	<i>Security Vulnerability Assessment of Legacy Applications at the Eagan Host Computing Services, Eagan, Minnesota</i>	8/30/06	X	X	

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-06-015	<i>Certificate Authority Public Key Infrastructure Compliance at the Information Technology and Accounting Service Center in Eagan, Minnesota</i>	9/1/06	X	X	
IS-AR-06-016	<i>System Software Controls at the Eagan, Minnesota and San Mateo, California Information Technology and Accounting Service Centers</i>	9/11/06	X	X	
IS-AR-06-017	<i>Enterprise Payment Switch Solution Phase 1: Requirements and Design</i>	9/27/06	X	X	
IS-AR-06-018	<i>Information System Access Controls at the Eagan, Minnesota, and San Mateo, California Information Technology and Accounting Service Centers</i>	9/27/06	X	X	
IS-WP-07-001	<i>Information for the Federal Bridge Certification Authority</i>	10/2/06	X	X	
IS-AR-07-001	<i>Human Capital Enterprise SAP Change Management Process</i>	10/18/06	X	X	
IS-CS-07-001	<i>Security Assessment Audit of Telephone Lines and Modems (PhoneSweep) at the International Business Operations Center in Jamaica, New York</i>	10/30/06	X		X

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-07-002	<i>Mainframe Service Continuity Planning and Testing at the Eagan, Minnesota, and San Mateo, California Information Technology and Accounting Service Centers</i>	11/16/06	X	X	
IS-AR-07-003	<i>Security Vulnerability Assessment of Legacy Applications at the Eagan Host Computing Services, Eagan, Minnesota</i>	12/7/06	X	X	
IS-AR-07-004	<i>Physical Security Controls at the Eagan, Minnesota; San Mateo, California; and St. Louis, Missouri Information Technology and Accounting Service Centers</i>	12/19/06	X		
IS-AR-07-005	<i>Data Integrity Review of Address Management System Facility Data</i>	12/22/06		X	
IS-AR-07-006	<i>National Customer Management System Encryption</i>	12/26/06	X	X	
IS-CS-07-002	<i>Security Vulnerability Assessment of Selected Servers and Databases That Support the Change of Address Program</i>	1/4/07	X	X	
IS-AR-07-007	<i>Enterprise Payment Switch Solution Phase II: Preparations for Security Testing</i>	2/23/07	X	X	
IS-AR-07-008	<i>The Postal Service's Efforts to Protect Sensitive Information</i>	2/26/07	X		

Report Number	Report Title	Issue Date	Program Area		
			Information Security	Computing Infrastructure	Network Infrastructure
IS-AR-07-009	<i>Fiscal Year 2006 Information Systems General Controls Capping Report</i>	2/26/07	X	X	
IS-AR-07-010	<i>Audit of Cellular Services</i>	3/29/07			X
IS-AR-07-011	<i>Headquarters Cellular Services</i>	3/30/07			X
IS-CS-07-003	<i>Security Vulnerability Assessment of the Servers and Databases Supporting the Postal Automated Redirection System</i>	5/14/07	X	X	
Total Reports: 75			69	55	13

APPENDIX B. MANAGEMENT'S COMMENTS

ROBERT L. OTTO
VICE PRESIDENT
CHIEF TECHNOLOGY OFFICER



July 27, 2007

KIM STROUD

SUBJECT: Draft Management Advisory – State of Information Technology within the Postal Service (Report Number IS-AR-07-DRAFT)

This provides Postal management's response to the subject audit report. We appreciate the opportunity to review and provide comments on this report. We are in agreement with the facts presented in the report as written, and as discussed in our exit conference. We look forward to the issuance of your "good news" final report.

The subject audit report contains information relating to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the Postal Service. Therefore, this information should be classified as restricted and exempted from disclosure under the Freedom of Information Act.

If you have any questions regarding our response and would like to discuss them further, please contact Paul Caiazzo at 202-268-3305.

A handwritten signature in black ink, appearing to read "Robert L. Otto".

Robert L. Otto

cc: H. Glen Walker
Joe Gabris
Jerry Reynolds
Norm Ringgold
Keith Kowitz
Pete Stark

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