OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 14, 2008

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

SUBJECT: Audit Report – Application Control Review of the Time and Attendance Collection System (Report Number IS-AR-08-014)

This report presents the results of our self-initiated audit of the Time and Attendance Collection System (TACS) (Project Number 07RG010IS000). Our objective was to determine whether TACS had sufficient controls in place to ensure that data and transactions are valid, authorized, and completely and accurately processed. Specifically, we reviewed controls surrounding input and approval of time records, user privileges, user authentication, and data integrity. In addition, we evaluated the reliability of reporting, specifically the Employee Everything Report. This audit addresses operational risk associated with TACS. Click here to go to Appendix A for additional information about this audit.

Conclusion

We determined TACS has sufficient application controls in place to ensure automated clock rings entered into the application were accurately accepted and processed. Also, we determined the Employee Everything Report and related interface were operating as intended and accurately reported transaction results. However, the U. S. Postal Service has an opportunity to strengthen least privilege controls, access controls, and security of sensitive information; and to improve Quality Assurance (QA) testing. The scope of our audit did not include a review of manual controls and supervisory responsibilities related to clock rings.

Electronic Badge Reader Creation Software and Printer

Employee Social Security numbers (SSN) can be displayed through some TACS application modules or printed on some TACS reports. The Postal Service took the initiative to protect employees' confidential and sensitive information, as directed in policy,[1] by using Employee Identification Numbers (EIN) for identification purposes instead of SSNs. However, management had not updated the Electronic Badge Reader (EBR) creation software to use these EINs as the primary means of identification.[2] [redacted]

Click here to go to Appendix B for our detailed analysis of this topic.

During the course of our audit, the Postal Service took action to begin eliminating the presentation of sensitive data. A change to the EBR creation software allows for the sensitive information to be replaced by other data.[3]

We recommend the Vice President, Information Technology Operations, coordinate with the Vice President, Controller, to:

1. Ensure management protects sensitive employee data used in the Electronic Badge Reader Program by eliminating the presentation of confidential Social Security numbers on computer screens and hardcopy reports by either obscuring the data or replacing it with other non-sensitive data identifiers.

Privileged Database Accounts

[redacted] [4] [redacted] [5] [redacted]

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

2. Assign privileged system and administration accounts to unique individuals.

[1] Handbook AS-805, *Information Security*, dated March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006), Section 3-5.2.

[2] [redacted]

[3] [redacted]

[4] [redacted]

[5] Handbook AS-805, *Information Security*, Section 9-5.3.2.

3. Ensure privileged account passwords are not shared and password renewal practices comply with Postal Service policy.

Encryption of Sensitive Information

[redacted][6] [redacted].[7] [redacted]

We recommend the Vice President, Information Technology Operations, direct the Manager, Finance Business Systems Portfolio, to:

4. Encrypt sensitive Time and Attendance Collection System data being stored in application files.

Time and Attendance Collection System Testing Environment

The TACS QA testing environment does not mirror the production environment and personnel cannot completely test all modifications with absolute assurance. Best practices and Postal Service policy recommend ensuring test environments are representative of the production operating environment and changes to the production environment are replicated in the test environment.[8] As changes to the production environment occurred, the Postal Service did not replicate them in the QA testing environment. A QA testing environment which mirrors production helps ensure changes will be adequately tested before being introduced into the production environment. Click here to go to Appendix B for our detailed analysis of this topic.

We recommend the Vice President, Information Technology Operations, direct the Manager, Finance Business Systems Portfolio, to:

5. Update the Quality Assurance testing environment to mirror the production environment.

[6] Handbook AS-805, Section 9-8.2.

[7] [redacted]

[8] Information Systems Audit and Control Association's *COBIT AI7.4 Test Environment,* IT Governance Institute, 2007, and U.S. Postal Service *Development and Operations Security Policy*, Section 5, (not dated).

Access to Production Database

Three Postal Service TACS developers had both read-only access to the TACS databases and unrestricted access privileges at the TACS business application level. Having both business user and database accounts allows developers to have inherited (accumulated) rights,[9] which put confidential and sensitive data at unnecessary risk. Postal Service policy[10] states that developers must not have access to production application systems. Management approved developer access to production application systems, as well as unrestricted read-only access to production databases, in order to expedite the handling of TACS change requests. Click here to go to Appendix B for our detailed analysis of this topic.

During the course of our audit, the Postal Service implemented changes to restrict developers to read-only access to production databases for application support. All access capabilities granting write, update and delete privileges were removed. Therefore, we are not making any recommendations to address this issue.

Sensitive Information Available to Users

[redacted]. Postal Service policy[11] states management must protect sensitive information from unauthorized access and disclosure and restrict access to authorized personnel with a need to know. [redacted].[12] This resulted in TACS users being able to obtain confidential and sensitive employee personal information.

During the course of our audit, the Postal Service made appropriate changes ensuring displayed employee SSNs were protected [redacted] Therefore, we are not providing recommendations for this issue.

Management's Comments

Management agreed with recommendations 1, 2, 4, and 5 and partially agreed with recommendation 3. Regarding recommendation 1, management changed the TACS badge card report to eliminate display of the SSNs. Management also will direct a [redacted]

[9] Coupled with their business accounts, which grant read, write, update, and delete privileges, developers can access databases with these assumed privileges and their actions will not be tracked based on their approved access to the databases.

[10] Handbook AS-805, Section 8-3, and U.S. Postal Service's *Development and Operations Security Policy*, Section 5.

[11] See footnote 1.

[12] When [redacted]

For recommendation 2, management stated the [redacted] team will develop processes to migrate from using shared privileged accounts to unique individual accounts by January 30, 2009.

Concerning the partial agreement with recommendation 3, management stated it is [redacted]. However, management stated they would use a software tool as a compensating control to monitor use of these accounts and to record an audit trail of activity. Management agreed with the password renewal compliance and stated that [redacted] would implement the renewal policy on TACS and all other databases. Management will research the marketplace and provide a recommended solution by December 30, 2008, for a software tool to manage the change of a large numbers of passwords at a time.

[redacted]

Finally, for recommendation 5, management stated they are investigating and designing the TACS test environment architecture as part of an initiative to become compliant with Sarbanes-Oxley. They will complete this effort by September 30, 2009. Management's comments, in their entirety, are included in Appendix C.

Evaluation of Management's Comments

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

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Gary C. Rippie, 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
Lynn Malcolm
Harold E. Stark
Joseph J. Gabris
Jo Ann E. Mitchell
Carol A Reich
David M. Stauffer
William E. Koetz
Christine L. Souter
Kathleen A. Warnaar
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

TACS is one of the largest Postal Service web-based applications providing real-time work hour data to help manage day-to-day operations. TACS accounts for the work hours of more than 650,000 Postal Service career and non-career employees and nearly $2 billion in salaries and benefits employees receive each pay period. TACS ensures all employees are paid by a uniform set of rules at a national level and eliminates differences in how payroll information is calculated for T&A. Employees' time can be entered into TACS in three different ways.

- Electronic Badge Reader – Employees swipe their badges at the beginning and end of their tours and when leaving for or returning from their designated lunch periods, generating a clock ring. Supervisors manually input all employee leave. These clock rings are written to the TACS database and are automatically accepted by TACS.

- Timecards – Employees record their time on a timecard, which may be entered in one of two ways: (1) an employee's supervisor logs on to the TACS application and enters timecard data into the Timecard Entry Module, or (2) a supervisor will call an 800 telephone number to establish a connection with TACS Voice Response[13] (TVR) and use a typical telephone numeric touch pad to enter the employee's time into the TACS application.

- Auto-Rings – Exempt employees can be established in TACS on auto-rings. Under this option, the employee's schedule is pre-populated in the TACS application, requiring only that deviations from their schedule be manually entered into the application.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to determine whether TACS has sufficient controls in place to ensure that data and transactions are valid, authorized, and completely and accurately processed. Specifically, we reviewed controls surrounding input and approval of time records, user privileges, user authentication, and data integrity. In addition, we validated the reliability of reporting for the Employee Everything Report.[14]

We gathered documentation and interviewed Postal Service personnel to identify and assess existing application controls in the TACS application. We limited our scope to the actual clock rings as entered into the application. Our audit did not include tests to determine that the information captured by the clock rings was accurate.

[13] TVR is used at small offices which do not have Internet connection.

[14] Ernst and Young requested that we attest to the reliability of the Employee Everything Report for the purpose of placing reliance on the accuracy of this report for their audit of the Postal Service's financial statements.

We tested the input of clock rings into the Clock Ring Editor Module and the Timecard Entry Module of TACS. [redacted]. We created several testing scenarios based on business rules of the application. We performed some of these scenarios to create error outcomes, and some to create non-error outcomes. For example, based on business rules we would expect the application to produce an error if an employee's work hours exceeded the scheduled 40 hours per week and no overtime was authorized. After creating scenarios for both the Clock Ring Editor Module and Timecard Entry Module, we input the testing scenarios into TACS and analyzed our results.

We tested the reliability of the computer-generated output presented in the Employee Everything Report. After obtaining a sample of employees, we ran an Employee Everything Report for all hours processed and recorded by TACS. We queried the database and used scripts provided by the TACS development team to obtain the raw rings entered into the application and written to the database. We performed a line-by-line analysis of this data to verify that all information input into the application processed as expected.

We conducted this performance audit from June through November 2007 and March through August 2008[15] 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management officials on July 15, 2008, and included their comments where appropriate.

[15] We did not work on this audit from December 2007 through February 2008 due to the unavailability of resources.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date	Monetary Impact	Report Results
Internal Controls Over Operation Clock Rings at the Margaret L. Sellers Processing and Distribution Center	NO-AR-07-008	August 24, 2007	N/A	Internal controls ensuring the accuracy of clock rings were in place and generally effective. However, based on our statistical sample of 220 employees, 7 percent were clocked into the incorrect operation which could result in management making incorrect decisions about resource allocations and the productivity of individual operations. In addition, management could improve internal controls over timecard security.
Audit of Database Administration Practices	IS-AR-07-016	August 20, 2007	N/A	The Postal Service needs to strengthen controls and processes surrounding access controls, segregation of duties and database administration. Specifically, improvements are needed for controlling developers' access to production databases and for managing user accounts.

APPENDIX B: DETAILED ANALYSIS

Electronic Badge Reader Creation Software and Printer

System queries or reports often displayed or printed confidential SSN data. [redacted].[16] Employees swipe their badges at EBR stations and generate clock rings. These clock rings are written to the TACS database and made available to the TACS application. [redacted]. Postal Service policy[17] states sensitive information must be protected from unauthorized access and disclosure, restricting access to authorized personnel having a need to know. The elimination of this confidential data from the EBR program will prevent unauthorized personnel from viewing it in TACS reports.[18]

During the course of our audit, the Postal Service began eliminating the presentation of sensitive data. [redacted]

Privileged Database Accounts

[redacted][19] [redacted]. [redacted] operates 7 days a week, 24 hours a day, and some changes may need to be made during off hours when the primary DBA is not available. These changes result from change requests that are tracked in the remedy system. [redacted] personnel receive the remedy ticket and tested scripts from the developers and incorporate the changes into the application database using the shared privilege account and password.

These practices do not comply with Postal Service policy. [redacted][20] [redacted] Also, policy[21] states that passwords for privileged accounts must be changed at least every 30 days and as quickly as possible upon departure of a system or DBA to maintain the security and integrity of the system.

[16] [redacted]

[17] [redacted]

[18] [redacted]

[19] [redacted]

[20] Handbook AS-805, Section 9-5.3.2.

[21] Handbook AS-805, Section 9-7.1.6 and 6-7.3.

Encryption of Sensitive Information

[redacted][22] [redacted]

[redacted]

Time and Attendance Collection System Testing Environment

The QA testing environment does not mirror production. Specifically, there are program version and processing differences with infrastructure. The QA testing environment does not currently have an EBR to test changes before implementing them into production. Changes to the TACS application are tested using data manually input to a TACS application module whereas the majority of data in TACS is captured via EBR.

Best practices promoted by the Information Systems Audit and Control Association recommend ensuring that test environments are representative of the production operating environment and changes to the production environment be replicated in the test environment.[23] Postal Service policy states:

> *…the testing environment must be representative of the operating landscape, including likely workload stress, operating system, technology solution software, database management systems, and network/ computing infrastructure found in the production environment. As the production environment changes, the test environment must also change to stay in synchronization.*[24]

Access to Production Database

[redacted][25] [redacted]

[22] Handbook AS-805, Sections 9-8.2 and 3-5.5.2.
[23] Information Systems Audit and Control Association, *COBIT AI7.4 Test Environment.*
[24] U.S. Postal Service's *Development and Operations Security Policy*, Section 5.
[25] Handbook AS-805, *Services*, Section 8-3.

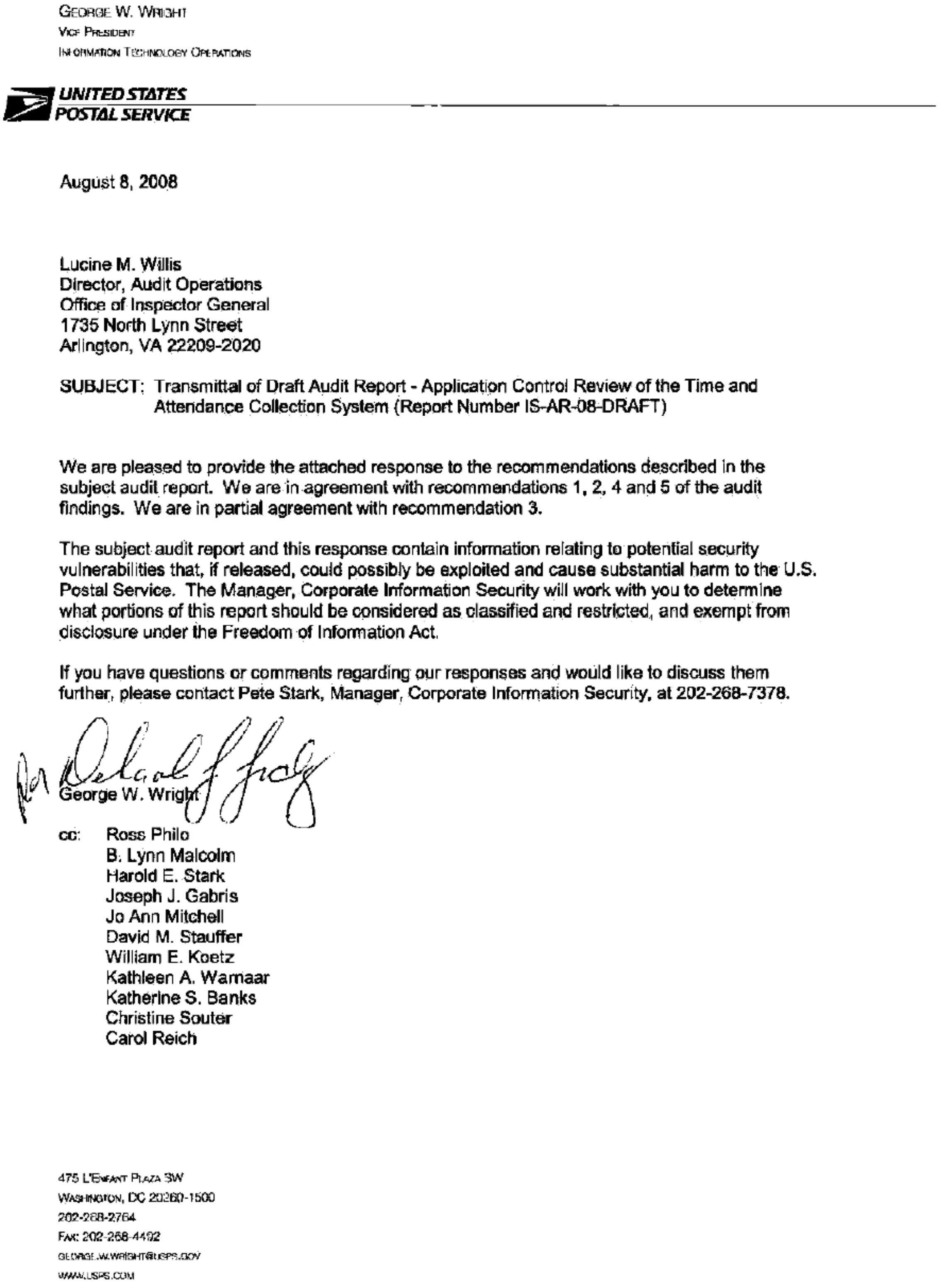
[redacted][26] [redacted].[27] [redacted]

During the course of our audit, the Postal Service implemented changes to ensure developers only have read-only access to production databases for application support. All access capabilities granting write, update and delete privileges were removed.

[26] Based on Handbook AS-805, Section 3-3.1, sensitivity determines the need to protect the confidentiality and integrity of the information. The three levels of sensitivity are (1) sensitive, (2) business-controlled sensitive, and (3) non-sensitive. Criticality reflects the need for continuous availability of the information. The three levels of criticality are (1) critical, (2) business-controlled critical, and (3) non-critical.

[27] [redacted]

APPENDIX C: MANAGEMENT'S COMMENTS



George W. Wright
Vice President
Information Technology Operations

UNITED STATES
POSTAL SERVICE

August 8, 2008

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

SUBJECT: Transmittal of Draft Audit Report - Application Control Review of the Time and Attendance Collection System (Report Number IS-AR-08-DRAFT)

We are pleased to provide the attached response to the recommendations described in the subject audit report. We are in agreement with recommendations 1, 2, 4 and 5 of the audit findings. We are in partial agreement with recommendation 3.

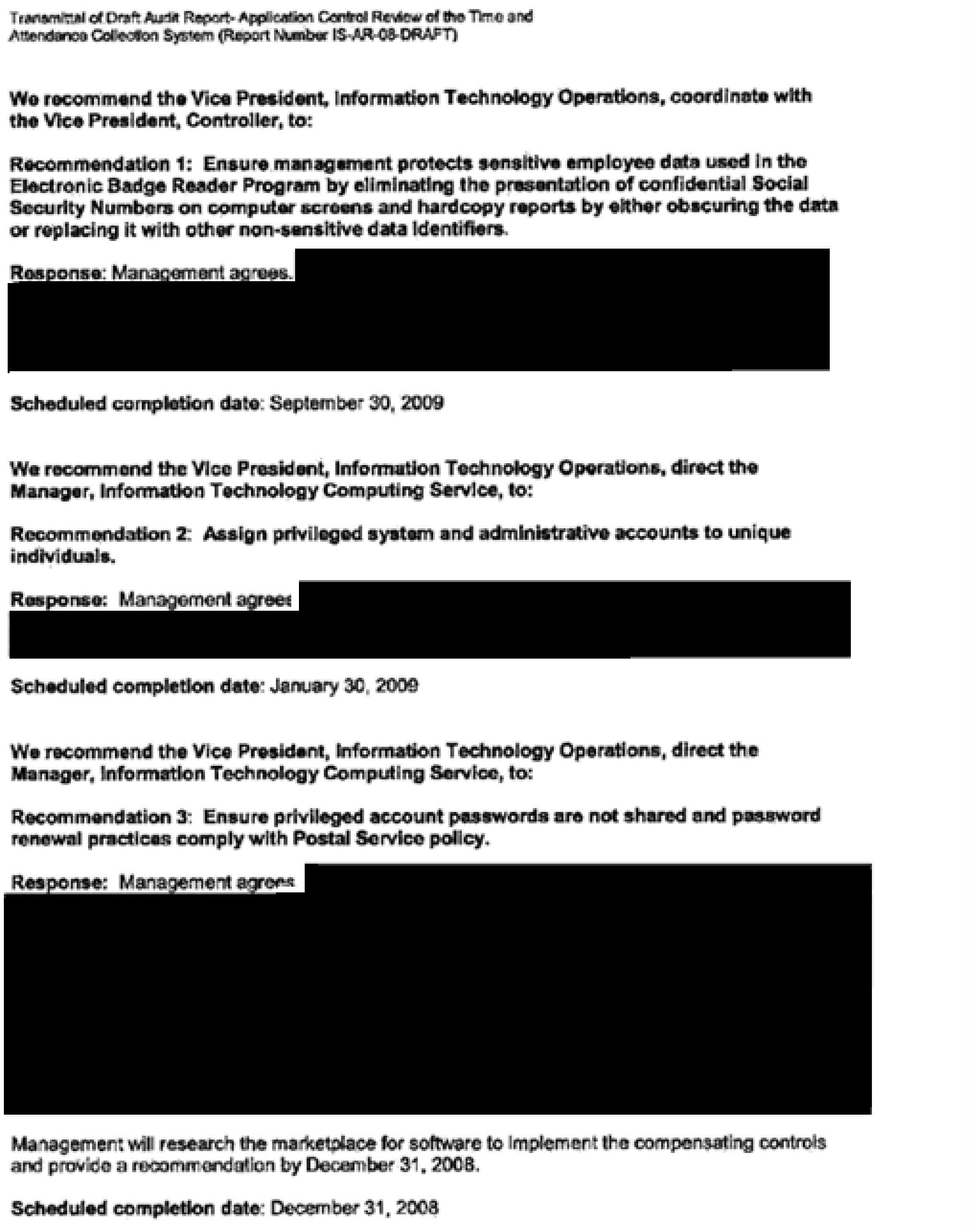
The subject audit report and this response contain information relating to potential security vulnerabilities that, if released, could possibly be exploited and cause substantial harm to the U.S. Postal Service. The Manager, Corporate Information Security will work with you to determine what portions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

If you have questions or comments regarding our responses and would like to discuss them further, please contact Pete Stark, Manager, Corporate Information Security, at 202-268-7378.

George W. Wright

cc: Ross Philo
B. Lynn Malcolm
Harold E. Stark
Joseph J. Gabris
Jo Ann Mitchell
David M. Stauffer
William E. Koetz
Kathleen A. Warnaar
Katherine S. Banks
Christine Souter
Carol Reich

475 L'Enfant Plaza SW
Washington, DC 20260-1500
202-268-2764
Fax: 202-268-4492
george.w.wright@usps.gov
www.usps.com



Transmittal of Draft Audit Report- Application Control Review of the Time and Attendance Collection System (Report Number IS-AR-08-DRAFT)

We recommend the Vice President, Information Technology Operations, coordinate with the Vice President, Controller, to:

Recommendation 1: Ensure management protects sensitive employee data used in the Electronic Badge Reader Program by eliminating the presentation of confidential Social Security Numbers on computer screens and hardcopy reports by either obscuring the data or replacing it with other non-sensitive data identifiers.

Response: Management agrees. [redacted]

Scheduled completion date: September 30, 2009

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

Recommendation 2: Assign privileged system and administrative accounts to unique individuals.

Response: Management agrees [redacted]

Scheduled completion date: January 30, 2009

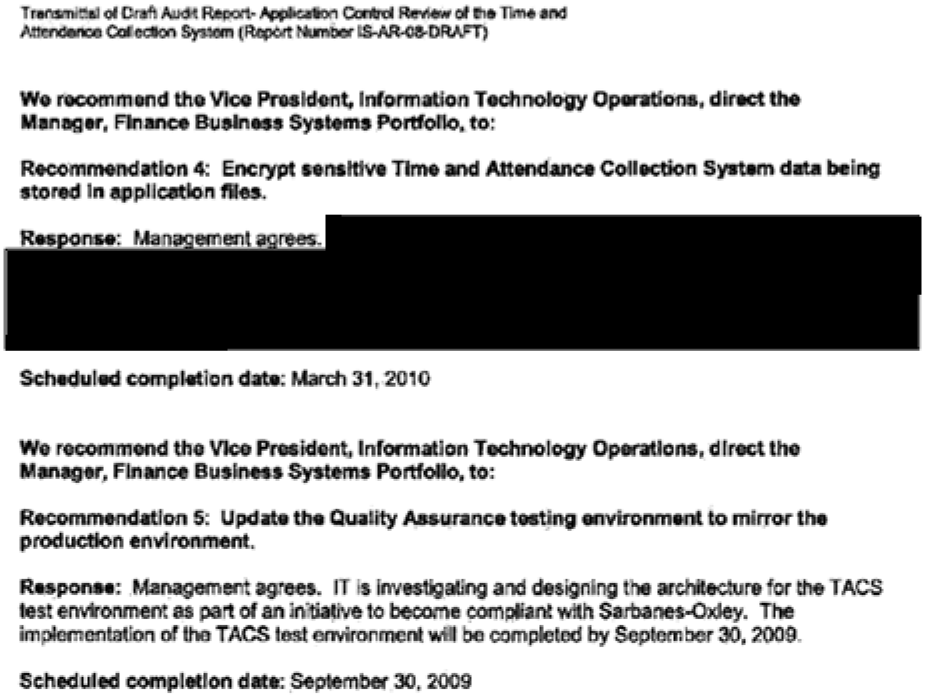
We recommend the Vice President, Information Technology Operations, direct the Manager, Information Technology Computing Service, to:

Recommendation 3: Ensure privileged account passwords are not shared and password renewal practices comply with Postal Service policy.

Response: Management agrees [redacted]

Management will research the marketplace for software to implement the compensating controls and provide a recommendation by December 31, 2008.

Scheduled completion date: December 31, 2008



Transmittal of Draft Audit Report- Application Control Review of the Time and Attendance Collection System (Report Number IS-AR-08-DRAFT)

We recommend the Vice President, Information Technology Operations, direct the Manager, Finance Business Systems Portfolio, to:

Recommendation 4: Encrypt sensitive Time and Attendance Collection System data being stored in application files.

Response: Management agrees. [redacted]

Scheduled completion date: March 31, 2010

We recommend the Vice President, Information Technology Operations, direct the Manager, Finance Business Systems Portfolio, to:

Recommendation 5: Update the Quality Assurance testing environment to mirror the production environment.

Response: Management agrees. IT is investigating and designing the architecture for the TACS test environment as part of an initiative to become compliant with Sarbanes-Oxley. The implementation of the TACS test environment will be completed by September 30, 2009.

Scheduled completion date: September 30, 2009