March 14, 2008

GEORGE W. WRIGHT
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

DEBORAH M. GIANNONI-JACKSON
VICE PRESIDENT, EMPLOYEE RESOURCE MANAGEMENT

SUBJECT: Audit Report – Update Processes for [redacted]
(Report Number IS-AR-08-009)

This report presents the results of our self-initiated review of the update processes to the [redacted][1] and [redacted][2] systems (Project Number 07RG013IS000). Our objective was to evaluate the controls over employee and contractor employment status updates to [redacted] and [redacted] systems. If employment status data do not flow accurately from [redacted], or if internal controls in these systems are not in place or working properly, it could result in improper or unauthorized user access to information systems.

Background

The [redacted] system has become an integral part of the day-to-day operations of the U.S. Postal Service. The system not only monitors who obtains access to various Postal Service resources, it also automates the creation and maintenance of user accounts. Its functionality provides efficiencies that allow for the elimination of the Postal Service (PS) Form 1357, Request for Computer Access, and the associated manual effort necessary to approve and create user accounts.

Employees and contractors use the [redacted] system to obtain automated access to registered Postal Service [redacted] and mainframe systems.[3] For example, entering a new hire in the [redacted] generates a PS Form 50,

---

1 [redacted]

2 [redacted] ™ ®

3 [redacted]

Notification of Personnel Action. [redacted] builds an employee profile for a new employee from the PS Form 50 data transmitted from [redacted] and assigns the employee a universal identifier (UID).[4] Then, bridging software extracts the employment data from [redacted] and populates an [redacted] logon ID[5] record in [redacted]. The logon ID remains inactive in [redacted] until the manager approves access. Over 100,000 additions, deletions, and changes occur weekly to [redacted] through [redacted] and the bridging software. [redacted]

[redacted]

To identify significant changes in employment data, [redacted] routinely runs automated jobs that provide daily reports. These jobs compare employee information records from the payroll system [redacted]. When [redacted] finds significant differences in employment information such as finance number or occupation code changes, they send a notification requesting the user provide a revised access request. Consistent with Handbook AS-805, *Information Security,*[6] if [redacted] does not receive a new PS Form 1357 within a specified time, they suspend and eventually delete the logonid.

[redacted] distinguishes a normal user from users who have different participant roles.[7] For example, the manager role (MGR) uses features of the application to approve access requests. If the user request comes from a contractor, a Contracting Officer's Representative must also approve. The Functional System Coordinator (FSC) role validates requests for access to critical or sensitive[8] applications, which requires an additional approval step. The FSC can also revoke user access to all applications if the manager does not. The FSC is also the application business owner. The Logon ID Administrator has final request approval and activates the account for new users. The requesting manager then receives notification of the activation and approval.

---

[4] [redacted]

[5] [redacted]

[6] According to Handbook AS-805, *Information Security*, March 2002 (updated with *Postal Bulletin* revisions through November 26, 2006), Section 9-6.3, Suspending Logon IDs, and Section 9-6.5, Terminating Logon IDs.

[7] Participant roles have access to the [redacted] system, administration module, or utilities. [redacted]

[8] Handbook AS-805, Section 3-3.2, Sensitivity and Criticality Category Independence, states "Sensitivity and criticality are independent designations. All Postal Service information must be evaluated to determine both sensitivity and criticality. Information with *any* criticality level may have *any* level of sensitivity designation and visa versa."

Several organizations manage or provide technical support for [redacted]. The Corporate Information Security Office, as Executive Sponsor for [redacted], provides oversight including development, production, and maintenance. The Database Support Services database administrators ensure Oracle database availability and performance, and access control to the database. The Information Technology Engineering and Architecture group manages the contractors supporting the [redacted] application infrastructure and the bridging software. The contractor, [redacted], develops and maintains the [redacted] application software and the bridging software to [redacted], as well as the system documentation.

[redacted][9]

[redacted] currently tracks rural carrier and Postal Inspection Service employees assigned to detail positions. Because these temporary employment changes require increased compensation, [redacted] generates a PS Form 50. This situation applies primarily to rural carriers who work in detail positions for more than 30 days. Besides tracking employees assigned to temporary positions using the PS Form 50, the Postal Service also uses PS Form 1723, Assignment Order. Payroll personnel use the PS Form 1723 to keep a record of executive and administrative service and bargaining unit employees assigned to detail positions at a higher level. Employees who work in higher level detail positions and meet certain conditions become eligible for higher compensation. [redacted] currently does not transmit PS Form 1723 data to [redacted] but could in the future if management changed business practices for employees assigned to detail positions.

Objective, Scope, and Methodology

See Appendix B for objective, scope, and methodology details.

Prior Audit Coverage

We did not identify any prior audits or reviews related to the objective of this audit.

[9] [redacted]

Results

The automated and manual processes accurately extracted employment status changes that were transmitted [redacted]; however, management needs to improve controls to better separate duties for users who can update [redacted]. Additionally, management needs to evaluate the business processes that affect employee status updates [redacted] and [redacted] to adequately separate duties between managers and users in [redacted]. Management also needs to evaluate the business processes [redacted] to allow [redacted] to better manage employee status changes, especially detail assignments that affect user access to critical or sensitive systems. Finally, management needs to improve [redacted] system documentation.

[redacted]. We made four recommendations to address these issues, including a joint recommendation to Employee Resource Management and Information Technology Operations to review the manager roles [redacted] and [redacted] to determine how to better integrate the roles. We also recommended that appropriate Postal Service organizational units establish requirements for tracking employees assigned to detail positions, implement a planned enhancement to [redacted] to ensure reviews take place when significant job assignment changes occur, and keep system documentation updated. While management did not agree with some facts in the findings leading up to recommendations 1 and 2, they recognized that the conditions were valid and agreed to correct them. Management fully agreed with recommendations 3 and 4. Management's comments and our evaluation of these comments are included in the report.

Separation of Duties

[redacted] Postal Service policy (policy) states that individuals' functional roles should be separate and their access should be limited to a minimum level. Separation of duties for application access is essential to ensure personnel have appropriate access levels to corporate information.

Security Interface for the Payroll System and the [redacted]

[redacted]

[redacted]

We are not providing a recommendation for this issue since management has an action in process to correct this condition.

Separating the MGR Role in [redacted]

[redacted][10]

[redacted]

[redacted]

Policy states that access to information resources must be specific to individuals' roles and responsibilities, and separation of duties and responsibilities will be considered when defining roles.[11] Additionally, personnel should only have access to sensitive and

[10] According to a system design document, the FSC must provide a rationale for denying a request.
[11] Handbook AS-805, Section 9-4.1.3, Separation of Duties.

critical information resources based on the minimum level of system functionality they need to perform their duties.[12]

The Corporate IT Portfolio organization formed a group[13] to help the Postal Service comply with Sarbanes-Oxley Act of 2002 (SOX) business requirements. We reviewed three security enhancements[14] the group plans to implement in [redacted] For example, when an employee requests a change in the assigned manager, the former manager and the new manager must approve this change. Management also plans to implement a process where the MGR or FSC performs a bi-annual review of user access to applications. [redacted]

Based on the planned SOX security enhancements, we are not providing a recommendation to make any changes to [redacted].

Recommendation

[redacted]

1. [redacted].

Management's Comments

[redacted]

[12] Handbook AS-805, Section 9-4.1.4, Least Privilege.

[13] The IT SOX/Postal Reform Portfolio group [redacted], as part of the "FY08 SOX Security Enhancements" project. The recently signed Postal Accountability and Enhancement Act of 2006 includes a requirement that the Postal Service be compliant with the SOX by the time it issues its first annual report in late 2010 (for FY 2010).

[14] [redacted]

Evaluation of Management's Comments

Although management disagreed with some facts in the finding, their response was in agreement with the recommendation's intent, and their comments are responsive. The actions planned or taken should correct the issues identified in the finding.

[redacted] Tracking for Employees Assigned to Detail Positions

Management did not design [redacted] to track employees assigned to detail positions. Additionally, management did not implement [redacted] to take full advantage of tracking detail positions. The IT SOX/Postal Reform group believes they can implement a process (with the assistance of Human Resources personnel) where employment information changes in [redacted] activate a notification to [redacted] managers to review the affected employees. Policy requires management to base access on the security principles of least privilege and the need to know. Tracking employees in detail assignments can prevent inappropriate access to applications because users who no longer require access are identified and their access needs can be reviewed and modified.

[redacted] did not have the full capability to track employees assigned to detail positions. [redacted] currently tracks 259 employees assigned to formal detail positions; however, according to management, over 23,000 employees work in detail assignments.

[redacted]

Without adequate controls to track employees assigned to detail positions, individuals may retain access to sensitive or critical information resources that they are not authorized to access after the detail ends. Preventing such unauthorized access eliminates potential modification, disclosure, or destruction of corporate information.

Policy states that management will grant access to sensitive and critical information resources based on providing personnel with the minimum level of system functionality needed to perform their duties.[15] Additionally, management must limit access to

[15] Handbook AS-805, Section 9-4.1.4, Least Privilege.

sensitive information resources to personnel who need to know the information to perform their duties.[16]

The IT SOX/Postal Reform group believes they can implement a process (with the assistance of Human Resources personnel) where employment information changes in [redacted] activate a notification to [redacted] managers to review the affected employees. For example, if any changes occur (duty station, finance number, occupation code, and employment status), [redacted] can pass them overnight to [redacted], which will generate emails to the appropriate managers. We believe management should leverage this capability in [redacted] so that unneeded access does not continue after termination of a detail assignment.

Recommendation

We recommend the Vice President, Employee Resource Management, coordinate with the Vice President, Information Technology Operations, to:

2. Review the capabilities and establish requirements in the [redacted] for tracking employees assigned to detail positions and how to pass timely and accurate data to [redacted].

Management's Comments

Management disagreed that there was an issue with data that is passed [redacted] for formal detail assignments where PS Form 50s were generated. Subsequent to receipt of the formal response, we received information to clarify this response. Management stated that the Executive Director, [redacted], will work with Information Technology [redacted] They targeted this action for completion by May 30, 2008.

Management additionally agreed that data for informal detail positions, not resulting in PS Form 50 activity, were not passed through the system to [redacted]. Management stated that the Executive Director, [redacted], would work with the managers of Employee Resource Management and Information Technology to develop requirements for tracking data for informal detail positions. Management targeted December 31, 2008, to complete this activity.

Evaluation of Management's Comments

Management disagreed that there was an issue with data passed to the [redacted] system. However, their response was in agreement with the recommendation's intent,

[16] Handbook AS-805, Section 9-4.1.2, Need to Know.

and their comments are responsive. The actions planned or taken should correct the issues identified in the finding.

Evaluation of [redacted] User Access

Management did not reevaluate [redacted] logon ID access when employees were reassigned. This occurred because management did not have any procedures in place to notify managers when employment changes occurred and when access should be reevaluated. Policy states that all managers have the responsibility of revoking access when it is no longer required. Reevaluating access when an employee's job responsibilities change helps ensure employees have access to only the data and systems needed to perform their work.

Employment changes affecting occupation code, finance number, or employment status could result in different access requirements to information systems. Except for terminations, [redacted] has no functionality to notify managers when employment changes occur and when access should be reevaluated. Managers or users can initiate access changes, but the FSCs have the ultimate responsibility for approving the appropriate level of access.

In the mainframe environment, [redacted] used programs to compare employee information records [redacted]

Policy states that all managers must immediately revoke access to information resources for personnel who no longer require it because of a change in job responsibilities, transfer, or termination.[17]

The IT SOX/Postal Reform group identified three SOX security enhancements[18] beginning in mid-2008 that will address this issue. Based on changes in employment information, appropriate [redacted] managers will receive timely notification to review these changes and determine if current employee access is required.

Recommendation

We recommend the Vice President, Information Technology Operations, direct the Manager, Corporate Information Security Office, to:

3. Develop and implement the planned [redacted] enhancement that will ensure access reviews take place when significant changes occur in job assignments.

[17] Handbook AS-805, Section 9-4.2.7, Revoking Access.
[18] [redacted]

Management's Comments

Management agreed with the recommendation. Management stated that, as part of the Sarbanes-Oxley effort, they are currently programming [redacted] to alert managers to review system access when an employee's job status changes. Management targeted May 30, 2008, to complete this activity.

Evaluation of Management's Comments

Management's comments are responsive to the recommendation, and the actions planned or taken should correct the issues identified in the finding.

System Documentation for [redacted]

The contractor did not maintain up-to-date system documentation for [redacted]. Policy states the principle of configuration management includes the responsibility of adequately maintaining system documentation.[19] Current system documentation is important for tracking system changes and ensuring the system is operating as designed.

[redacted]

Good configuration management provides integrity and traceability to software throughout the change life cycle. As a best practice, keeping system documentation current is important for tracking system changes and assuring the system is operating as designed.

Recommendation

We recommend the Vice President, Information Technology Operations, direct the Manager, Corporate Information Security Office, to:

4. Review and update system documentation for [redacted], and implement a process to ensure system documentation is kept current in the future.

[19] Management Instruction AS-850-2002-10, *Information Technology Change and Configuration Management*, Overview section, August 22, 2002.

Management's Comments

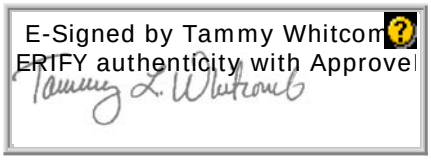
Management agreed with the recommendation. Management stated that, as part of the Sarbanes-Oxley enhancements to [redacted], they will ensure that documentation is kept up-to-date, including any required changes to documentation due to system enhancement or maintenance. Management targeted June 30, 2008, to complete these activities.

Evaluation of Management's Comments

Management's comments are responsive to the recommendation, and the actions planned or taken should correct the issues identified in the finding.

The U.S. Postal Service Office of Inspector General (OIG) considers recommendations 1 through 3 significant, and therefore requires OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. These recommendations should not be closed in the follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

We appreciate the cooperation and courtesies provided by your staff. 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: Ross Philo
H. Glen Walker
Harold E. Stark
John P. Byrne
Joseph J. Gabris
Gregory "Dean" Larrabee
Michael E. Goldman
Larry V. Goodman
Jerry M. McClure
Steven W. Monteith
Nancy M. Laich
Katherine S. Banks

APPENDIX A. EMPLOYMENT STATUS DATA FLOW

Redacted

[redacted]

APPENDIX B. OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to evaluate the controls over employee and contractor employment status updates to the [redacted]

We conducted this audit at the Information Technology Service Center in Raleigh, North Carolina; the Information Technology and Accounting Service Center in Eagan, Minnesota; and at [redacted] a contractor in [redacted]. Specifically, we worked with managers in the following functional areas: IT Engineering & Architecture [redacted][20] [redacted][21] [redacted]

To accomplish this objective, we interviewed key managers to identify the information systems that provide employment status data to [redacted]. We also identified the processes that passed employment hiring, termination, and change (PS Form 50) data from [redacted] and from the [redacted] Furthermore, we identified internal controls (such as participant roles) in [redacted] to verify management had adequately separated the duties of employees assigned these roles.

We reviewed manual and automated procedures that managers used to track employee status changes. Additionally, we identified manual and automated processes that allow users to gain access to the [redacted] and mainframe environments. Finally, to determine if the Postal Service had plans to make major changes to any of the systems providing employment status data, we reviewed a document[22] highlighting 20 planned security enhancements to [redacted]. The IT SOX Postal Report Portfolio Organization identified these enhancements to comply with SOX business requirements.

To determine the number of active employees in [redacted], we used automated tools and analyzed about 1.3 million user records [redacted][23] We identified active users based on the values in the user status and employee status fields.[24] [redacted][25] We tested the [redacted] for duplicate records and found none.

---

[20] [redacted]

[21] [redacted]

[22] "[redacted] FY08 SOX Security Enhancements" was dated October 2007.

[23] We obtained authorization to gain access to the [redacted] and downloaded records on October 21, 2007.

[24] [redacted]

[25] [redacted]

We conducted this audit from August 2007 through March 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We used manual and automated techniques to analyze the computer-processed data. Based on the results of these tests and assessments, we generally concluded the data were sufficient and reliable to use in meeting the objective.

APPENDIX C. MANAGEMENT'S COMMENTS

UNITED STATES POSTAL SERVICE

March 4, 2008

TAMMY L. WHITCOMB

SUBJECT: Update Process for [redacted]
Report Number IS-AR-08-DRAFT

We are pleased to provide the attached responses to the recommendations in the subject audit report. We are in agreement with findings three and four and where feasible have taken or are taking corrective actions to address all requirements of the recommendations detailed in the report.

[redacted]

Recommendation 1

We recommend the Vice President, Employee Resource Management, coordinate with the Acting Vice President, Chief Technology Officer to:

[redacted]

Response

Management disagrees that there is a problem with the flow of data [redacted] for permanent positions. For these transactions, an action is created in [redacted] which generates a PS Form 50. [redacted] currently passes PS Form 50 data each night to the [redacted] so the system is current.

One issue that has been identified is that [redacted] is designed to allow the employee to self-designate a new manager. [redacted] and Information Technology are currently building a two-level approval process through which both the employee's current manager and the newly designated functional manager must approve the change.

The Executive Director, [redacted] will work with [redacted] and Information Technology to ensure that the two-level approval process is implemented in a timely manner. Targeted completion date: May 30, 2008.

475 L'Enfant Plaza SW
Washington DC 20260
www.usps.com

Recommendation 2

We recommend the Vice President, Employee Resource Management, coordinate with the Acting Vice President, Chief Technology Officer to:

- Review the capabilities and establish requirements [redacted] for tracking employees assigned to detail positions and how to pass timely and accurate data to eAccess.

Response

Management disagrees that there is an issue with data being passed [redacted] for detail assignments where PS Forms 50 are generated. Data for formal detail positions that result in a PS Form 50 is passed each night [redacted] and the system is current. Targeted completion date: May 30, 2008.

Management agrees that data for informal detail positions that do not result in a PS Form 50 activity are currently not trackable items within [redacted] and no data is passed through the system. The Executive Director, [redacted] will work with Employee Resource Management, Information Technology, and [redacted] to develop requirements for tracking data for informal detail positions by the end of calendar year 2008. Based on the scope of the requirements, implementation plans will be developed at that time.

Recommendation 3

We recommend the Vice President, Acting Chief Technology Officer, direct the Manager, IT Service Center, to:

- Develop and implement the planned [redacted] enhancement that will ensure access reviews take place when significant changes occur in job assignments.

Response

Management agrees. The capability of alerting managers to an employee's change in job status for the purpose of reviewing their system access rights is currently being programmed within [redacted] as part of the SOX effort. Targeted completion date: May 30, 2008.

Recommendation 4

We recommend the Vice President, Acting Chief Technology Officer, direct the Manager, Corporate Information Security Office, to:

- Review and update system documentation for [redacted] and implement a process to ensure system documentation is kept current in the future.

Response

Management agrees. As part of the SOX enhancements to [redacted] the developer will ensure that the documentation is kept up to date. The developer will also ensure as part of its

enhancement and maintenance that any required changes to documentation are made. Targeted Completion date: June 30, 2008.

Deborah Giannoni-Jackson
Vice President
Employee Resource Management

George W. Wright
Vice President
Information Technology Operations

cc: H. Glen Walker
Harold E. Stark
John P. Byrne
Joseph J. Gabris
Gregory "Dean" Larrabee
Michael E. Goldman
Larry V. Goodman
Jerry M. McClure
Steven W. Monteith
Nancy M. Laich
Katherine S. Banks