



November 13, 2008

GEORGE W. WRIGHT  
VICE PRESIDENT, INFORMATION TECHNOLOGY OPERATIONS

DEBORAH GIANNONI-JACKSON  
VICE PRESIDENT, EMPLOYEE RESOURCE MANAGEMENT

SUBJECT: Audit Report – Security Policies and Procedures (Corporate-Wide) at the Information Technology and Accounting Service Centers for Fiscal Year 2008 (Report Number IS-AR-09-002)

This report presents the results of our audit of corporate-wide security planning and program management at the U.S. Postal Service's Information Technology and Accounting Service Centers (IT/ASCs) located in [REDACTED] (Project Number 08RD001IS003). The objectives were to determine whether management established a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. We performed this self-initiated review as part of the fiscal year (FY) 2008 information systems audit of general controls at IT/ASCs. See [Appendix A](#) for additional information about this audit.

### Conclusion

Overall, management has established information security policies and procedures to protect critical and sensitive information resources. These include, but are not limited to, implementing the components of a security management structure and including security procedures in hiring and termination practices. However, our review identified opportunities to improve compliance with these policies and procedures. Specifically, management can improve personnel policy controls by initiating security clearance processing for all employees occupying sensitive positions. In addition, management could improve their identification of threats and vulnerabilities to computing resources by performing periodic application risk assessments.

## Security Clearances

Management did not perform security clearance processing for nine of 454 Postal Service career IT employees in “sensitive” positions.<sup>1</sup> This occurred because Corporate Personnel Management employees were unsure of policies and responsibilities for initiating security clearance processing for positions classified as sensitive. Performing security clearances protects sensitive and critical Postal Service resources from potential loss and ensures that only reliable and trustworthy individuals access these resources. When we brought this issue to management’s attention, they took corrective action to initiate the nine security clearances. See [Appendix B](#) for our detailed analysis of this topic.

We recommend the Vice President, Human Resources, direct the Manager, Corporate Personnel Management, to:

1. Develop a process to ensure security clearances are initiated for individuals in positions classified as sensitive.
2. Provide reports to the Security Control Officer on a semi-annual basis to track the security clearance status of employees in sensitive positions at the [REDACTED] Information Technology and Accounting Service Centers.

## System and Application Reviews

Management could not provide documentation to verify they had completed a current risk assessment on the six applications<sup>2</sup> we reviewed. This occurred because employees did not conduct or document risk assessments or the re-assessments that are required every 3 years as defined by Security Risk Management policy.<sup>3</sup> Performing risk assessments on a timely basis ensures the Postal Service develops adequate security measures to protect existing information resources. See [Appendix B](#) for our detailed analysis of this topic.

---

<sup>1</sup> Handbook AS-805, *Information Security*, March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006), Section 6-4.1, states that sensitive positions, as defined in the *Administrative Support Manual (ASM) 27*, Security, include those in which personnel could, in the normal performance of their duties, cause material adverse effect to Postal Service information resources. [REDACTED]

<sup>2</sup> [REDACTED]

<sup>3</sup> *Information Technology (IT) Manual, Security Risk Management Policy*, Information Resource Risk Management, dated March 25, 2008, states that risk assessments must be re-assessed and the risk assessment report updated at least every 3 years following deployment of a resource unless earlier re-assessment is warranted.

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

3. Perform risk re-assessments on the [REDACTED] applications reviewed during this audit.
4. Establish milestones to review all sensitive and critical applications for current risk assessments and complete the re-assessments on those applications that are not current.

### Management's Comments


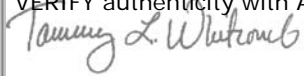
The Vice President, Employee Resource Management, agreed with recommendation 1 and stated Corporate Personnel Management would work with the Postal Inspection Service to ensure that a process is in place to initiate the necessary sensitive security clearances by January 15, 2009. Management stated they agree with the intent of recommendation 2 and will work with the Postal Inspection Service to ascertain the best process for providing information to the Security Control Officer (SCO).

The Vice President, Information Technology Operations, agreed with recommendations 3 and 4. For recommendation 3, the Corporate Information Security Office (CISO) will work with the appropriate Information Technology Business Systems portfolios to complete risk assessments by [REDACTED], for the six applications reviewed during this audit. Concerning recommendation 4, management will establish a risk reassessment schedule by December 31, 2008, and will complete the risk reassessments by [REDACTED]. See [Appendix C](#) for management comments in their entirety.

### 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  
Deputy Assistant Inspector General  
for Revenue and Systems

#### Attachments

cc: Ross Philo  
Harold Stark  
Joseph J. Gabris  
Elizabeth Hepner  
Katherine S. Banks

## APPENDIX A: ADDITIONAL INFORMATION

### BACKGROUND

A corporate-wide security program is the foundation of an organization's security control structure and a reflection of senior management's commitment to addressing security risks. Handbook AS-805<sup>4</sup> establishes the Postal Service's information security policies for appropriately identifying information resources and business requirements and protecting those information resources. The intent of information security policies is to ensure the creation and implementation of an environment that:

- Protects information resources critical to the Postal Service;
- Protects information as mandated by federal laws;
- Protects the personnel information and privacy of employees and customers;
- Reinforces the reputation of the Postal Service as an institution deserving public trust;
- Complies with due diligence standards for the protection of information resources; and,
- Assigns responsibilities to relevant Postal Service officers, executives, managers, employees, contractors, partners, and vendors.

The Postal Service has delegated the Manager, Corporate Information Security, authority for the development, implementation, and management of the information security program.<sup>5</sup>

### OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives were to determine whether management established a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

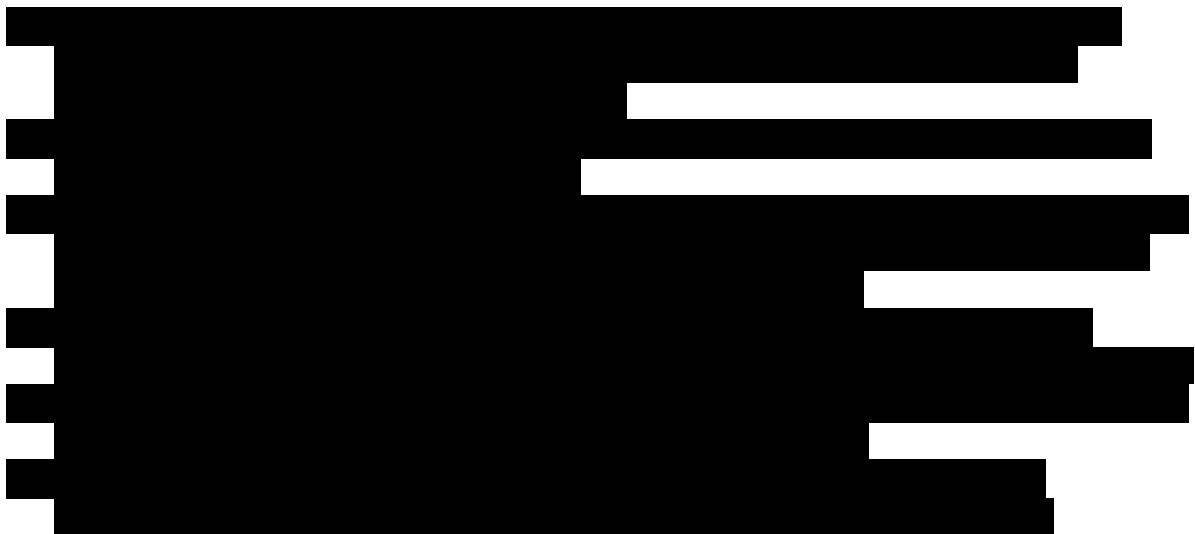
The scope of our review included corporate-wide security policies and procedures at the U.S. Postal Service's IT/ASCs located in [REDACTED]

---

<sup>4</sup> Handbook AS-805 has been incorporated into the new *Information Technology (IT) Manual, Corporate Information Security*, March 25, 2008. [REDACTED]

<sup>5</sup> *IT Manual, Corporate Information Security, Roles and Responsibilities*, March 25, 2008.

Our review covered the main platforms the Postal Service uses in its computing environment.<sup>6</sup> We judgmentally selected the following six applications to review for FY 2008.<sup>7</sup>



To determine if management performed, documented and updated risk assessments for the selected applications on a regular basis, we reviewed security risk management and IT recertification policies and procedures, interviewed key Postal Service personnel, and reviewed risk assessment documentation.

To determine if management documented, approved, and periodically reviewed security plans for the selected applications, we interviewed key Postal Service personnel and reviewed documentation.

To determine if management has established a security management structure, we reviewed documentation detailing the roles and responsibilities associated with Postal Service information security. To verify that management clearly assigned information security responsibilities, we reviewed the Postal Service's Information Security Plan, which identifies the owners and managers of computer resources. To determine if owners and users were aware of security policies, we interviewed system owners to determine what training employees had received and whether they were aware of their security-related responsibilities. To determine if management implemented an incident response capability, we interviewed management officials and reviewed an incident handling activity.

To determine if hiring policies address security, we reviewed Postal Service policies, interviewed key Postal Service personnel, and reviewed sensitive positions to determine

<sup>6</sup> [Redacted]

<sup>7</sup> The criteria for selection included a system or application that is financial or directly supports the financial statements; has a nationwide impact; is classified sensitive or critical while in production; was not recently reviewed by an OIG or Ernst & Young audit team; and is identified as Sarbanes-Oxley related.

whether management had performed security clearances. To determine if termination policies address security, we reviewed Postal Service policies and interviewed key Postal Service personnel. To verify that employees have adequate security training, we reviewed the Postal Service's employee training and professional development program.

We conducted this performance audit from February through November 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 used manual and automated techniques to analyze computer-processed data. Based on the results of these tests and assessments, we generally concluded that the data were sufficient and reliable to use in meeting the objectives. We discussed our observations and conclusions with management officials during the audit and on October 1, 2008, and included their comments where appropriate.

**PRIOR AUDIT COVERAGE**

Report Title	Report Number	Final Report Date	Report Results
<p><i>Separation of Duties at the [REDACTED] Information Technology and Accounting Service Centers</i></p>	<p>IS-AR-07-017</p>	<p>August 29, 2007</p>	<p>Overall policies, procedures, and internal controls were adequate to separate duties for personnel accessing critical information system resources at the data centers. However, controls to determine which career employees required sensitive security clearances needed strengthening. Specifically, management did not always review and update the classification of sensitive positions for employees at the three IT/ASCs in a timely manner. Also, some ASC career employees had sensitive security clearances, while other ASC employees in similar positions did not. Management agreed with all five recommendations and all remain open because action has not been completed.</p>
<p><i>Personnel Security Controls at the [REDACTED] Information Technology and Accounting Service Centers</i></p>	<p>IS-AR-04-011</p>	<p>September 8, 2004</p>	<p>Internal controls over hiring and termination procedures for Postal Service employees and contractors were generally effective. There were no exceptions in the review of initial security clearances and updates for contractors; however, security clearance updates were not obtained for 20 Postal Service career employees holding sensitive positions at the [REDACTED] IT/ASCs. Management completed corrective action for the recommendation and this issue is closed.</p>



## APPENDIX B: DETAILED ANALYSIS

### Security Clearances

Nine of 454<sup>8</sup> career employees in IT positions classified as “sensitive” did not have security clearances. In order to determine which IT positions at the [REDACTED] IT/ASCs require a security clearance, the SCO refers to the Information System Sensitive Position Register. The register lists all current IT positions and occupation codes for positions classified as sensitive. The SCO is responsible for maintaining a security clearance database for career and contract employees at the [REDACTED] IT/ASCs.<sup>9</sup> The Postal Service uses this database to track interim, final, and updated sensitive security clearances<sup>10</sup> for current career employees and contractors in sensitive positions. The Postal Inspection Service is responsible for conducting background investigations and granting security clearances<sup>11</sup> for Postal Service career employees and contractors.<sup>12</sup>

We requested current information on the status of security clearances; in providing this information to us, the SCO compared the current Human Resource staffing report to the security clearance database and identified nine employees who did not have security clearances. One employee was a new hire and all but two of the remaining eight had been promoted into sensitive positions since 2005. Corporate Personnel Management, which handles Executive Administrative Services hires and promotions, assumed the CISO office was responsible for the initial security clearance documentation for IT sensitive positions.

When an employee accepts a career position with the Postal Service, Corporate Personnel Management is responsible for providing the initial security clearance documentation and instructions. They forward this information to the Postal Inspection Service, Operations Support Group (ISOSG), Security Investigation Service Center, for processing. The ISOSG grants the interim clearance within 10 days of receiving the paperwork and the final clearance follows the full background review. The ISOSG forwards notification of the interim and final security clearances to the SCO, who uses this information to update the security clearance database.

<sup>8</sup> [REDACTED].

<sup>9</sup> This requirement was established based on the audit, *Personnel Security Controls at the [REDACTED] IT/ASCs* (Report No. IS-AR-04-011, dated September 8, 2004). Management expanded the security clearance database used by the SCO in [REDACTED] to include employees assigned to sensitive positions at the [REDACTED] IT/ASCs.

<sup>10</sup> ASM 13, Section 272.22, July 1999 (updated with *Postal Bulletin* revisions through September 27, 2007) states that sensitive clearances are considered for Postal Service employees who, by virtue of their duties, have access to sensitive information restricted to the highest levels of the federal government or OIG files, Postal Inspection Service files, national security (classified) information, or sensitive information essential to executive decision making.

<sup>11</sup> *IT Manual, Corporate Information Security, Roles and Responsibilities*, page 2, March 25, 2008.

<sup>12</sup> ASM 13, Section 272.3, July 1999 states that individuals who provide contract services to the Postal Service (including contractors, contractors' employees, subcontractors, and subcontractors' employees at any tier) and who have access to occupied Postal Service facilities and/or to Postal Service information and resources (including postal computer systems) must obtain a clearance as provided in Section 272 before getting access.

## System and Application Reviews

Management could not provide documentation to verify they had completed risk assessments for the six applications we reviewed. When we requested support to determine if the risk assessments were performed and documented on a regular basis, management stated they could not locate all of the documents but would provide any documentation available. According to Postal Service policy, a risk assessment is required for all information resources and will be performed in conjunction with system development. Further, risk assessments must be updated at least every 3 years following the deployment of an information resource.<sup>13</sup> We requested documentation to verify that the re-assessments were current and that management had updated them every 3 years. Management provided documentation for three of the six systems reviewed – [REDACTED]

[REDACTED]. Based on our review of those documents, the required re-assessments had not been performed.

Recertification re-evaluates the protection of existing resources to determine if the risk associated with deployment can be managed throughout the lifecycle of the resource.<sup>14</sup> It is the responsibility of the CISO to re-assess and re-certify information resources.

Performing risk assessments helps make certain that management identifies and considers all threats and vulnerabilities, identifies the greatest risks, and makes appropriate decisions regarding which risks to accept and which to mitigate through security controls.

---

<sup>13</sup> *IT Manual, Corporate Information Security, Policy, Processes, and Standards, Security Risk Management Policy, March 25, 2008.*

<sup>14</sup> *IT Manual, Corporate Information Security, Recertification Process, March 25, 2008.*

## APPENDIX C: MANAGEMENT'S COMMENTS

DEBORAH GWANNONI-JACKSON  
Vice President  
Employee Resource Management



October 30, 2008

Ms. Lucine Willis  
Director, Audit Operations  
1735 North Lynn St.  
Arlington, VA 22209-2020

SUBJECT: Draft Audit Report – Security Policies and Procedures (Corporate-Wide) at the [redacted] Information Technology and Accounting Service Centers for Fiscal Year 2008 (Report Number IS-AR-09-DRAFT)

Dear Ms. Willis:

Thank you for the opportunity to review and comment on the subject draft audit report. We have reviewed your recommendations concerning the process to initiate sensitive security clearances, and below is the response to each recommendation.

### Recommendation – Security Clearances:

We recommend the Vice President, Human Resources, direct the Manager, Corporate Personnel Management, to:

1. Develop a process to ensure security clearances are initiated for individuals in positions classified as sensitive.

#### Management Response

Management agrees. Corporate Personnel Management will work with the appropriate Inspection Service personnel to ensure that a process is in place to secure the initiation of necessary sensitive security clearances.

Scheduled Completion Date: January 15, 2009

2. Provide reports to the Security Control Officer on a semi-annual basis to track the security clearance status of employees in sensitive positions at the [redacted] Information Technology and Accounting Service Centers.

#### Management Response

While we agree with the intent of the recommendation, we are working with the Inspection Service to ascertain the best process for providing the information to the Security Control Officer.

Scheduled Completion Date: March 31, 2009

475 L'ENFANT PLAZA SW, ROOM 9840  
WASHINGTON, DC 20260-4200  
Fax: 202-268-3803  
WWW.USPS.COM

If you have any questions or comments regarding this response, please contact Elizabeth Hepner,  
Manager, Corporate Personnel Management, at (202) 268-2295.

  
Deborah Giannoni-Jackson

Security Policies and Procedures (Corporate-Wide) at the  
Information Technology and Accounting Service Centers  
for Fiscal Year 2008

IS-AR-09-002

GEORGE W. WRIGHT  
VICE PRESIDENT  
INFORMATION TECHNOLOGY OPERATIONS



October 30, 2008

Lucine M. Willis  
Director, Audit Operations  
Office of Inspector General  
1735 N. Lynn Street, Room 11044  
Arlington, VA 22209-2020

SUBJECT: Draft Audit Report - Security Policies and Procedures  
(Corporate-Wide) at the [REDACTED]  
[REDACTED] Information Technology and Accounting Service Centers for Fiscal  
Year 2008 IS-AR-09-DRAFT (Project Number 08RD001IS003)

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendations 3 and 4 of the report and the response is attached.

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

If you have any questions or comments regarding this response please contact [REDACTED]  
Corporate Information Security [REDACTED]

George W. Wright

Attachment

cc: Ross Philo  
H. Glen Walker  
Deborah Giannoni-Jackson  
Elizabeth Hepner  
Harold E. Stark  
Joseph J. Gabris  
Katherine S. Banks  
audittracking@uspsaig.gov

475 L'ENFANT PLAZA SW  
WASHINGTON, DC 20260-1500  
202-268-2764  
FAX: 202-268-4492  
GEORGE.WRIGHT@USPS.GOV  
WWW.USPS.COM

Security Policies and Procedures (Corporate-Wide) at the [REDACTED]  
[REDACTED] Information Technology and Accounting Service Centers for  
Fiscal Year 2008 (Project Number 08RD001IS003)

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

3. Perform risk assessments on the six applications reviewed during this audit.

**Management Response**

Management agrees. Corporate Information Security will work with the appropriate  
Information Technology Business Systems portfolios to schedule and complete audits for:

**Scheduled Completion Date:** May 31, 2009

4. Establish milestones to review all sensitive and critical applications for current risk  
assessments and complete the re-assessments on those applications that are not  
current.

**Management Response**

Management agrees. We will establish the final schedule by December 31, 2008, and will  
complete the re-assessments by December 31, 2009.

**Scheduled Completion Date:** December 31, 2009