September 18, 2009

ROSS PHILO
EXECUTIVE VICE PRESIDENT, CHIEF INFORMATION OFFICER

SUBJECT: Audit Report – External Public Key Infrastructure Services – Fiscal Year 2009 (Report Number IS-AR-09-012)

This report presents the results of our audit of the U.S. Postal Service's external Public Key Infrastructure (PKI) services (Project Number 09RG017IS000). The objective was to determine whether the Postal Service effectively managed its external PKI services in compliance with established guidance. This audit was performed at the request of Postal Service management to ensure that the external PKI services continue to operate at a level to become cross-certified with the U.S. Government's Federal Bridge Certification Authority (FBCA). See Appendix A for additional information about this audit.

Conclusion

The Postal Service generally managed its external PKI services[1] in compliance with established guidance. However, we identified inconsistencies between Postal Service policies, FBCA policies, and the external PKI environment.

Postal Service PKI Policies and FBCA Certificate Policy (CP)

We found inconsistencies with internal Postal Service PKI policies and between Postal Service and FBCA policy. Postal Service staff did not perform periodic reviews to ensure PKI policies were consistent with each other and with federal PKI policy. Inconsistent PKI policies could delay future cross-certification between the Postal Service and the FBCA. See Appendix B for our detailed analysis of this topic.

Postal Service External PKI Policies and PKI Environment

The Postal Service external PKI environment was not consistent with certain policies in their Certification Practice Statements (CPSs). Postal Service PKI policies were not periodically reviewed to ensure the environment was operating in compliance with stated policies because of limited focus on cross-certification prior to the planned closing of the external PKI environment. Management could delay future cross-

[1] PKI is the combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions.

certification between the Postal Service and the FBCA by not operating the external PKI environment in compliance with PKI policies. See Appendix B for our detailed analysis of this topic.

When brought to their attention, management took action to correct the issues we identified. While we acknowledge management's timely action to resolve the issues, we are making a recommendation that, if implemented, should prevent similar issues in future years.

We recommend the Executive Vice President, Chief Information Officer, direct the Manager, Corporate Information Security, to:

1. Establish milestones to periodically review Postal Service Public Key Infrastructure policies and environment in relation to Federal Bridge Certification Authority Certificate Policy.

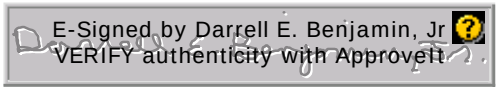
Management's Comments

Management agreed with the recommendation. On an annual basis beginning February 2010, the PKI manager will ensure a cross-certified Certificate Authority (CA) is compared for consistency to the FBCA's Certificate Policies and also that the Postal Service CPSs are compared with one another for consistency of language and procedures. See Appendix C for management's 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 recommendation and their corrective action 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 Frances E. Cain, Director, Information Technology, or me at (703) 248-2100.



Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachments

cc: John T. Edgar
Charles L. McGann, Jr
Mark J. Stepongzi
Joseph J. Gabris
Bill Harris

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

PKI is the combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions. A PKI relies on the exchange of digital certificates between authenticated users and trusted resources. A CA is a basic component of a PKI. A CA issues certificates to users, computers, and services and manages those certificates.

To support PKI-enabled applications, an organization must design and implement the CA hierarchy. Common roles in a CA hierarchy include a root CA, a policy CA, and an issuing CA. The Postal Service's external PKI[2] consists of a root CA, an intermediate CA, and two subordinate CAs in Eagan, MN.

The CP is a written document that defines how an organization issues and uses certificates and what measures the organization uses to validate the subjects of the certificates. The CP also includes the legal requirements an organization must follow when using certificates that its PKI issues. The CPS is a statement of practices a CA uses to issue, revoke, and manage certificates. Different practice statements may exist on each CA in the hierarchy based on the type of certificates the CA issues and to whom the CA issues them.

Homeland Security Presidential Directive 12 (HSPD-12)[3] established a federal policy to create and use a government-wide secure and reliable form of identification for federal employees and contractors. Currently, [redacted]. However, the Federal Information Processing Standard Publication 201 requires every HSPD-12 credential the government issues to contain an external digital certificate. As a result, the Postal Service created a CA server room [redacted] that houses the external PKI environment. This environment could authenticate and verify government-wide identification badges issued to Postal Service employees and contractors.

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is an interagency body set up under the Chief Information Officers Council to enforce digital certificate standards for trusted identity authentication across federal agencies and among federal agencies and outside bodies. The FBCA is an information system that facilitates an entity accepting certificates issued by another entity for a transaction.

In support of HSPD-12, the FPKIPA approved the Postal Service's external PKI for cross-certification in October 2006 at a medium hardware level. The FPKIPA requires

[2] The Postal Service refers to their policy CA as an intermediate CA and refers to their issuing CA as a subordinate CA.
[3] *Policy for a Common Identification Standard for Federal Employees and Contractors*, dated August 27, 2004.

an annual compliance audit and considers a delta compliance audit[4] acceptable in lieu of a full compliance audit if no significant changes to policies, procedures, or operations have occurred during the previous year. Although the Postal Service is no longer cross-certified, we conducted this audit to ensure the Postal Service external PKI services continue to operate at a level to become certified with the FBCA.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine whether the Postal Service effectively managed its external PKI services in compliance with established guidance. We conducted our work [redacted].

As permitted by *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)* Section 8.1 and requested by Postal Service management, we performed a delta compliance audit covering all changes to policies, procedures, or operations that may have occurred during the previous year.

We reviewed the following topics as required by a delta compliance audit for the external PKI environment:

- Personnel controls
- Separation of duties
- Internal audit review frequency and scope
- Types of events recorded in physical and electronic audit logs
- Protection of physical and electronic audit data
- Physical security controls
- Backup and archive generation and storage
- Items requiring resolution from the fiscal year (FY) 2008 PKI compliance audit

We used the following Postal Service policy documents, dated May 26, 2009, for this audit:

- *USPS Public Key Infrastructure (PKI) X.509 Certificate Policy (CP),* Version 1.67
- *USPS Root Certification Authority (CA) Certification Practice Statement (CPS),* Version 1.19
- *USPS Intermediate Certification Authority (CA) Certification Practice Statement (CPS),* Version 1.19
- *USPS Subordinate Certification Authority (CA) Certification Practice Statement (CPS),* Version 1.19

[4] A delta compliance audit covers all significant changes from the previous year and also covers specific topics described in the Objectives, Scope, and Methodology section of this report.

To determine whether personnel controls were in place, we reviewed security clearance records for PKI personnel and interviewed staff regarding proper training for PKI personnel. Further, we verified that PKI personnel received notification of changes to CA operations and verified that CP and CPS documents were available via the Internet.

To determine if separation of duties were effective, we reviewed the official designation of PKI roles and responsibilities, interviewed staff regarding sensitive tasks that require at least two individuals to complete, verified that operations manuals were available to PKI personnel, reviewed group and user settings [redacted], and reviewed CA server configurations.

To verify PKI auditing functions, we interviewed staff regarding internal auditing procedures, frequency, and scope; reviewed events recorded in audit logs and audit log summary reports; and reviewed CA server audit policy settings. To verify the security of physical and electronic audit data, we reviewed and tested PKI security settings and verified that physical controls were in place for access to the CA room.

To validate physical security controls, we reviewed CA room access lists and tested access controls to the room. We interviewed [redacted] facility staff regarding environmental controls and observed and validated controls in the physical environment.

To verify procedures for backup and archive generation and storage, we interviewed staff regarding backup and archival processes, validated the daily backup mechanism, witnessed the movement of backup media for off-site rotation, and verified archive retention periods.

To validate that management has taken corrective action on items from the FY 2008 PKI compliance audit, we verified the changes during fieldwork and reviewed the current CP and CPS documentation versions to ensure the stated changes were in place.

We conducted this performance audit from April through September 2009 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 throughout the audit and on September 4, 2009, and included their comments where appropriate.

PRIOR AUDIT COVERAGE

Report Title	Report Number	Final Report Date	Report Results
Compliance Audit of the Postal Service's External Public Key Infrastructure Services	IS-AR-08-017	September 11, 2008	In general, we found the Postal Service was effectively managing its PKI services in compliance with established guidance as stated in their CP and CPS. However, we identified 12 instances of non-compliance between the Postal Service's PKI policies and its external PKI environment. Of these, management corrected two and developed resolution plans for the remaining 10. Management agreed with our recommendation and stated they would establish milestones to implement resolution for the remaining non-compliant issues in the external PKI environment by December 31, 2008. During the FY 2009 audit, we verified that nine of the 10 remaining instances of non-compliance were completed and that management was in the process of correcting the remaining issue.
Compliance Audit of the Postal Service's External Public Key Infrastructure Services	IS-AR-08-001	October 5, 2007	In general, we found the Postal Service's external PKI environment complies with their CP, CPS, and any applicable Memorandum of Agreement . However, the Postal Service could improve their external PKI environment by mitigating the remaining instances of its non-compliance with Postal Service PKI policies and procedures in the external PKI environment. Management agreed with our recommendation and stated they would develop a risk mitigation plan by October 31, 2007. We verified that management resolved the remaining FY 2007 instances of non-compliance during the FY 2008 audit.
Information for the Federal Bridge Certification Authority	IS-WP-07-001	October 2, 2006	We concluded that, as of September 1, 2006, the Postal Service's PKI operations conformed to the CPS documents.

Report Title	Report Number	Final Report Date	Report Results
Certificate Authority Public Key Infrastructure Compliance [redacted]	IS-AR-06-015	September 1, 2006	We performed a follow-up audit and reviewed items identified in a March 2006 audit performed by Klynveld Peat Marwick Goerdeler LLP. We determined the Postal Service had corrected most of the issues identified in the report. However, management could make improvements by establishing and assigning the HSPD-12 Registration Authorities and Subscribers and completing the CA-PKI backup environment. Management agreed with the recommendation and stated that the completion date for the PKI backup site was September 1, 2006.

APPENDIX B: DETAILED ANALYSIS

Postal Service PKI Policies and FBCA CP

We found differences between the Postal Service CP, the Postal Service root CA CPS, intermediate CA CPS, subordinate CA CPS, and the FBCA CP. Specifically we found:

- The Postal Service CP did not specify PKI in the titles of the CA Administrator, Operator, and Backup Operator as stated in the root, intermediate, and subordinate CPS.

- The Postal Service CP, root, intermediate, and subordinate CPS did not contain the word, "Security", in the Section 5.3.1 title as stated in the Section 5.3.1 title in the FBCA CP.

- Role responsibilities of the PKI Certificate Manager, CA Administrator, and PKI Disaster Recovery Facility Coordinator were missing in the Postal Service CP, intermediate CPS, and subordinate CPS.

[redacted]

Postal Service staff did not perform periodic reviews of PKI policies to ensure they were consistent with each other and with federal PKI policy. Inconsistent PKI policies could delay future cross-certification between the Postal Service and the FBCA.

Postal Service External PKI Policies and PKI Environment

We found some policies stated in the Postal Service CPS were not followed in the Postal Service external PKI environment. Specifically:

- The PKI [redacted] were not consistent with the description of the file in the root, intermediate and subordinate CPS.

- All Postal Service PKI [redacted] from what was stated in the root, intermediate, and subordinate CPS.

- [redacted].

Postal Service PKI policies were not periodically reviewed to ensure the environment was operating in compliance with stated policies because of limited focus on cross-certification prior to the planned closing of the external PKI environment. Management

could delay future cross-certification between the Postal Service and the FBCA by not operating the external PKI environment in compliance with PKI policies.

In Table 1, we summarized the results of our review of the Postal Service CP and CPS documents. All 711 items we reviewed were compliant at the time we issued this report.

Table 1 – Status of Compliance

Status of Items Reviewed	Total	Percentage
Compliant with environment	701	98.6
Non-compliant items corrected	10	1.4
Non-compliant items outstanding	0	0.0
Total items reviewed	711	100.0

APPENDIX C: MANAGEMENT'S COMMENTS

ROSS PHILO
EXECUTIVE VICE PRESIDENT
CHIEF INFORMATION OFFICER

UNITED STATES POSTAL SERVICE

September 11, 2009

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

SUBJECT: Transmittal of Draft Audit Report – External Public Key Infrastructure Services FY 2009 (Report Number IS-AR-09-DRAFT) Project Number 09RG017IS000

Thank you for the opportunity to review and comment on the subject draft audit report. We are in agreement with recommendation 1 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 Gerri Wallace, Corporate Information Security at (202) 268-6821.

Ross Philo

Ross Philo

Attachment

cc: John T. Edgar
Charles L. McGann, Jr.
Mark J. Stepongzi
Jerome G. Reynolds
Joseph J. Gabris
Bill Harris
audittracking@uspsoig.gov

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

Review of the Postal Service's External Public Key Infrastructure Services – FY 2009
Report Number IS-AR-09-DRAFT (Project Number 09RG017IS000)

We recommend the Executive Vice President, Chief Information Officer; direct the Manager, Corporate Information Security to:

1. Establish milestones to periodically review the Postal Service external Public Key Infrastructure policies and environment in relation to Federal Bridge Certification Authority Certificate Policy.

   Management Response
   Management agrees with the recommendation. CISO has updated the Certificate Authority (CA) PKI Manager Operations Manual that beginning February 2010, on an annual base; the PKI Manager will ensure a cross-certified CA is compared for consistency to the Federal Bridge Certificate Authority's Certificate Policies and also that the Postal Service Certificate Practice Statements (CPSs) are compared to one another for consistency of language and procedures.

   Scheduled completion date: completed, closure requested.

APPENDIX D: COMPLIANCE LETTER TO FEDERAL PUBLIC KEY INFRASTRUCTURE POLICY AUTHORITY

The audit letter of compliance and background information required for the FPKIPA begins on the next page.

September 18, 2009

ROSS PHILO
EXECUTIVE VICE PRESIDENT, CHIEF INFORMATION OFFICER

SUBJECT: External Public Key Infrastructure Services – Fiscal Year 2009

We performed an audit to determine if the U.S. Postal Service effectively managed its external Public Key Infrastructure (PKI) services in compliance with established guidance. This audit was performed to ensure that the external PKI services continue to operate at a level to become certified with the U.S. Government's Federal Bridge Certification Authority.

Audit Methodology

We conducted this audit from April through September 2009, in accordance with generally accepted government auditing standards. As permitted by *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)* Section 8.1, we performed a delta compliance audit covering all changes to policies, procedures, or operations that may have occurred during the previous year. We reviewed the following topics as required by a delta compliance audit for the external PKI environment:

- Personnel controls
- Separation of duties
- Internal audit review frequency and scope
- Types of events recorded in physical and electronic audit logs
- Protection of physical and electronic audit data
- Physical security controls
- Backup and archive generation and storage
- Items requiring resolution from the FY 2008 PKI compliance audit

Documents and Criteria

We used the following Postal Service policy documentation, dated May 26, 2009, as criteria during our audit:

- *USPS Public Key Infrastructure (PKI) X.509 Certificate Policy(CP)*, Version 1.67
- *USPS Root Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.19.

- *USPS Intermediate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.19.
- *USPS Subordinate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.19.

Evaluation of Effective Management of Postal Service External PKI Environment in Compliance with Established Guidance

As of September 15, 2009, the Postal Service effectively managed its external PKI environment in compliance with established guidance. We reviewed 711 external PKI components documented in the criteria listed previously. Although we found 10 instances of non-compliance, we considered them insignificant to the overall external PKI environment.

The attachment to this letter contains the identity and qualifications of the U.S. Postal Service Office of Inspector General (OIG) personnel who conducted this audit.

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Revenue and Systems

Attachment

cc: John T. Edgar
Charles L. McGann, Jr
Mark J. Stepongzi
Joseph J. Gabris
Bill Harris

ATTACHMENT: BACKGROUND FOR FPKIPA AUDIT LETTER OF COMPLIANCE

Identity of the Auditors:

United States Postal Service
Office of Inspector General
1735 N. Lynn Street
Arlington, VA 22209-2020

Darrell E. Benjamin, Jr
Frances M. Cain
Michael Blaszczak
Ruth Smolinski
Kimberly Jones
Maria Gomez

Competence of the Auditors:

Darrell Benjamin, CPA, CIA, 20 years of audit experience
Frances Cain, CISA, 17 years of audit experience
Michael Blaszczak, CISA, CIPP, 13 years of audit experience
Ruth Smolinski, CISA, 3 years of audit experience
Kimberly Jones, 9 years of audit experience
Maria Gomez, CISA, CIA, 10 years of audit experience

Experience of Auditors Auditing PKI Systems:

The OIG has been involved in the Postal Service's PKI effort since August 2005. The OIG has performed several audits of the PKI environment.

Relationship of the Auditor to the U.S. Postal Service:

The OIG was authorized by law in 1996. The Inspector General, who is independent of Postal Service management, is appointed by and reports directly to the nine Presidentially-appointed Governors of the Postal Service. The primary purpose of the OIG is to prevent, detect, and report fraud, waste and program abuse and promote efficiency in the operations of the Postal Service.