September 15, 2010

ROSS PHILO
CHIEF INFORMATION OFFICER AND EXECUTIVE VICE PRESIDENT

SUBJECT: Audit Report – External Public Key Infrastructure Services – Fiscal Year 2010 (Report Number IS-AR-10-013)

This report presents the results of our audit of the U.S. Postal Service's external Public Key Infrastructure (PKI) services (Project Number 10RG014IT000). The objective was to determine whether the Postal Service effectively managed its external PKI services to comply with established guidance. We performed this audit at the request of Postal Service management to ensure that external PKI services continue to operate at a level to remain cross-certified with the U.S. Government's Federal Bridge Certification Authority. See Appendix A for additional information about this audit.

PKI is the combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions. PKI relies on the exchange of digital certificates between authenticated users and trusted resources. The Certificate Policy is a written document that defines how an organization issues and uses certificates and the measures the organization uses to validate the subjects of the certificates.

Conclusion

The Postal Service generally managed its external PKI services in compliance with established guidance. However, we identified inconsistencies between the Postal Service's Certificate Policy, Certification Practice Statements, and operations in the external PKI environment.

Postal Service PKI Policies and Environment

There were [redacted] instances where the operations of the Postal Service's external environment did not conform to the requirements of the Certification Practice Statements. In addition, there were 12 instances of inconsistencies between the Certificate Policy and Certification Practice Statements. Postal Service personnel did not perform periodic reviews of its external PKI operations and policies to ensure conformance. Inconsistencies may cause misinterpretation of PKI policies and delays in maintaining cross-certification with the Federal Bridge Certification Authority. For example, the roles and responsibilities memorandum did not contain the PKI auditor's

role as listed in the Certificate Policy and Root, Intermediate, and Subordinate Certification Practice Statements. See Appendix B for our detailed analysis of this topic.

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

We recommend the chief information officer and executive vice president direct the manager, Corporate Information Security, to:

1. Develop procedures to ensure reviews of applicable policies and processes are performed following changes to the Postal Service's external Public Key Infrastructure environment.

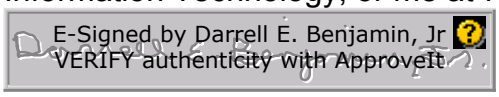
Management's Comments

Management agreed with the recommendation. Management will review the Federal PKI Policy Authority meeting minutes to determine if there are any policy changes and, if so, will update the Certificate Policy and Certification Practice Statements documents as required. Additionally, they will conduct a quarterly review of implemented changes to ensure consistency between the Certificate Policy, Certification Practice Statements, and operations of the external PKI environment. See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

The U.S. Postal Service Office of Inspector General considers management's comments responsive to the recommendation and the 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: Deborah J. Judy
Charles L. McGann, Jr.
Corporate Audit and Response Management

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. PKI relies on the exchange of digital certificates between authenticated users and trusted resources. A Certification Authority is an essential component of the Microsoft PKI solution. In a Windows Server 2003 network, a Certification Authority is a Windows Server 2003 computer with Certificate Services installed. A Certification Authority issues certificates to users, computers, and services and manages those certificates.

To support PKI-enabled applications, an organization must design and implement the Certification Authority hierarchy. Common roles in a Certification Authority hierarchy include a root, policy, and an issuing Certification Authority. The Postal Service's external PKI[1] consists of a root, an intermediate, and two subordinate Certification Authorities.

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

Homeland Security Presidential Directive 12 established a federal policy[2] 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 Homeland Security Presidential Directive 12 credential the government issues to contain an external digital certificate. As a result, the Postal Service created a Certification Authority 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 is an interagency body established under the Chief Information Officers Council to enforce digital certificate

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

standards for trusted identity authentication across federal agencies and among federal agencies and outside bodies. The Federal Bridge Certification Authority is an information system that facilitates an entity accepting certificates issued by another entity for a transaction.

In support of Homeland Security Presidential Directive 12, the Federal Public Key Infrastructure Policy Authority approved the Postal Service's external PKI for cross-certification in April 2008 at a [redacted] hardware level. The Federal Public Key Infrastructure Policy Authority requires a full and complete compliance audit of all mandatory criteria to serve as the baseline for the triennial audits. We conducted this audit to ensure the Postal Service's external PKI services continue to operate at a level to remain cross-certified with the Federal Bridge Certification Authority.

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] To accomplish the objective, we evaluated whether:

- The Postal Service's Root, Intermediate, and Subordinate Certification Practice Statements conformed to the Postal Service's Certificate Policy.

- PKI operations complied with requirements in the Root, Intermediate, and Subordinate Certification Practice Statements.

We performed a compliance audit of all mandatory criteria as stated in the *FPKIPA Triennial Compliance Audit Requirements*. Mandatory criteria includes a review of all procedures and controls; previous compliance audit findings for associated changes and corrective actions; and all changes to policies, procedures, personnel, and system and technical aspects since the previous compliance audit.

We used the following Postal Service policy documents as criteria to evaluate whether PKI policies conformed to PKI policies and whether PKI operations complied with PKI policy:

- *United States Postal Service Public Key Infrastructure (PKI) X.509 Certificate Policy (CP)*, Version 1.68, dated March 8, 2010, last updated August 12, 2010.

- *United States Postal Service Root Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.

- *United States Postal Service Intermediate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.

- *United States Postal Service Subordinate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.

  - Handbook AS-805*, Information Security,* dated November 2009.

To validate conformance, we interviewed staff to discuss policies and compared statements in the Certification Practice Statements to corresponding statements in the Certificate Policy to determine whether the statements were the same or different.

To validate operations, we observed operations and interviewed PKI personnel to determine if actual practices and procedures were as stated in the Certification Practice Statements.

To validate that management had taken corrective action on the FY 2009 PKI compliance audit recommendation, we verified the status during fieldwork and determined that management implemented the recommendation.

We conducted this performance audit from February through September 2010 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 August 30, 2010, 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-09-012	9/18/2009	The Postal Service was effectively managing its PKI services in compliance with established guidance as stated in their Certificate Policy and Certification Practice Statements. However, we identified and management corrected 10 instances of non-compliance between the Postal Service's PKI policies and its external PKI environment. Management agreed with our recommendation and stated they will review and compare the Certificate Policy and Certification PS documents for accuracy and consistency by February 2010. During the FY 2010 audit, we verified that management successfully implemented the FY 2009 recommendation.
Compliance Audit of the Postal Service's External Public Key Infrastructure Services	IS-AR-08-017	9/11/2008	The Postal Service was effectively managing its PKI services in compliance with established guidance as stated in their Certificate Policy and Certification Practice Statements. However, we identified [redacted] 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 [redacted] Management agreed with our recommendation and stated they would establish milestones to implement resolutions 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. This project is closed.
Compliance Audit of the Postal Service's External Public Key Infrastructure Services	IS-AR-08-001	10/5/2007	In general, the Postal Service's external PKI environment complies with their Certificate Policy, Certification Practice Statements, and any applicable Memorandums 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. This project is closed.

Report Title	Report Number	Final Report Date Report	Results
Information for the Federal Bridge Certification Authority	IS-WP-07-001	10/2/200 6	The Postal Service's PKI operations, as of September 1, 2006, conformed to the Certification Practice Statements documents. This project is closed.
Certificate Authority Public Key Infrastructure Compliance [redacted]	IS-AR-06-015	9/1/2006	We performed a follow-up audit and reviewed items identified in a March 2006 audit performed by Klynveld Peat Marwick Goerdeler LLP. 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 back-up environment. Management agreed with the recommendation and stated that the completion date for the PKI back-up site was September 1, 2006. This project is closed.

APPENDIX B: DETAILED ANALYSIS

Postal Service PKI Policies and PKI Environment

There were [redacted] instances where the operations of the Postal Service's external environment did not conform to the requirements of the Certificate Practice Statements. For example:

- The Corporate Information Security Office roles and responsibilities memorandum for the Homeland Security Presidential Directive 12 project did not contain the PKI auditor's role listed in the Certificate Policy and Root, Intermediate, and Subordinate Certification Practice Statements'.

- PKI personnel [redacted] ensuring proper documentation as stated in the Root, Intermediate, and Subordinate Certification Practice Statements.

- The Root and Intermediate servers [redacted] therefore the [redacted] as stated in the Root and Intermediate Certification Practice Statements, was not valid.

- Power and air conditioning back-up power capabilities were inaccurately stated in the Certificate Policy and the Root, Intermediate, and Subordinate Certification Practice Statements.

Additionally, we found [redacted] instances of documentation inconsistencies in the Certification Practice Statements which did not provide sufficient detail to support corresponding Certificate Policy requirements. For example, the Subordinate Certification Practice Statements was missing a paragraph regarding registration authorities which was included in the Certificate Policy. Further, statements were missing in the Root and Intermediate Certification Practice Statements concerning the Certificate Revocation List scheduling details as included in the Certificate Policy.

Management placed limited focus on reviewing PKI policies because the Postal Service is not actively issuing certificates in this environment. Operating the external PKI environment in compliance with policies and consistent documentation maintains cross-certification and improves the understanding of policies.

In Table 1, we summarized the results of our review of the Postal Service's Certificate Policy and Certification Practice Statements documents. All 4,261 items we reviewed were compliant at the time we issued this report.

Table 1 – Status of Compliance

Status of Items Reviewed	Items Reviewed	Percentage
Compliant with environment	4,236	99.4%
Non-compliant items corrected	25	0.6%
Non-compliant items outstanding	0	0.0%
Total items reviewed	4,261	100.0%

APPENDIX C: MANAGEMENT'S COMMENTS

ROSS PHILO
EXECUTIVE VICE PRESIDENT
CHIEF INFORMATION OFFICER

UNITED STATES POSTAL SERVICE

September 7, 2010

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

SUBJECT: Draft Audit Report – Review of the Postal Service's External Public Key Infrastructure Services – FY 2010 (Report Number IS-AR-10-XXX)

Thank you for the opportunity to review and comment on the subject draft audit report. We have attached our response for recommendation number one.

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.

for Ross Philo

Attachment

cc: Charles L. McGann
Jamie Gallagher

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

We recommend the executive vice president and chief information officer direct the manager, Corporate Information Security, to:

1. Develop procedures to ensure reviews of applicable policies and processes are performed following changes to the Postal Service's external Public Key Infrastructure environment.

Management Response

Management agrees with the recommendation. Federal PKI Policy Authority conducts regularly scheduled meetings to discuss and vote on policy changes. Minutes of these meetings are published on the FPKIPA Web site. USPS CA will review the minutes and update USPS CP and CPS documentation, as required. USPS CA will conduct a quarterly review of implemented changes to ensure consistency between the USPS CP, CPSs, and operations of the external PKI environment.

Anticipated completion date: April 30, 2011

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

The auditor letter of compliance and background information required for the Federal Public Key Infrastructure Policy Authority begins on the next page.

September 15, 2010 R eport Number: IS-AR-10-013

ROSS PHILO
CHIEF INFORMATION OFFICER AND EXECUTIVE VICE PRESIDENT

SUBJECT: External Public Key Infrastructure Services

We performed an audit to determine whether 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 remain certified with the U.S. Government's Federal Bridge Certification Authority.

Audit Methodology

We conducted this audit from February through September 2010 in accordance with generally accepted government auditing standards. As recommended by the Federal Public Key Infrastructure Policy Authority Triennial Compliance Audit Requirements, we performed a full and complete compliance audit of all mandatory criteria. Mandatory criteria includes a review of all procedures and controls; previous compliance audit findings for associated changes and corrective actions; and all changes to policies, procedures, personnel, and system and technical aspects since the previous compliance audit.

Documents and Criteria

We used the following Postal Service policy documentation as criteria during our audit:

- *United States Postal Service Public Key Infrastructure (PKI) X.509 Certificate Policy (CP)*, Version 1.68, dated March 8, 2010, last updated August 12, 2010.
- *United States Postal Service Root Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.
- *United States Postal Service Intermediate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.

- *United States Postal Service Subordinate Certification Authority (CA) Certification Practice Statement (CPS)*, Version 1.20, dated March 8, 2010, last updated August 12, 2010.

- Handbook AS-805, *Information Security,* dated November 2009.

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

As of September 15, 2010, the Postal Service effectively managed its external PKI environment in compliance with established guidance. We reviewed [redacted] external PKI components documented in the criteria documented above. Although we found [redacted] instances of non-compliance, which management corrected during our audit, we considered them insignificant to the overall external PKI environment.

The attachment to this letter contains the identities 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: Deborah J. Judy
Charles L. McGann, Jr.

Background for Federal Public Key Infrastructure Policy Authority Auditor 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 E. Cain
Michael Blaszczak
Maria Gomez
David Horton
Ursula Sundre
Kimberly Jones
Ruth Smolinski

Competence of the Auditors:

Darrell Benjamin, Jr., CPA, CIA, 21 years of audit experience
Frances E. Cain, CISA, 18 years of audit experience
Michael Blaszczak, CISA, CIPP, 14 years of audit experience
Maria Gomez, CISA, CIA, 11 years of audit experience
David Horton, CISSP, CEH, 10 years of audit experience
Ursula Sundre, CISA, 10 years of audit experience
Kimberly Jones, 10 years of audit experience
Ruth Smolinski, CISA, 4 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 and 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 operation of the Postal Service.