OFFICE OF INSPECTOR GENERAL
Washington, DC 20268-0001

Date: November 14, 2008

To: Dan G. Blair, Chairman

From: Jack Callender, Inspector General

Subject: Transmittal of Final Audit Report—FISMA Compliance and Information Security Controls
Report Number AR-08-02A-02

This report presents the results of our audit of the Postal Regulatory Commission's (PRC) compliance with the Federal Information Security Management Act (FISMA), as well as its implementation of information security controls recommended in our prior audit (Audit Report 07-02A-01).

Overall, the PRC made substantial progress in the past year towards full compliance with FISMA and towards implementing the recommendations of OIG's prior audit. Some areas in which PRC could make further progress are detailed in this report.

We appreciate the cooperation and courtesies provided by your staff during our audit. If you have any questions, please contact me at 202-789-6817.

cc: Vice Chairman Nanci E. Langley
Commissioner Ruth Y. Goldway
Commissioner Tony Hammond
Commissioner Mark Acton

POSTAL REGULATORY COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL AUDIT REPORT

FISMA COMPLIANCE AND INFORMATION SECURITY CONTROLS

Audit Report AR-08-02A-02

November 14, 2008

Table of Contents

Introduction

Background

The Federal Information Security Management Act (FISMA) (Title III of the E-Government Act)[1] provides a framework for securing government information technology (IT). FISMA requires each federal agency to develop, document, and implement an agency-wide information security program for information and information systems supporting agency operations and assets. As mandated by FISMA and the Office of Management and Budget (OMB)[2], the National Institute of Standards and Technology (NIST) develops standards and guidelines for providing adequate information security for federal agency operations and assets.

Each year, OMB collects information from agencies regarding IT Security and privacy management using common reporting templates. Some federal agencies[3] are required to complete annual FISMA reports and quarterly updates; others, including the PRC, complete only an abbreviated annual report.[4] Although it is only required to submit abbreviated reports, the PRC has the same compliance obligations as other federal agencies. We reviewed their current FISMA compliance status using OMB's full fiscal year (FY) 2007 and 2008 FISMA reporting templates as benchmarks. We also reviewed actions taken to address recommendations in our prior audit report, Information Technology Governance and Information Security Planning (Report No. 07-02A-01).

Objectives, Scope and Methodology

The objective of this audit was to determine if the PRC is in compliance with FISMA requirements and if IT-control issues in prior audits have been sufficiently addressed.

To accomplish our objective, we interviewed key PRC personnel and reviewed relevant policies, procedures and other documentation. In addition, we reviewed FY 2007 and 2008 FISMA reporting templates for large agencies, PRC's 2007 FISMA report, and the prior PRC audit report (Information Technology Governance and Information Security Planning, No. 07-02A-01) to determnine their current compliance status as well as actions taken to address recommendations in the prior audit report.

We conducted this performance audit from July through October, 2008 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. These standards require that we plan and

[1] Public Law 107-347, enacted December 17, 2002.
[2] Office of Management and Budget (OMB) Circular A-130, Section 8b (3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.
[3] Chief Financial Officer (CFO) Act agencies and agencies participating in the President's Management Agenda scorecard process (i.e., agencies with E-Government scorecards)
[4] As a federal agency that employs 100 or fewer FTEs, PRC uses OMB's Microagency Reporting Template to fulfill its annual FISMA and privacy reporting requirements.

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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We did not assess the reliability of computer-generated data. We discussed our observations and conclusions with management officials during the audit and on October 21, 2008.

Prior Audit Coverage

OIG conducted the most recent prior audit of information security management at the PRC and issued a final report, Information Technology Governance and Information Security Planning (PRC-OIG Report No. 07-02A-01) on January 30, 2008. OIG made five recommendations to PRC management: that the PRC complete a formal information security plan; implement an organizational structure with defined roles and responsibilities; develop formal information security policies and procedures; document PRC's enterprise architecture; and implement an ongoing monitoring plan with achievable and realistic goals. PRC management agreed with all five recommendations and committed to implementing each by specific dates.

Results

1. FISMA Compliance Status

The PRC made substantial progress in FY 2008 towards full compliance with FISMA and privacy requirements, although some progress remains to be made. This is due to PRC's challenge to ensure its IT systems support evolving business processes using existing, limited resources.

To ensure compliance with FISMA, federal agencies must protect their information, operations, and assets in accordance with National Institute of Standards and Technology (NIST) standards. This includes developing and maintaining an inventory of major information systems; providing information security for information and information systems supporting agency operations and assets; complying with minimally acceptable system configuration requirements; and developing a Plan of Action and Milestones (POA&M) process for planning, implementing, evaluating, and documenting remedial actions addressing deficiencies in information security policies, procedures, and practices. Federal agencies must also ensure personal identifiable information (PII) is safeguarded as required by the E-Government Act and the Privacy Act. This includes performance measures on managing sensitive information (including PII) and providing the URL of the centrally located page on its web site that list working links to Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).

The PRC prepared its FISMA report in FY 2007 using the more extensive reporting templates normally used by larger agencies. We identified the following twelve areas of concern in the 2007 report:

1. The PRC reported that it lacked a formal breach notification policy.

2. The PRC reported that it lacked a formal policy outlining rules of behavior and corrective actions for failure to protect personally identifiable information (PII).
3. The PRC reported that it had not met standards for testing of security controls for agency and contractor systems.
4. The PRC reported that it had not met standards for testing of contingency plans for agency and contractor systems.
5. The PRC reported that it lacked formal policies and procedures covering National Institute of Standards and Technology (NIST) Special Publications 800-53 and 800-53a.
6 The PRC reported that it had not developed formal tools, techniques, and technologies used for incident reporting.
7. The PRC reported that it had not provided Information Technology (IT) security awareness training for employees and contractors.
8. The PRC reported that it had not provided training on the security implications of peer-to-peer file sharing.
9. The PRC reported that it lacked formal policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement.
10. The PRC reported that it lacked formal procedures for using emerging technologies and countering emerging threats included in security policy.
11. The PRC did not provide information for three performance measures used for measuring the effectiveness or efficiency of security policies and procedures.
12. The PRC did not provide a URL location of an agency web site listing working links to Privacy Impact Assessments.

As a result of our review of PRC's current status on the items identified, we determined management has taken actions to address or partially address eleven of the twelve items. One item has not been addressed:

- Items 1, 3, 5, 6, 7, and 8 have been addressed,
- Items 2, 4, 9, 10, and 11 have been partially addressed, and
- Item 12 has not been addressed.

In addition, we reviewed PRC's compliance status for items newly included in the FY 2008 FISMA large agency reporting templates. New 2008 FISMA requirements cover the following areas:

- Privacy reviews conducted during the last fiscal year;
- Information about advice given by the Senior Agency Official for Privacy (SAOP) on formal written policies, procedures, guidance, or interpretations of privacy requirements issued by the agency;
- Number of written complaints for each type of privacy issue allegation received by the SAOP during the last fiscal year; and
- Number of complaints received by the SAOP for alleged privacy violations that were referred to another agency with jurisdiction.

We found the PRC has not conducted privacy reviews during the past year, although they maintain a database containing personally identifiable information. PRC management indicated they have not received any complaints during FY 2008 regarding its management of privacy information.

Although the PRC has made progress in strengthening its information security program, addressing and completing the following activities will ensure progress to an effective information technology security program and compliance with FISMA:

- Conduct privacy reviews;
- Test contingency plans for agency and contractor systems;
- Adhere to incident reporting policies and procedures;
- Document emerging technology and countering emerging threat procedures; and
- Provide working links to privacy impact assessments.

In addition, effectively managing sensitive information ensures the balance of the need to maintain information about PRC employees and customers, while protecting unwarranted invasions of their privacy.

2. Actions Taken On Prior Audit Recommendations

We reviewed actions taken by the PRC for five recommendations made in the prior audit report, Information Technology Governance and Information Security Planning (PRC-OIG Report No. 07-02A-01) and found management has addressed four of the recommendations. Specifically, the PRC has addressed recommendations two through five as follows:

- Implemented an organizational structure with defined roles and responsibilities.
- Implemented formal information security policies and procedures.
- Documented the enterprise architecture.
- Implemented an ongoing monitoring plan with achieval and realistic milestones for completion. However, PRC's Plan Of Actions and Milestones (POAM) does not reflect the mapping of specific program and system-level security weaknesses, remediation needs, resources required for implementation, and scheduled completions dates.

The PRC has not yet implemented formal security plans although their response to OIG recommendations indicated a completion date of June 30, 2008. A security plan should provide an overview of the security requirements of an information system and describe the controls in place or planned for meeting those requirements. Having documented security plans in place will help to ensure PRC's information systems are protected.

Recommendations

1. **We recommend the PRC continue to strengthen its information security program in accordance with the Federal Information Security Management Act.**

   Management Comments

   PRC Management provided a response to the draft of this audit report on October 31, 2009. A copy of that response is included as Appendix I of this report. Management agreed with this recommendation and committed to strengthen PRC's information security program on an ongoing basis.

   Evaluation of Management's Comments

   Management's comments are responsive to the recommendation, and the action taken or planned should correct the issue identified.

2. **We recommend the PRC revise its information technology Plan Of Actions and Milestones document to reflect the mapping of specific program and system-level security weaknesses, remediation needs, resources required for implementation, and scheduled completions dates; and ensure its actions are aligned with its long and short-term strategic goals and mission.**

   Management Comments

   Management agreed with this recommendation and committed to revise its Plan of Action and Milestones accordingly by June 30, 2009.

   Evaluation of Management's Comments

   Management's comments are responsive to the recommendation, and the action taken or planned should correct the issue identified.

3. **We recommend the PRC list its database maintaining personally identifiable information as a separate system in future FISMA reports.**

   Management Comments

   Management agreed to this recommendation and committed to include its administrative database as a separate system in future FISMA reports if the personally identifiable information contained in the database cannot be removed due to continual use for mission purposes.

Evaluation of Management's Comments

Management's comments are responsive to the recommendation, and the action taken or planned should correct the issue identified.

POSTAL REGULATORY COMMISSION

Office of the Secretary and
Administration

October 31, 2008

Jack Callender, Inspector General
Postal Regulatory Commission
901 New York Avenue, NW
Washington, DC 20268

Dear Jack:

The Commission is pleased to receive the guidance contained in your recently completed Audit Report Number AR-08-02A-02 on FISMA Compliance and Information Security Controls.

The Commission is pleased that you recognized the substantial progress and effort it has made towards full compliance with FISMA and privacy requirements during Fiscal Year 2008. The Commission intends to add links to its Privacy Impact Assessments to its web site, as mentioned on page 3, as soon as possible, but no later than the end of Fiscal 2009. In regards to your three formal recommendations:

- Recommendation 1: The Commission agrees to continue to strengthen its information security program in accordance with the Federal Information Security Management Act and recognizes Information Security is an ongoing and constant process.

- Recommendations 2: The Commission agrees and will revise its Plan Of Actions and Milestones (POAM) document to reflect the mapping of specific program and system-level weaknesses, remediation needs, resource required for implementation and scheduled completions dates. The Commission intends to accomplish this task by June 30, 2009. It will also strive to maintain an alignment of these actions and its long and short-term strategic goals and mission.

- Recommendation 3: The Commission agrees and if the Personally Identifiable Information contained in the "admin database" cannot be removed because of continual use for mission purposes, it will list it as a separate Information System beginning with Fiscal 2009 FISMA reports.

Sincerely,

Steven W. Williams