

# **POSTAL REGULATORY COMMISSION**

## **OFFICE OF INSPECTOR GENERAL**



### **FINAL REPORT**

## **INFORMATION SECURITY MANAGEMENT AND ACCESS CONTROL POLICIES**

**Audit Report 10-02-A01  
December 17, 2010**

# *Table of Contents*

---

<b>INTRODUCTION</b> .....	1
Background .....	1
Objectives, Scope, and Methodology .....	2
Prior Audit Coverage .....	3
<b>RESULTS</b> .....	3
Follow up on Prior Audit Recommendations .....	3
Recommendation 1 .....	4
Management’s Comments .....	5
Evaluation of Management’s Comments .....	5
Recommendation 2 .....	5
Management’s Comments .....	6
Evaluation of Management’s Comments .....	6
Access Controls .....	6
Recommendation 3 .....	7
Management’s Comments .....	7
Evaluation of Management’s Comments .....	7
<b>APPENDIX A</b> .....	8
<b>APPENDIX B</b> .....	10

# *Introduction*

---

## **Background**

This document presents the results of our follow up audit on Federal Information Security Management Act (FISMA) compliance activities and access controls in the Postal Regulatory Commission's (PRC) information security policy.<sup>1</sup> Our objective was to determine whether the control issues identified and recommendations made in the 2008 FISMA audit have been sufficiently addressed, and whether the PRC Information Technology (IT) security policy is adequate to prevent unauthorized access to PRC data and resources.

In a November 2008 report to the PRC Chairman,<sup>2</sup> the PRC Office of Inspector General (OIG) presented the results of our audit work on compliance with FISMA and implementation of security controls. The November 2008 report identified twelve areas of concern related to FISMA compliance and included three recommendations to strengthen its security information program, revise its IT Plan of Actions and Milestones (POAM) document, and list its database containing Personally Identifiable Information (PII) as a separate system in future FISMA reports. In an April 2010 report,<sup>3</sup> the PRC OIG presented the results of audit work on physical access controls related to the handling of non-public information in response to requests by Congress and the PRC Chairman. Subsequent to this report, Congress expressed an interest in controls the PRC has implemented to protect sensitive information provided by the U.S. Postal Service. During this audit, we reviewed follow-up activities addressing recommendations in the November 2008 report and the adequacy of access controls in PRC's information security policy.

FISMA (Title III of the E-Government Act)<sup>4</sup> provides a framework for securing government information technology. FISMA requires federal agencies to develop, document, and implement an enterprise-wide program to provide information security for the information and its systems that support the operations and assets of the agency.

FISMA requires micro agencies<sup>5</sup> to submit information on their system's inventory, as well as the status of its certification and accreditation program. In addition, micro agencies must submit information on the status of security configuration management, incident response and reporting, security training, plans of action and milestones, remote access, account and identity management, continuous monitoring, contingency planning, as well as oversight of contractor's systems. Micro agencies, including PRC, must submit FISMA annual report information via CyberScope.<sup>6</sup>

---

<sup>1</sup> *Postal Regulatory Commission Information Security Policy*, Version 1.7, dated March 17, 2008.

<sup>2</sup> *FISMA Compliance and Information Security Controls*, Report Number AR-08-02A-02, dated November 14, 2008.

<sup>3</sup> *Postal Regulatory Commission's Handling of Non-Public Information*, Report Number 10-01-A01, dated April 10, 2010. The PRC-OIG conducted this audit with assistance from the Inspections and Evaluation Staff of the Treasury Inspector General for Tax Administration.

<sup>4</sup> Public Law 107-347, Title III – Information Security, Section 301, Subsection 3541, enacted December 17, 2002.

<sup>5</sup> Micro agencies employ 100 or fewer full time employees.

<sup>6</sup> CyberScope is the platform for the FY 2010 FISMA submission process.

OMB policies require federal agencies to follow National Institute of Standards and Technology (NIST). Because of FISMA, NIST has implemented the FISMA Implementation Project, which promotes the development of key security standards and guidelines to support the implementation of and compliance with FISMA. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. NIST publishes the Federal Information Processing Standards, which governs the minimum security requirements. The minimum security requirements cover 17 security-related areas designed to protect the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems. Access control is one of the 17 security requirements and requires organizations to limit information system access to authorized users, as well as processes acting on behalf of authorized users. NIST access controls also require organizations to limit information system access to the types of transactions and functions that authorized users are permitted to exercise. Organizations are also required to develop, disseminate, and review/update a formal and documented access control policy. Access control areas include, but are not limited to, authorizations for logical access, separation of duties, least privilege, unsuccessful login attempts, and encryption. Additionally, organizations should establish personnel security requirements including security roles and responsibilities for third-party providers and monitor provider compliance. Third-party providers include contractors and other organizations providing information system development, IT services, and network and security management.

## **Objectives, Scope, and Methodology**

Our audit objectives were to determine whether the control issues identified and recommendations made in the 2008 FISMA audit have been sufficiently addressed, and whether the PRC's IT security policy is adequate to prevent unauthorized access to PRC data and resources.

To accomplish our objectives, we interviewed key PRC personnel and reviewed relevant policies, procedures, and other documentation. We reviewed fiscal years 2008, 2009, and 2010 FISMA reporting requirements, the PRC's 2008 annual FISMA report submitted to OMB, as well as the January 2008 and April 2010 prior audit reports. We also reviewed the PRC's security plan, performance metrics, Continuity of Operations Plan (COOP), intrusion reports, and other relevant documents to determine actions taken to address the issues and recommendations in the November 2008 audit report. We reviewed the PRC's information security policy as well as various NIST publications related to access controls and encryption. We compared the *Postal Regulatory Commission Information Security Policy* to NIST access controls and Postal Service's Handbook AS-805, *Information Security*.

An audit team on detail from the United States Postal Service OIG conducted this performance audit from June through December 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations

and conclusions with management officials on November 18, 2010, and included their comments where appropriate.

We did not assess the reliability of computer generated data.

## **Prior Audit Coverage**

*Postal Regulatory Commission's Handling of Nonpublic Information* (Report Number 10-01-A01 dated April 30, 2010). PRC OIG made two recommendations to PRC management regarding the development of a formal training program on security requirements for safeguarding non-public information, and the development of a method of reporting security incidents related to nonpublic information. The PRC made a commitment to implement these recommendations.

*FISMA Compliance and Information Security Controls* (Report Number AR-08-02A-02 dated November 14, 2008). PRC OIG made three recommendations to PRC management to strengthen its information security program, revise its information technology Plan of Actions and Milestones document, and list its database containing PII as a separate system in future FISMA reports. PRC management agreed with all the recommendations.

*Information Technology Governance and Information Security Planning* (Report Number 07-02A-01 dated January 30, 2008). PRC-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.

## ***Results***

---

The PRC is progressing in some areas of its IT security program. However, the PRC has not sufficiently addressed the areas of concern and fully implemented recommendations one and two identified in our November 2008 audit report. In addition, access controls in PRC's information security policy could be strengthened by aligning the policy with NIST access control standards.

### **Follow up on Prior Audit Recommendation**

While the PRC made progress to address the three recommendations listed in the November 2008 audit report, recommendations one and two remain open.

The November 2008 audit report listed twelve areas of concern, six of which the PRC addressed before the final report was issued. In response to the prior report first recommendation, the Commission agreed to continue to strengthen its information security program in accordance with FISMA. However, our follow up review determined that the PRC has not taken action to address concerns in four areas:

- The PRC's PII Breach Notification Policy<sup>7</sup> does not address rules of behavior and corrective actions for failure to protect PII as required by the Office of Management and Budget (OMB) policy.<sup>8</sup> PRC management acknowledged the omission and indicated that this is due to recent turnover in PRC IT personnel.
- PRC has not completed the implementation of its incident policy or procedures for reporting security incidents to the Computer Emergency Response Team in accordance with FISMA requirements and NIST standards.<sup>9</sup> Although the PRC revised its incident reporting guidelines from the draft version we reviewed in the 2008 audit, these guidelines remain in draft. PRC management has not approved these policies because PRC IT has not completed their penetration testing of the PRC network.
- The PRC has not finalized their COOP or conducted the final testing of the COOP. This occurred because the PRC rate adjustment hearings took priority, and the network could not be disrupted while the hearings were being conducted. Policy<sup>10</sup> requires the development and testing of a contingency plan.
- The three performance metrics<sup>11</sup> PRC identified to measure the effectiveness and efficiency of security policies and procedures were not different from the ones used in the FISMA reporting instructions. FISMA<sup>12</sup> requires agencies to develop three performance metrics used to measure effectiveness and efficiency of security policies and procedures. These metrics must be different from the ones used in the FISMA reporting instructions. This occurred because management was not aware of this requirement.

Addressing these four issues will strengthen the PRC's information security program and improve the protection of sensitive information.

We recommend the Postal Regulatory Commission:

1. Continue to strengthen its information security program in accordance with the Federal Information Security Management Act by:
  - addressing rules of behavior and corrective actions for failure to protect personally identifiable information in its Personally Identifiable Information Breach Notification Policy;

---

<sup>7</sup> Personally Identifiable Information Breach Notification policy dated October 3, 2008.

<sup>8</sup> OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, Attachment 4: Rules and Consequences, dated May 22, 2007.

<sup>9</sup> NIST Special Publication 800-53 Revision 3, *Information Security*, dated August 2009, pages F63 and F64.

<sup>10</sup> NIST Special Publication 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, dated May 2010; NIST Special Publication 800-53 Revision 3, *Information Security*, dated August 2009, and Postal Rate Commission, *Information Security Policy* dated March 17, 2008.

<sup>11</sup> The PRC identified their three performance metrics as (1) number of incidents, (2) number of attempts, and (3) response relating to intrusion incidents.

<sup>12</sup> OMB M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009. Chief Information Officer Questions, Question 9: Performance Metrics for Security Policies and Procedures, Question 4: Incident Detection, Monitoring, and Response Capabilities; and Question 8: Incident report.

- completing the implementation and finalizing its incident policy or procedures for reporting security incidents to the National Computer Emergency Response Team;
- finalizing and conducting tests of their Continuity of Operations Plan; and
- developing the performance metrics for effectiveness and efficiency of security policies and procedures.

### Management's Comments

PRC Management provided a response to a draft of this audit report on December 15, 2010. A copy of that response is included as Appendix B of this report. Management agreed with this recommendation and committed to implement the four items above by June 3, 2011.

### Evaluation of Management's Comments

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

In response to the 2008 audit report second recommendation, the Commission agreed to revise its POAM to reflect the mapping of specific program and system-level security weaknesses, remediation needs, resources required for implementation, and scheduled completion dates; and to ensure its actions are aligned with its long and short-term strategic goals and mission. The target completion date was June 2009.

Our follow up review noted the progress PRC has made from its 2008 POAM to address specific program and system-level security weaknesses, remediate its needs, and identify resources required for implementation, as required by FISMA.<sup>13</sup> Overall, PRC has completed 73% of the items listed in the 2010 POAM while 27% of the items are in progress. However, we also noted that the PRC does not consistently document completion or anticipated completion dates in the POAM. For example, the PRC has not documented completion dates for any of the 46 completed items in the 2010 POAM. This occurred because of recent turnover in PRC IT personnel.

Completion of the POAM will ensure PRC's actions are aligned with its long and short term strategic goals and mission.

We recommend the Postal Regulatory Commission:

2. Complete the Information Technology Plan of Actions and Milestones to reflect scheduled completion dates to ensure its actions align with its long and short-term strategic goals and mission.

---

<sup>13</sup> OMB M-09-29, pages 9 and 12.

### Management's Comments

Management agreed with this recommendation, and committed to updating its POAM by June 3, 2011.

### Evaluation of Management's Comments

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

In response to the 2008 audit report third recommendation, the PRC agreed to list its database containing PII as a separate system in future FISMA reports if they could not remove PII from the database due to continual use for mission purposes. We were unable to determine whether the PRC listed its database<sup>14</sup> as a separate system because the PRC has not filed their 2009 annual FISMA report with OMB. In addition, PRC has not removed the PII from the database. Policy states all information systems should be included as part of the FISMA report.<sup>15</sup> This oversight occurred because the PRC has experienced a recent turnover in their IT staff.

Effectively managing sensitive information ensures controls are in place to protect employee privacy.

**Corrective Action:** The PRC listed the database containing PII in its 2010 annual FISMA report; therefore, we will not make a recommendation.

## Access Controls

The PRC information security policy addresses 10 of the 16 access controls standards required by NIST. However, the policy only partially addresses five standards and one standard is not addressed. This occurred because recent turnover of PRC IT personnel resulted in delays in updating the security policy. In addition, we noted that the PRC information security policy addresses six related identification<sup>16</sup> and authentication<sup>17</sup> controls required by NIST.

NIST provides access control standards for low, moderate and high impact systems as defined by Federal Information Processing Standards.<sup>18</sup> We reviewed the 16 NIST baseline access controls for all system impact levels along with the seven accompanying enhanced controls for moderate and high impact systems. The PRC has categorized its information and information systems as moderate and high, which requires compliance with baseline controls and applicable enhanced controls. See Appendix A for details on our review of PRC's information security policy compliance.

---

<sup>14</sup> The Admin Database is a Microsoft Access file that maintains employee information including PII.

<sup>15</sup> OMB M-09-29, *FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, dated August 20, 2009 and CIO Questions Attachment.

<sup>16</sup> Identification is the process of associating a person or information resource with a unique enterprise wide identifier (for example, a user logon ID).

<sup>17</sup> Authentication is the process of verifying the claimed identity of an individual, workstation, or originator.

<sup>18</sup> Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, dated February 2004.



We also compared the PRC information security policy to the Postal Service Handbook AS-805, *Information Security*, to benchmark the Postal Service's access control policy.<sup>19</sup> While the PRC information security policy includes most of the security controls listed in Handbook AS-805, it only partially addresses remote access, wireless access, and minimum standards for encryption. The PRC policy also does not state whether laptops and notebook computers are or should be encrypted. In addition, the PRC information security policy does not define personal identification numbers, smart cards and tokens, or biometrics. The PRC is not required to follow Postal Service Handbook AS-805; therefore, we are not making a recommendation.

The implementation of access controls protects the confidentiality and integrity of information from unauthorized users.

We recommend the Postal Regulatory Commission:

3. Update the PRC Information Security Policy to reflect access controls that align with National Institute of Standards and Technology access control standards.

#### **Management's Comments**

Management agreed with this recommendation and committed to update its information security policy by June 3, 2011.

#### **Evaluation of Management's Comments**

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

---

<sup>19</sup> Postal Service Handbook AS-805, *Information Security*, dated November 2009.

**APPENDIX A: DETAILED ANALYSIS**

**Access Controls**

Table 1. PRC Compliance with NIST Access Controls.

NIST STANDARDS		PRC INFORMATION SECURITY POLICY STATUS					
Control	Code	Baseline Addressed			Enhancements Addressed		Details
		Yes	Partially	No	Yes	Partially	
1. Access Control Policy and Procedures	AC-1	X					
2. Account Management*	AC-2	X				X	a) Temporary and emergency accounts are not specifically identified or addressed. b) The policy does not indicate the access will be automatically terminated after a defined period.
3. Access Enforcement	AC-3	X					
4. Information Flow Enforcement	AC-4	X					
5. Separation of Duties	AC-5	X					
6. Least Privilege *	AC-6	X				X	The policy does not state users of information system accounts, or roles with access to defined/specific security functions or security-relevant information are required to use non-privileged accounts (for example, accounts with read-only access), or roles, when accessing other system functions.
7. Unsuccessful Login Attempts	AC-7	X					
8. System Use Notification	AC-8	X					

NIST STANDARDS		PRC INFORMATION SECURITY POLICY STATUS					Details
Control	Code	Baseline Addressed			Enhancements Addressed		
		Yes	Partially	No	Yes	Partially	
9. Concurrent Session Control	AC-10		X				The policy does not address limitations on the number of concurrent sessions allowed by the information systems as required. Rather, it indicates the information resource must provide the administrator-configurable capability to limit the number of concurrent logon sessions for a given user.
10. Session Lock	AC-11	X			X		
11. Permitted Actions without Identification or Authentication *	AC-14	X			X		
12. Remote Access *	AC-17	X			X		
13. Wireless Access *	AC-18		X		X		The policy does not specifically cover the enforcement of wireless connections to information systems.
14. Access Control for Mobile Devices *	AC-19	X			X		
15. Use of External Information Systems *	AC-20	X				X	The policy does not: a) address approved information system connection or processing agreements with organizational entities hosting external information systems; b) provide specific limitations on the use of their portable storage media by authorized individuals on external information systems.
16. Publicly Accessible Content	AC-22			X			The policy does not contain specific language that addresses this control.

\*These access controls include baseline and enhancement controls.

**APPENDIX B: MANAGEMENT RESPONSE**



POSTAL REGULATORY COMMISSION  
Washington, DC 20268-4001

Office of the Secretary

December 15, 2010

Mr. Jack Callender  
Inspector General  
Postal Regulatory Commission  
901 New York Avenue, N.W.  
Washington, DC 20268

Re: Transmittal of Draft Audit Report — Information Security Management and Access Control Policies Report Number 10-02-A01

Dear Mr. Callender,

Thank you for the opportunity to review the December 7, 2010, Draft Audit Report of the Information Security Management and Access Control Policies 10-02-A01.

The Commission agrees with the recommendation to continue to strengthen the information security program in accordance with the Federal Information Security Management Act (FISMA) and will take the following action:

- Update Breach Policy to include rules of behavior and corrective actions for failure to protect PII. Completion Date June 3, 2011.
- Finalize the incident Policy to include the requirements and procedure for reporting incidents to US-CERT. Completion date: Date June 3, 2011.
- Finalize testing of COOP site. Completion Date: Date June 3, 2011.
- Develop performance metrics for effectiveness and efficiency of security policy and procedure as outlined by NIST. Completion Date: June 3, 2011.


The Commission agrees with the recommendation to include completion dates on all Plan of Actions and Milestones and will take the following action:

- Update the POAM to include completion dates on all items. Completion Date: Date June 3, 2011.

The Commission agrees with the recommendation to update the Information Security Policy to align with NIST access control standards as they apply to micro-agencies.

- Update the Postal Regulatory Commission Information Security Policy. Completion Date: Date June 3, 2011.

We do not find any portion of this report exempt from the provisions of the Freedom of Information Act. The Commission appreciates your efforts and assistance in this matter.



Shoshana Grove,  
Secretary and Chief Administrative Officer