POSTAL REGULATORY COMMISSION

OFFICE OF INSPECTOR GENERAL

FINAL AUDIT REPORT

INFORMATION TECHNOLOGY GOVERNANCE AND INFORMATION SECURITY PLANNING

Audit Report 07-02A-01
January 30, 2008

Digitally signed by Jack Callender
DN: cn=Jack Callender, o=PRC, ou=OIG,
email=prc-ig@prc.gov, c=US

JACK CALLENDER
INSPECTOR GENERAL

TABLE OF CONTENTS

PAGE

EXECUTIVE SUMMARY 1

INTRODUCTION 2

Background 2

Objectives, Scope and Methodology 3

RESULTS 4

Information Security Plans 5

Information Security Policies and Procedures 6

Ongoing Monitoring 6

RECOMMENDATIONS 7

GLOSSARY 9

AGENCY RESPONSE 12

EXECUTIVE SUMMARY

Introduction

We audited the Postal Regulatory Commission's (PRC) information technology governance and information security planning to assess and ensure that the PRC is taking a proactive approach in managing risk by aligning PRC's information security plan to overall agency strategic plans, planning an organizational structure with clearly identified roles and responsibilities with regard to information security, planning to develop secure enterprise architecture and planning to document security objectives. The PRC has taken the initiative to adhere to the Federal Information Security Management Act (FISMA) of 2002, Title III of the E-Government Act (Public Law 107-347), which requires that all federal agencies develop and implement an agency-wide security program to safeguard Information Technology (IT) assets and data of the respective agency.

Results in Brief

PRC has taken a proactive approach concerning its information security governance. However, the PRC does not have a formal comprehensive information security plan that identifies management objectives. It has failed to identify an organizational structure and associated roles and responsibilities. The PRC has not identified an enterprise architecture that describes the current and future structure and identifies expected user behavior. It does not have formal information security policies and procedures that identify appropriate security controls required to ensure the security of its information assets. Finally, the PRC has not established an ongoing monitoring plan with milestones for completion to ensure that its objectives are achieved.

Summary of Recommendations

The PRC should continue to support preparation, completion and final approval of a formal information security plan; implement an organizational structure with defined roles and responsibilities; implement formal information security policies and procedures; document the enterprise architecture and implement an ongoing monitoring plan with achievable and realistic milestones for completion.

INTRODUCTION

Background

The Postal Regulatory Commission (PRC) was established by the Postal Accountability and Enhancement Act of 2006 (PAEA), (Public Law 109-435), enacted on December 20, 2006. Like most federal agencies, the PRC relies on information technology (IT) to run its operations and to provide public access to PRC proceedings and Postal Service information.

The National Institute of Standards and Technology (NIST) [1] defines information security governance as ***"the process of establishing and maintaining a framework and supporting management structure and processes to provide assurance that information security strategies are aligned with and support business objectives; are consistent with applicable laws and regulations through adherence to policies and internal controls; and provide assignment of responsibility, all in an effort to manage risk"***. [2]

An agency's information security governance structure should ensure that information security controls support its mission in an appropriate and cost-effective manner, while managing evolving information security risks. Title III of the E-Government Act of 2002 (Public Law 107-347), the Federal Information Security Management Act[3] (FISMA) requires that all federal agencies develop and implement an agency-wide security program[4] designed to safeguard the agency's IT assets and data. Relevant laws and regulations place the responsibility and accountability for information security at all levels within federal agencies from the agency head to each Information Technology (IT) user. Based on these laws and regulations, NIST has developed a body of standards, guidance and practices for agencies to follow. PRC management has made a commitment to meeting FISMA's requirements.

[1] NIST is the standards-defining agency of the U.S. government, formerly the National Bureau of Standards. It is one of three agencies that fall under the Technology Administration (www.technology.gov), a branch of the U.S. Commerce Department that is devoted to advancing American economic growth using technology. (www.nist.gov)

[2] Special Publication 800-100, Information Security Handbook: A Guide for Managers, provides an overview of information security elements that managers can understand, establish and implement as an effective information security program.

[3] FISMA encourages federal agencies to understand their information systems and sets forth specific requirements that the agency's information security program should abide by or stipulate rationale as to why the agency could not adhere to these standard requirements.

[4] A "security program" to be effective must: (a) provide for periodic assessment of risk; (b) implement policies and procedures that are based on the risk assessment; (c) provide plans for information security for the organization's networks, facilities, and information systems; provide security awareness training; (d) provide for the performance of periodic testing and evaluation, as well as planning, implementing, evaluating and documenting remedial activities of the information security policies, procedures, practices and security controls; (e) provide procedures for detecting and reporting incidents; and (f) plan for the assurance of continuity.

In order for information security governance to be effective, management's planning should include identifying the agency's IT assets, assigning values to the assets, documenting, developing and then implementing security policies, procedures, standards and guidelines that provide for the integrity[5], confidentiality[6] and availability[7] of these assets. In addition, the PRC's information security governance structure should support the overall mission and strategic plans of the organization. The key components of an information security governance structure are illustrated in Figure 1.

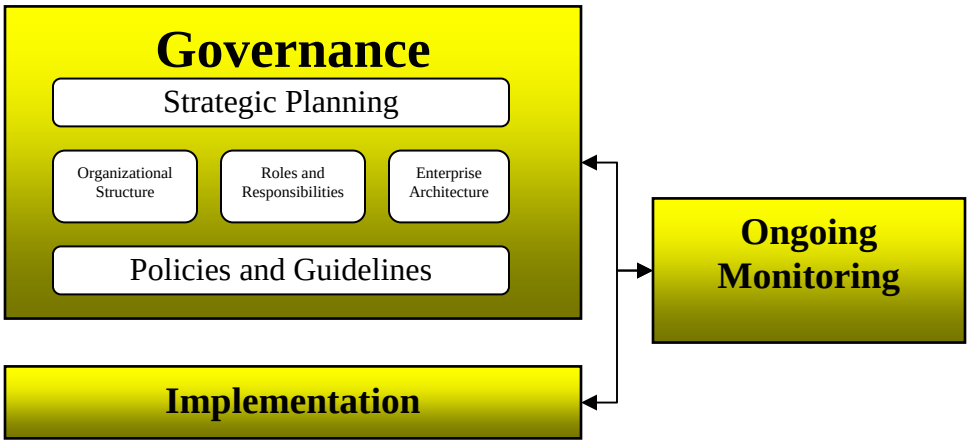

Figure-1 Information Security Governance Components
NIST Special Publication 800-100[8]

Objectives, Scope and Methodology

The purpose of this audit is to ensure that the Postal Regulatory Commission is taking a proactive approach in managing risk by aligning its information security plans and governance structure with the agency's overall mission, goals and objectives to ensure thorough information security planning. We relied on the PRC to provide its information security plans including: (i) plans for an organizational structure which identifies specific roles and responsibilities for information and information assets; (ii) plans for agency-wide security policies and procedures for ensuring that management objectives for information and information technology are being maintained; (iii) plans for enterprise architecture that is secure and protected both internally and externally against loss or

[5] Integrity is defined as the guarding against improper modification or destruction and includes ensuring information non-repudiation and authenticity.
[6] Confidentiality is defined as the preservation of authorized restrictions on information access and disclosure including means for protecting personal privacy and proprietary information.
[7] Availability is defined as ensuring timely and reliable access to and use of information.
[8] National Institute of Standards and Technology, Information Security Handbook: A Guide for Managers. Special Publication 800-100 provides an overview of information security elements for managers.

misuse; and (iv) a Plan of Action and Milestones[9] (POA&M) from which to assess these ongoing monitoring efforts. We verified the existence or availability of this data and not the completeness or the specific controls effected.

RESULTS

The PRC has taken a proactive approach in the establishment of information technology governance and information security strategic planning. PRC should continue to establish and implement an information security governance program through the organization's growth and development that appropriately identifies and ensures the adequacy and effectiveness of security to the enterprise information assets. Effective information security planning and governance can be accomplished if the PRC ensures that:

- Information security is integrated with enterprise management, strategic planning, capital planning and enterprise architecture.
- Information security is implemented and maintained to meet any appropriate requirements, laws, regulations and PRC's organizational policies.
- Information security organizational structure is adequate as the PRC evolves with PAEA legislation requirements.
- Information security polices are communicated to all stakeholders at all levels of the PRC organization to ensure that individuals will be held responsible for their actions.
- Information security responsibilities are assigned to appropriately trained individuals.
- Improvement and performance of information security is performed through continuous monitoring.

Improvement and performance of information security is required through continuous monitoring. PRC has obtained through contract services: (i) an independent assessment and suggested approach on the development of PRC's strategic goals, organizational structure and development of job performance structure and criteria; and (ii) an independent risk evaluation and suggested guidance of security controls in accordance with NIST Special Publication 800-53. In addition, the PRC is working to ensure the enterprise architecture is secure as it progresses through re-engineering and redesigning of its Web site. PRC has not yet completed all of the appropriate components for an effective information security governance environment.

Although PRC management was responsive to requests for information regarding its information security plans, organizational structure, agency-wide security policies, management objectives for information technology and current enterprise architecture,

[9] POA&M's are used by management to assist in identifying, assessing, prioritizing and monitoring the progress of corrective efforts for security weaknesses found in programs and systems, as identified in NIST Special Publication 800-100.

many of these documents were not yet completed.

Information Security Plans

The PRC does not have written and approved security plans. The information security plans should provide an overview of the security requirements of the organization and further describe the controls planned for meeting these requirements. Formal security plans are important to any organization. An organization's security plan is management's communication mechanism that provides for the information security structure of the organization.

The security plan should serve as a guide to define the functional and divisional plans that include information systems and information technology. This written security plan should:

- Provide a framework for decisions and security of information and information assets;
- Provide a basis for more detailed planning.

The PRC should finalize a comprehensive information security plan and create security plans for each of its information systems. The PRC should seek guidance in the creation and finalization of its security plans through the standards, guidance and baselines as identified in:

- *Federal Information Processing Standards (FIPS) 200 Minimum Standard Security Requirements for Federal Information and Information Systems in seventeen security related areas;*
- *NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems;* and
- *NIST Special Publication 800-18, Rev-1, Guide for Developing Security Plans for Federal Information Systems,* Appendix A.

The PRC should ensure that the information security plans are sufficient and current to accommodate the information security environment, agency mission and operational requirements.

Organizational Structure

The information security plans should delineate the organizational responsibilities as well as the expected behavior of all who have access to the PRC's systems. The individual who assumes this role of managing and addressing security in the organization carries a significant and potentially critical responsibility that may include the performance of risk assessments to the implementation of security policies and procedures. The security plan should cover all aspects of the organization from human resource issues to specifically defining security duties and the PRC systems used in the organizational environment.

Roles and Responsibilities

PRC should create information security plans that, at a minimum, identify information security roles and responsibilities and provide a baseline of security controls and rules for exceeding the baseline. The roles and responsibilities should clearly identify PRC's expectations for user compliance and repercussions for noncompliance.

Enterprise Architecture

The PRC should continue to develop, document and identify its current enterprise architecture. The enterprise architecture should describe the current and future structure and behavior of an organization's processes, information systems and personnel that are aligned with the organization's core goals and strategic direction. A strong enterprise architecture process helps to determine if:

- The current architecture supports and adds value;
- Major changes or modifications to the architecture are necessary;
- The current architecture supports the PRC's goals.

Information Security Policies and Procedures

The PRC does not have formal written information security policies and procedures which identify agency practices, rules, laws and regulations and how the PRC chooses to manage, protect and distribute sensitive and non-sensitive information securely. Information security policies and procedures are essential to the organization's information security controls and should be developed by the PRC. Without written and approved information security policies and procedures in place, the PRC cannot ensure the continued availability, confidentiality and integrity of its information assets.

Ongoing Monitoring

The PRC does not have an ongoing monitoring process in place to ensure that its planned mission and objectives are on target and that the appropriate security controls are in place to protect the overall agency environment. PRC's information governance structure (i.e., security plans, organizational structure, roles and responsibilities) can be enhanced by an ongoing monitoring and assessment process ensuring its mission and objective are appropriate as originally planned. This ongoing review process also ensures that present information security controls do not become obsolete. It also provides for opportunities to discover the advent of new technologies that may better serve and support the agency in the future.

RECOMMENDATIONS

The PRC should continue to:

- *Support preparation, completion and final approval of a formal information security plan;*

  Management Response[10]

  Management agreed with our recommendation and stated that the security plan will supplement and support the Commission's IT security policy currently under review. The Commission plans to complete its information security plan by June 30, 2008.

  Evaluation of Management Response

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

- *Implement an organizational structure with defined roles and responsibilities;*

  Management Response

  Management agreed with our recommendation and stated that the PRC expects to implement an organizational structure with better defined roles and responsibilities by March 31, 2008.

  Evaluation of Management Response

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

- *Implement formal information security policies and procedure;*

  Management Response

  Management agreed with our recommendation and stated that the PRC has performed a risk assessment of its security controls that will be used as a foundation in formulating its security policy and plan to be implemented by June 30, 2008.

[10] Management's comments in their entirety are included in Appendix II of this report.

Evaluation of Management Response

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

- *Document the enterprise architecture;*

Management Response

Management agreed with our recommendation and stated that the PRC is researching and documenting the enterprise architecture of the existing information technology structure. The Commission expects to have a formal enterprise architecture structure prepared by first quarter 2009.

Evaluation of Management Response

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

- *Implement an ongoing monitoring plan with achievable and realistic milestones for completion.*

Management Response

Management agreed with our recommendation and stated that the Commission expects to implement a formal monitoring plan upon completion of the security policies by June 30, 2008.

Evaluation of Management Response

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

We appreciate the courtesies and cooperation extended during this audit. If you need additional information, please contact Jack Callender at (202) 789-6817.

APPENDIX I

GLOSSARY

ITEM	DESCRIPTION
Agency	Any executive department, government corporation, government controlled operation, or other establishment in the executive branch of the government, or any independent regulatory agency.
Federal Information Processing Standards (FIPS) Publications Series	Issued by the National Institute of Standards and Technology (NIST) FIPS are the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).
Federal Information Security Management Act (FISMA) of 2002	The FISMA Act is the primary legislation governing federal information security programs. It delegates to the National Institute of Standards and Technology (NIST) the responsibility to develop detailed information security standards and guidance for federal information systems with the exception of national security systems. FISMA also delegates to OMB the oversight of federal agencies' information security implementation. Further, FISMA provides the framework for securing federal government IT resources, including key federal government and agency roles and responsibilities, requiring agencies to integrate information security into their capital planning and enterprise architecture processes, requiring agencies to conduct annual information security reviews of all programs and systems, and reporting the results of those reviews to OMB. Enacted

	as Title III of the E-Government Act of 2002, has tasked NIST with responsibilities for standards and guidelines, and development of: • Standards to be used by all federal agencies to categorize all information and information systems collected or maintained by or behalf of each agency based on objectives of providing appropriate levels of information security according to risk levels; • Guidelines for determining the types of information and information systems to be included in each category; and • Minimum information security requirements, e.g., management, operational, and technical controls.
Guidelines	Official advice or recommendation indicating how something should be done or what sort of action should be taken in a particular circumstance.
Information Security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
Procedures	Detailed step by step instructions.

Security Controls	The management, operational, and technical controls (i.e. safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Policy	A security policy provides for the basic information technology security procedures for management, the rules for employees to adhere to and the standards for which the information technology staff must maintain.
Standards	Provide the level or quality or excellence that is accepted as the norm or by which actual attainments are judged.
Strategic Plan	A strategic plan is prepared to accomplish a framework for decisions. It is visionary by nature and does not reflect specific details and or tasks to accomplish in the short term.

APPENDIX II

POSTAL REGULATORY COMMISSION

Office of the Secretary

January 9, 2008

Mr. Jack Callender
Inspector General
Postal Regulatory Commission
901 New York Avenue, NW
Suite 200
Washington, DC 20268

RE: Response to Inspector General Audit Report 07-02A-01- Audit of Information Technology Governance, and Information Security Planning

Dear Mr. Callender:

At the Chairman's request, I am pleased to respond to the above Audit and to see that it concluded with the following recommendations:

> *The PRC should continue to support preparation, completion, and final approval of a formal information security plan, implement an organizational structure with defined roles and responsibilities, implement formal information security policies and procedures, document the enterprise architecture, and implement an ongoing monitoring plan, with achievable and realistic milestones for completion.*

The Commission will respond to these recommendations one at a time:

1. **Continue to support preparation, completion, and final approval of a formal information security plan.**

The Commission expects to complete and implement its formal information security plan by June 30, 2008.

This plan will both supplement and support the Commission's IT Security Policy, currently under review.

901 New York Avenue NW, Suite 200 | Washington, DC 20268-0001 | Phone: (202) 789-6840
Fax: (202) 789-6886 | www.prc.gov

2. Implement an organizational structure with defined roles and responsibilities.

The Commission expects to implement an organizational structure with defined roles and responsibilities by March 31, 2008, for the Chief Information Officer and the Senior Agency Information Security Officer.

In addition, the daily responsibilities for the Network Administrator and User Support Staff have been drafted and defined and is under review as part of the PRC IT Security Policy.

Part of the new organizational structure of the Commission is the addition of a new Assistant Director for Strategic and Performance Planning within the Office of the Secretary and Administration. This individual's role will be to insure agency progress on many of the recommendations contained in this Audit.

3. Implement formal information security policies and procedures.

General Dynamics Information Technology under contract with the Commission, created a Risk Assessment analysis entitled, "PRC Risk Evaluation and Guidance on NIST SP800-53 Security Controls" that the Commission is using to formulate its comprehensive Security Policy and Plans. It is anticipated that a policy and plan will be formally implemented by June 30, 2008.

4. Document the enterprise architecture.

The Commission is currently researching and drafting documentation to diagram the formal Enterprise Architecture (EA) of the existing information technology systems. The diagram of the EA will align with the Commission's Strategic Plan, currently in draft and under review. As the Commission continues to define its new business processes, it is expected that a formal EA structure may not be ready for full implementation before the first quarter of 2009.

5. Implement an ongoing monitoring plan, with achievable and realistic milestones for completion.

The Commission expects to implement a documented, formal monitoring plan and to complete implementation of its security policies and plans by June 30, 2008.

Steps were taken during 2007 to address many identified operational and security related weaknesses in the Commission IT environment, including:

- Replaced our software-based Firewall with a new, hardware-based Firewall;
- Added an Email Security and Anti-Spam appliance;
- Added a network bandwidth monitoring and control appliance;
- Upgraded the Commission's Anti-Virus software to better manage server and desktop AV configuration;
- Encrypted the Commission's web-based, email access to use HTTPS protocol;

901 New York Avenue NW, Suite 200 | Washington, DC 20268-0001 | Phone: (202) 789-6840
Fax: (202) 789-6886 | www.prc.gov

- Added a VPN appliance that utilizes Secure Socket Layer (SSL) or IPSEC encryption to ensure the security of data transferred between PRC resources and client devices;
- Conducted the first formal IT Security Awareness Training which received 100 percent successful participation from staff and contractors, and,
- Implemented the first formal Email Policy, that outlines users and Commission responsibilities as to electronic mail and added this policy as well as the Commission's "limited use" policy to its IntraNet site for all personnel.

The Commission appreciates this opportunity to comment on the findings of your Report.

Sincerely,

Steven W. Williams

901 New York Avenue NW, Suite 200 | Washington, DC 20268-0001 | Phone: (202) 789-6840
Fax: (202) 789-6886 | www.prc.gov