OFFICE OF INSPECTOR GENERAL

Audit Report

Evaluation of the Railroad Retirement Board Medicare Contractor's Information Security

Report No. 08-04
September 26, 2008

RAILROAD RETIREMENT BOARD

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) evaluation of the Railroad Retirement Board (RRB) Medicare contractor's information security.

Background

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA). These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid over $9.8 billion in benefits during fiscal year (FY) 2007. The RRB is headquartered in Chicago, Illinois and has 53 Field Offices across the nation.

The RRB's information system environment consists of two general support systems and six major application systems, one of which is the administration of Medicare entitlement. Each system has been designated as a moderate impact system in accordance with standards and guidance promulgated by the National Institute of Standards and Technology (NIST).

The RRB's Medicare program provides health insurance to persons ages 65 and older, as well as certain other persons under age 65 who are entitled to monthly benefits based on total disability. The RRB enrolls railroad beneficiaries for Medicare coverage, collects for Part B supplemental medical insurance, and oversees a nationwide contract for the processing of Part B claims. As of the end of fiscal year 2007, approximately 503,400 persons were enrolled in Medicare Part A, and about 487,400 of them were also enrolled in Part B. The RRB's Medicare contractor for Part B claims made payments totaling $897 million in fiscal year 2007.

This evaluation was conducted pursuant to Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), which requires annual agency program reviews, Inspector General security evaluations, an annual agency report to the Office of Management and Budget (OMB), and an annual OMB report to Congress. FISMA also establishes minimum requirements for the management of information security in nine areas.

- Risk Assessment
- Policies and Procedures
- Testing and Evaluation
- Training
- Security Plans
- Remedial Action Process
- Incident Handling and Reporting
- Continuity of Operations
- Inventory of Systems

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity, and availability. The agency's information security program includes information systems provided by contractors. The RRB's Medicare contractor has stated that their entity-wide systems security program has been implemented, documented, approved and monitored in accordance with methodologies and requirements established by the Centers for Medicare and Medicaid Services (CMS), the cognizant Federal agency.

The Bureau of Information Services (BIS), under the direction of the Chief Information Officer is responsible for the RRB's information security and privacy programs. The Office of Programs is responsible for the Medicare major application, including oversight of its contractor operations.

Objective, Scope and Methodology

This evaluation was performed to meet FISMA requirements for an annual OIG evaluation of information security for an RRB contractor operation during FY 2008. Our evaluation consisted of examining documents prepared by the RRB's Medicare contractor to support FISMA compliance in accordance with NIST guidance, including the design of FISMA required controls. These documents are provided to the RRB to support the RRB's oversight role for the RRB Medicare program, including FISMA compliance. Our evaluation did not include an assessment of whether the controls listed in any of the documents were operating or effective, nor did we evaluate the documents to determine compliance with CMS methodologies and requirements.

In addition to examining the above-referenced documents, we assessed whether a web-based component application recently implemented by the RRB in January 2008, for use by the Medicare contractor, adequately addressed authentication and privacy risks in accordance with OMB requirements.[1] This component application allows employees of the Medicare contractor to report specific transactions to the RRB for updating various RRB information systems.

The primary criteria for this evaluation included:

- FISMA requirements;
- OMB Circular A-130, "Management of Federal Information Resources";
- OMB memoranda; and
- NIST standards and guidance.

Our work was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain

[1] Authentication is the process in which the identity of a user is verified, often as a prerequisite to allowing access to resources in an information system.

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. Fieldwork was conducted at RRB headquarters in Chicago, Illinois from May through September 2008.

RESULTS OF EVALUATION

The Office of Programs has received a level of information from their Medicare contractor that would facilitate their oversight role for the RRB's Medicare program, including FISMA compliance. However, some improvement is needed in ensuring risk-based assessments for the RRB's information security and privacy program.

The details of our review, including recommendations for corrective action, follow. Agency management has agreed to take the recommended corrective actions for all recommendations. The full text of management's responses is included in this report as Appendix I.

FISMA Related Documentation

The RRB's Medicare contractor has provided RRB management with documentation to support compliance with certain FISMA requirements. RRB management provided us with copies of the following FISMA related documents:

- system security plan,
- risk assessment,
- self-assessment, and
- Plan of Actions and Milestones (POAM).

CMS is the primary recipient of these materials because they are the cognizant Federal agency for FISMA compliance with respect to Medicare contractors. Our assessment included a comparison of these documents with applicable NIST guidance for general form and content.

System Security Plan

Our evaluation of the system security plan using NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems" showed that while the plan contained extensive control descriptions, it did not list the individual controls specified in NIST SP 800-53, "Recommended Security Controls for Federal Information Systems." We also observed that the plan did not specify which of the individual controls were "common." A common control is generally managed by an organizational entity other than the information system owner and is shared by multiple system owners. The system security plan presents a background of the program that implies multiple organizational entities which suggests common controls may be applicable.

Risk Assessment

We evaluated the risk assessment using NIST SP 800-30, "Risk Management Guide for Information Technology Systems" and observed that the document follows a NIST compliant methodology. We noted, however, that the control recommendations that are required by NIST are only referenced in the document and not presented individually.

Additionally, the risk assessment document does not reflect whether or not CMS management or auditors recommended controls that would mitigate the risks to an acceptable level, and that those recommended controls were implemented by the Medicare contractor.

Self-Assessment

The Medicare contractor's self-assessment is well documented and directly references the individual controls from NIST SP 800-53 and well as other directives such as the Health Insurance Portability and Accountability Act and the Government Accountability Office Federal Information System Controls Audit Manual.

Plan of Actions and Milestones

We evaluated the POAM using criteria established by OMB. POAM instructions are highlighted by OMB each year in their annual FISMA reporting instructions. Detailed POAM data elements required by OMB are provided in OMB M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act." While POAMs are no longer required to follow the exact format shown in the above referenced guidance, all of the data elements must still be included.[2] We observed that the POAM generally complies with OMB guidance. However, we did note that some milestone completion information was not consistently provided within the POAM. Additionally, we did not find any overall status information regarding the state of weakness correction such as "ongoing" or "completed".

E-Authentication Risk Assessment

An E-Authentication Risk Assessment was not prepared before a newly developed RRB web-based application was implemented. NIST defines electronic authentication (e-authentication) as "the process of establishing confidence in user identities electronically presented to an information system."

OMB M-04-04, "E-Authentication Guidance for Federal Agencies," provides agencies with the guidance for determining the level of e-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence. OMB M-08-21, "FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," defines an e-authentication application as an application that:

- is web-based;
- requires authentication; and
- extends beyond the borders of the agency's enterprise (e.g. multi-agency, government-wide, or public facing).

[2] Since this review was for a contractor operation, we did not consider the data element which estimates the Federal budget funding resources required to address any weaknesses identified in the POAM.

In January 2008, the RRB implemented a web-based component application for use by the Medicare contractor. This component application allows employees of the Medicare contractor to report specific transactions to the RRB for updating various RRB information systems. This application meets the e-authentication criteria established in OMB M-08-21.

RRB management did not ensure that the E-Authentication Risk Assessment was prepared in accordance with OMB guidance. As a result, the RRB cannot provide assurance that the risks associated with improper authentication methods are addressed in the new application.

Recommendation

1. We recommend that the Office of Programs prepare an E-Authentication Risk Assessment for the newly implemented application.

Management's Response

The Office of Programs has agreed, and will complete an assessment.

Privacy Impact Assessment

A privacy impact assessment was not prepared before a newly developed RRB web-based application was implemented. A privacy impact assessment is an analysis of how information is handled to ensure the handling conforms with legal, regulatory, and policy requirements regarding privacy. A privacy impact assessment is essentially a risk assessment of the practices involving privacy-related information.

OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," requires agencies to prepare privacy impact assessments when they use information technology to collect new information or when they develop or buy new systems to handle collections of personally identifiable information.[3]

As discussed above, the RRB implemented a web-based component application in January 2008 for use by their Medicare contractor. This component application allows employees of the Medicare contractor to report specific transactions to the RRB for updating various RRB information systems. These transactions include personally identifiable information and, therefore, meet the criteria established in OMB M-03-22.

RRB management did not ensure that the privacy impact assessment was prepared in accordance with OMB guidance. As a result, the RRB cannot provide assurance that

[3] Personally identifiable information is any information about an individual maintained by an agency which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

the risks associated with collecting and handling privacy-related information are addressed in the new application.

Recommendation

2. We recommend that the Office of Programs prepare a privacy impact assessment for the newly implemented application.

Management's Response

The Office of Programs concurs with the recommendation and will complete the assessment.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)
RAILROAD RETIREMENT BOARD

SEP 2 5 2008

TO: Letty Benjamin Jay
Assistant Inspector General for Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

THROUGH: Dorothy Isherwood
Director of Programs

SUBJECT: **Draft Report – Evaluation of the Railroad Retirement Board Medicare Contractor Information Security**

Recommendation 1	The Office of Programs should prepare an E-Authentication Risk Assessment for the newly implemented application.
OP response	We agree. We will complete the assessment by March 31, 2009.
Recommendation 1	The Office of Programs should prepare a privacy impact assessment for the newly implemented application.
OP response	We concur. We will complete the assessment by March 31, 2009.

cc: Director of Policy and Systems