# OFFICE OF INSPECTOR GENERAL

# Audit Report

## Evaluation of Information Security for the Railroad Retirement Board's Financial Interchange Major Application

**Report No. 08-03**
**September 26, 2008**

***This abstract summarizes the results of the subject audit. The full report includes information protected from disclosure and has been designated for limited distribution pursuant to 5 U.S.C. § 552.***

## RAILROAD RETIREMENT BOARD

Report Abstract
Evaluation of Information Security for the Railroad Retirement Board's
Financial Interchange Major Application
OIG Report No. 08-03
Dated September 26, 2008

This abstract summarizes the results of the Office of Inspector General's (OIG) evaluation of Information Security for the Railroad Retirement Board's (RRB) financial interchange major application.

The Federal Information Security Management Act (FISMA) mandates that agencies develop, document and implement an agency wide information security program. FISMA establishes minimum information security requirements. These requirements are listed in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Recommended Security Controls for Federal Information Systems."

The financial interchange is a collective term that describes a series of legally mandated periodic fund transfers between the Social Security Administration, the Railroad Retirement Board, the Centers for Medicare and Medicaid Services and the Treasury. The amounts transferred are the result of a complex statistical projection, and the Bureau of Actuary is responsible for determining the amount to be transferred each year. The Bureau of Information Services maintains the general support systems in which the financial interchange major application operates. In June 2008, the RRB received a net transfer for Fiscal Year 2007 of over $3.5 billion, representing 39% of RRB financing sources for that year.

Our work shows that the Bureau of Actuary needs to strengthen application-level controls in the financial interchange major application system. Our evaluation of applicable NIST security requirements disclosed weaknesses in access controls, contingency planning, systems development, systems documentation, and asset inventory.

Access Controls

We identified access and sharing permissions that did not restrict the financial interchange files and folders in a manner consistent with the principle of least privilege. Additionally, we identified individuals with high-level privileges and non-unique identification and passwords. The overall information security program is weakened because the Bureau of Actuary has increased its risk to an unacceptable level by allowing employees more access than necessary to accomplish their job function, as well as inadequate accountability for some individuals.

Contingency Planning

We noted that the financial interchange major application had never been tested off-site for disaster recovery purposes. As a result, the Bureau of Actuary cannot ensure that the financial interchange major application can be restored from backup tapes and be fully functional in case of a disaster.

Systems Development

We observed that the Bureau of Actuary has not incorporated a formal systems development life cycle methodology when they make changes to the financial interchange major application. The informal method of systems development used by the Bureau of Actuary has resulted in undetected errors and inconsistencies in recent changes to the application's edit code and Help file. Since edit codes provide input integrity when data is entered into the application, errors and inconsistencies can result in incorrect calculations in the financial interchange transfer amount.

Systems Documentation

Our review also showed that the Bureau of Actuary needs to develop complete, accurate system documentation to support the financial interchange major application system. We found discrepant, incomplete or inaccurate systems information in various documents maintained by the agency. Discrepant and incomplete system documentation undermines the security and management control programs as a whole.

Asset Inventory

The RRB's inventory records do not accurately identify the agency's existing information technology equipment. We noted a personal computer listed in the agency's fixed asset inventory which had been previously disposed of by the Bureau of Information Services several years prior to our review. A physical inventory performed by the Bureau of Information Services between the disposal date and the date of our review did not identify and correct the inaccurate data. We found that the Bureau of Information Services has draft procedures for the periodic inventory of equipment, but they do not provide for subsequent actions when equipment can not be located. As a result, the RRB is unable to fully assess the security risk and potential data breach when equipment is not found.

We have made specific recommendations for corrective actions to strengthen these application controls and address the weaknesses identified in our audit. The Bureau of Actuary and the Bureau of Information Services have agreed to implement our recommendations to improve the information security related to the financial interchange major application.