OFFICE OF INSPECTOR GENERAL

Audit Report

Audit of the Adequacy of Interface Application Controls in the Financial Management Integrated System

Report No. 14-11
August 14, 2014

RAILROAD RETIREMENT BOARD

TABLE OF CONTENTS

INTRODUCTION

This report presents the results of the Office of Inspector General's audit of interface application controls in the Financial Management Integrated System (FMIS).

Background

The Railroad Retirement Board (RRB) is an independent agency in the executive branch of the Federal government. The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and the Railroad Unemployment Insurance Act. The RRB paid $11.7 billion in retirement/survivor benefits and $84.5 million in unemployment and sickness insurance benefits during Fiscal Year 2013.

The RRB uses its financial management system to record financial transactions and to support the preparation of the agency's annual financial statements. In October 2013, the RRB transitioned from an older mainframe based financial management system, the Federal Financial System (FFS), to a new web-based cloud hosted system, FMIS. FMIS is owned by the agency's Bureau of Fiscal Operations and was authorized to operate by the Chief Financial Officer on September 30, 2013. FMIS is the core system for budget formulation and execution, procurement, payment and receivable management, general ledger management, debt collection and external reporting.

Information is passed between FMIS and other applications through automated or manual data exchanges. These exchanges of information are interfaces within the definition established in the U.S. Government Accountability Office (GAO) *Federal Information System Controls Audit Manual* (FISCAM).[1] Some of the FMIS interfaces include:

- payroll and transit benefit information with the RRB's shared service provider, the General Services Administration;
- trial balance, fund balance, and accounting information exchanged with the U.S. Department of the Treasury;
- credit card purchase data obtained from Citibank;
- RRB travel expenses and reimbursement information received from a government contractor;
- disbursement information to Treasury for payments to vendors and employee reimbursements;
- billings for medical exams and consulting medical opinions provided by a contractor supporting RRB disability claims processing; and
- RRB procurement data passed to USASpending.gov, along with procurement opportunities posted to a federal procurement website.

[1] *Federal Information System Controls Audit Manual*, GAO-09-232G, February 2009.

Controls over interfaces ensure the timely, accurate, and complete processing of information between applications and other feeder and receiver systems on an ongoing basis.[2] The objectives of interface controls are to: (1) implement an effective interface strategy and design, and (2) implement effective interface processing procedures. These procedures should ensure that:

- Interfaces are processed completely, accurately, and only once in the proper period.
- Interface errors are rejected, isolated, and corrected in a timely manner.
- Access to interface data and processes are properly restricted. Data is reliable and obtained only from authorized sources.[3]

The interface strategy the RRB used for the new FMIS was to adapt as much of the interface design and processes in place under the prior FFS. Therefore, the RRB did not have to significantly redesign interfaces between its new financial system, other internal RRB systems, other government agencies or RRB contractors when converting to FMIS. Most interfaces involve manual uploads of files from one system to another. For many interfaces, the RRB only had to adapt the file download and upload processes previously used in FFS.

This audit supports the RRB's Strategic Plan's second strategic goal to "[s]erve as responsible stewards for our customers' trust funds and agency resources." This goal includes an objective to "ensure effectiveness, efficiency, and security of operations." This audit addresses controls that ensure security of operations.

This audit will also directly support the Office of Inspector General's mandated annual Federal Information Security Management Act (FISMA) evaluation and indirectly support the Office of Inspector General's audit of the RRB's financial statements.[4]

Audit Objective

The audit objective was to assess the adequacy of the interface application controls in the FMIS.

Scope

The scope of the audit was the FMIS interface application controls that were in place from October 2013 through March 2014.

[2] FISCAM, GAO-09-232G, page 428.
[3] FISCAM, GAO-09-232G, page 430.
[4] *Federal Information Security Management Act of 2002*, Public Law 107-347.

Methodology

To accomplish the audit objective, we:

- reviewed pertinent laws and guidance;
- reviewed applicable RRB policies and procedures to ensure compliance with laws and guidance;
- interviewed agency management and staff to gain an understanding of interface processes and interface controls;
- evaluated the design of interface application controls; and
- determined if applicable interface controls had been placed into operation.

The primary criteria for this audit included FISCAM, FISMA, and National Institute of Technology (NIST) guidance.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

We conducted our fieldwork at RRB headquarters in Chicago, Illinois from January through June 2014.

RESULTS OF REVIEW

Our audit determined that FMIS interface application controls are adequately operating as designed; however, we did note that the RRB needs to revise the System Security Plan (SSP) for FMIS. The SSP does not adequately describe the RRB's interfaces and leaves information about interconnected applications and systems incomplete.

The details of these audit findings and our recommendation for corrective action follow.

Agency management concurs with our recommendation. The full text of management's response is included in this report in Appendix I.

FMIS System Security Plan Requires Revisions

The FMIS SSP contains incomplete interface descriptions and information because the SSP was prepared by the shared service provider and was not adequately reviewed by RRB management.

Description of Interfaces in System Security Plan Can Be Improved

The SSP for FMIS does not adequately describe the interface processes between FMIS and other systems. Besides identifying the interfaces, there is no description of basic information such as how interfaces are set up, how and when data will be exchanged, and what data will be exchanged.

NIST guidance for interconnections recommends that security plans contain information regarding interconnections such as:

- names of the systems;
- owners of the interconnected systems;
- type of interconnections;
- short discussion of major concerns or considerations in determining interconnection;
- hardware and software used;
- interaction among systems; and
- security concerns and rules of behavior governing the interconnection.[5]

Although RRB management reviewed the SSP as a basis for system authorization, they did not ensure it contained sufficient information to describe systems interfaces.

[5] *Security Guide for Interconnecting Information Technology Systems,* NIST Special Publication (SP) 800-47, August 2002, pages 4-5.

Lack of adequate descriptions of interface processes can impair stakeholders understanding of the interfaces, resulting in a weaker control environment. In addition, without adequate descriptions of the interface processes in the FMIS SSP, risks to the RRB's information systems might not be fully evident to the system's authorizing official.

FMIS System Security Plan Interface Table Should Be Completed

The FMIS SSP included a table to provide information about interconnected applications; however, much of the information in the table was missing. Table fields showing the existence of an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA) for data sharing between applications, the dates of these agreements, and their renewal dates were all marked "TBD" (to be determined). Additionally, the system owner field for each interconnected application was blank and the missing information was not provided anywhere else in the SSP.

NIST guidance on the development of security plans for federal information systems states that an ISA, MOU, or MOA is needed between systems that share data that are owned or operated by different organizations. The SSP should provide the following information concerning the authorization for the connection to other systems or the sharing of information:

- name of system;
- organization;
- type of interconnection;
- authorizations for interconnection (ISA, MOU/MOA);
- date of agreement;
- Federal Information Processing Standards Publication 199 category;
- certification and accreditation status of system; and
- name and title of authorizing official(s).[6]

Although RRB management reviewed the SSP as a basis for system authorization, they did not ensure the interface table was fully completed with the information required by NIST whenever data is shared with other systems.

Failure to complete the interconnections table in the SSP could result in misunderstandings about the existence and legitimacy of agreements over interfaces and delays in making updates when these agreements expire.

[6] *Guide for Developing Security Plans for Federal Information Systems*, NIST SP 800-18, Revision 1, February 2006, page 23.

Recommendation

We recommend that the Bureau of Fiscal Operations revise the FMIS SSP to provide the required information about each interface, and update the interconnections table accordingly.

Management's Response

The Bureau of Fiscal Operations concurs with our recommendation and has established a target date for completion. They will revise the FMIS SSP to provide the required information about each interface and will update the interconnections table.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

August 13, 2014

TO : Daniel Eckert
Acting Assistant Inspector General for Audit

FROM : George V. Govan
Chief Financial Officer

George Govan

SUBJECT: Draft Report - Audit of the Adequacy of Interface Application Controls in the Financial Management Integrated System

This is in response to your request for comments on the above draft report. Following are my comments on the recommendation addressed to the Bureau of Fiscal Operations (BFO).

We recommend that the Bureau of Fiscal Operations:

> ***Revise the FMIS SSP to provide the required information about each interface, and update the interconnections table accordingly.***
>
> We concur. BFO will revise the Financial Management Integrated System's System Security Plan to provide the required information about each interface and will update the interconnections table.
>
> Target Completion Date: September 30, 2014.

If there is any additional information you need, please advise me.

cc: Tom McCarthy, Chief of TADS
Kris Garmager, Financial Systems Manager
Mike Zulevic, IT Specialist
Jean Hines, Financial Systems Specialist
Jerry Gilbert, Chief Security Officer
Susan Leszkowicz, Supervisory Auditor