OFFICE OF INSPECTOR GENERAL

Audit Report

Audit of the Railroad Retirement Board's Privacy Program

Report No. 13-11
September 20, 2013

RAILROAD RETIREMENT BOARD

EXECUTIVE SUMMARY

Background

The Railroad Retirement Board (RRB), Office of Inspector General (OIG) conducted an audit to assess the adequacy of the RRB's privacy program to ensure that the RRB is in compliance with current and anticipated requirements for privacy. The audit focused on the initial and annual privacy training for RRB employees and contractors, the privacy reviews that are performed, the privacy reports that are filed, and the policies and procedures of the privacy program.

Findings

The RRB-OIG identified the following weaknesses:

- Contractor personnel are not adequately identified.
- The instructional memo from Acquisition Management to the contracting officer's representative needs revision.
- Contractor personnel did not receive annual privacy training.
- Outdated privacy and security training materials are provided to new employees.
- Administrative circulars are outdated.
- Privacy considerations need to be included with systems development requests.
- A strategic organizational privacy plan needs to be developed to include policies on the validation of personally identifiable information (PII), communication between bureaus regarding changes in PII, and the use and protection of PII in testing, training, and research.

Recommendations

To address the identified weaknesses, we recommended that RRB officials take the following actions:

- Update and maintain the Contractor Security Control Log to reflect all contractor personnel that work at the RRB during the life of the contract, and indicate if they will have access to PII.
- Revise the instructions to the contracting officer's representative to update the Contractor Security Control Log and implement a control to ensure those updates are made.
- Revise the methods for identifying contractor personnel and distributing the annual privacy training, and implement a control to verify that all contractors receive annual training.
- Revise and update the privacy and security awareness training documents, and update the privacy training materials provided to new employees.

- Revise Administrative Circulars IRM-2 and IRM-15 to reflect current security and privacy documents and procedures.
- Revise Form G-436A to include privacy related questions and an approval by the Chief Privacy Officer.
- Develop a strategic organizational privacy plan that is multi-organizational and represents the RRB as a whole.
- Develop policies for the validation of PII, the communication between bureaus regarding changes in PII, and the use and protection of PII in testing, training, and research.

Management's Response
Agency management concurs with all recommendations. The full texts of management's responses are included in this report in Appendices I and II.

TABLE OF CONTENTS

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) audit of the Railroad Retirement Board's (RRB) privacy program.

Background

The RRB is an independent agency in the executive branch of the Federal government. The agency administers 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. These programs provide income protection during retirement and in the event of disability, death, or temporary unemployment or sickness.

During fiscal year (FY) 2012, railroad retirement and survivor benefit payments totaled $11.4 billon, net of recoveries and offsetting collections, to about 573,000 beneficiaries. Railroad unemployment and sickness insurance benefit payments totaled $76 million in FY 2012, net of recoveries and offsetting collections, to about 27,000 beneficiaries. During FY 2012, the RRB also paid benefits on behalf of the Social Security Administration (for which the RRB is reimbursed) amounting to $1.4 billion to about 114,000 beneficiaries.[1]

Congress established the OIG to provide independent oversight of the RRB's programs and operations. This audit supports the RRB's strategic goals and objectives to ensure effectiveness, efficiency, and security of operations in the administration of programs. It also supports the requirement that the OIG evaluate the RRB's overall information security program and practices under the Federal Information Security Management Act of 2002 (FISMA).[2]

The Privacy Act of 1974 requires Federal agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.[3]

Section 208 of the E-Government Act of 2002 details privacy provisions that ensure sufficient protections of personal information.[4] The responsibilities and guidance for privacy impact assessments and privacy protections on agency websites are also detailed.

Office of Management and Budget (OMB) Circular A-130 requires agencies to establish a level of security for all agency information systems.[5] Appendix I of the circular details the responsibilities for implementing the reporting and publication requirements of the

[1] *Railroad Retirement Board Performance and Accountability Report,* Fiscal Year 2012*,* page 21.
[2] *Federal Information Security Management Act of 2002,* Public Law 107-347, Title III.
[3] *Privacy Act of 1974,* 5 U.S.C. § 552a.
[4] *E-Government Act of 2002,* Public Law 107-347.
[5] *Management of Federal Information Resources,* OMB Circular A-130, November 2000.

Privacy Act of 1974. Appendix III of the circular establishes a minimum set of controls and assigns agency responsibilities for security of automated information. It further specifies that agencies shall implement and maintain a security program, including the preparation of policies, standards, and procedures.

The National Institute of Standards and Technology (NIST) released Special Publication (SP) 800-53, Revision 4 as final on April 30, 2013; however, it was only available as a draft at the beginning of this audit.[6] This publication contains Appendix J, which provides a structured set of privacy controls that help organizations enforce requirements derived from Federal privacy legislation, policies, regulations, directives, standards, and guidance. These controls were evaluated as part of this audit.

The RRB has developed a privacy program to protect the personally identifiable information (PII) it retrieves and maintains.[7] This program is operated under the direction of the Chief Information Officer, who is the Senior Agency Official for Privacy, and the Chief Privacy Officer. The Chief Privacy Officer works closely with the Chief Security Officer and the Office of Administration's Division of Acquisition Management (Acquisition Management); especially when initial and annual training is conducted, and when he conducts his annual FISMA review for contracts. Acquisition Management works with the RRB's contracting officer's representatives (COR) in monitoring the contractors that perform services for the agency.

Audit Objective

The audit objective was to assess the adequacy of the RRB's privacy program to ensure that the RRB is in compliance with current and anticipated requirements for privacy.

Scope

The scope of the audit was the privacy program in effect between FY 2008 and FY 2013 at the RRB's headquarters in Chicago, Illinois.

Methodology

To accomplish our objective, we:

- reviewed pertinent laws and guidance;
- interviewed RRB employees involved in the privacy program;
- reviewed RRB policies and procedures applicable to the privacy program, and determined if they are operating as intended;

[6] *Security and Privacy Controls for Federal Information Systems and Organizations,* NIST SP 800-53, Revision 4, April 2003.

[7] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

- reviewed the annual FISMA privacy reports and reported actions taken on current privacy initiatives related to PII holdings and social security number use for the period FY 2009 through FY 2012;
- determined if the privacy reviews were performed in compliance with OMB requirements;
- reviewed the privacy impact assessment reports for the RRB's five major applications for compliance with OMB requirements;
- reviewed the system of record notices published in the Federal Register and maintained on the RRB's website; and verified the RRB's practices related to the security and quality of data, information sharing, and accounting for disclosures;
- analyzed the privacy training materials provided to new employees by Human Resources for compliance with OMB 07-16;
- identified new employees hired in FY 2013, and determined if privacy training acknowledgments were obtained prior to providing system access;
- reviewed the annual privacy training records for FY 2012, and analyzed the results of the training provided to employees and contractors; and
- reviewed the contractor training records for initial privacy training in FY 2008 through FY 2013, and identified whether training had been provided.

The primary criteria used in this audit included:

- The Privacy Act of 1974;
- The E-Government Act of 2002;
- OMB guidance and memoranda;
- NIST standards and guidance; and
- RRB policies and procedures.

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 objectives. 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 the RRB's headquarters in Chicago, Illinois, from December 2012 through July 2013.

RESULTS OF AUDIT

Our audit found that the RRB's privacy program is not adequate enough to ensure that they are in compliance with the current privacy requirements and anticipated requirements established in NIST SP 800-53, Revision 4 published in April, 2013. The need for improvement in the administration of the required privacy training and the policies required under the recently issued guidance has been identified as follows:

- contractor personnel are not adequately identified;
- the instructional memo from Acquisition Management to the COR needs revision;
- contractor personnel did not receive annual privacy training;
- outdated privacy and security training materials are provided to new employees;
- administrative circulars are outdated;
- privacy considerations need to be included with systems development requests; and
- a strategic organizational privacy plan needs to be developed to include policies on the validation of PII, communications between bureaus regarding PII changes, and the use and protection of PII in testing, training, and research.

The details of our findings and recommendations for corrective action are discussed throughout the remainder of this report. Agency management concurs with all recommendations. The full texts of management's responses are included in Appendices I and II of this report.

Contractor Personnel Are Not Adequately Identified

The RRB is not identifying every employee of the contractor working for the RRB, resulting in incomplete tracking of privacy requirements. The RRB utilizes a Contractor Security Control Log (log) in the administration of the privacy requirements for contractors. The log is not complete and does not contain all of the information necessary to confirm that the privacy requirements have been addressed.

The controls in NIST SP 800-53, Revision 4 require that the RRB assess contractor compliance with privacy requirements, which includes privacy training and certification of acceptance of the responsibilities for privacy requirements. Acquisition Management provides instructions to the COR that detail their responsibilities relating to privacy. These instructions require the COR to provide the contract administrator information regarding any system of records which the contractor could access; and to provide the Chief Privacy Officer the names of the entire contractor's staff assigned to the contract at the start of the contract, as well as any replacement or additional staff during the life of the contract.

The log was developed to satisfy a previous OIG recommendation to identify and track contracted individuals; however, it does not identify every employee of the contractor. We performed a review of the log for FY 2012 and compared the contractors listed with

those contractors that have access to PII. This identified a contractor with personnel that have access to PII, but was not included on the log. Interviews with the Chief Privacy Officer and the CORs confirmed that every contractor staff change made during the life of the contract is not being communicated to the Chief Privacy Officer. Interviews with Acquisition Management determined that they did not maintain documentation from the COR supporting access to PII that the contractor may have while working at the RRB.

The effectiveness of the log is dependent upon the COR and their updates regarding the contractor staff and whether that staff has access to PII or a system of records. The instructional memo from Acquisition Management to the COR needs to be revised to require the COR to update the log with that information.

Without complete records regarding every employee of the contractor and whether they have access to PII, the RRB will not be able to adequately ensure all privacy requirements for contractors are met.

Recommendations

1. We recommend that the Bureau of Information Services work with the Office of Administration, Division of Acquisition Management, and the agency's contracting officer's representatives to maintain the Contractor Security Control Log, ensure that it is continually updated to reflect all contractors and their staff that work at the RRB, and indicate whether the contractor staff will have access to PII or a system of records.

2. We recommend that Office of Administration, Division of Acquisition Management, revise the instructions to the contracting officer's representative and implement a control to ensure the Contractor Security Control Log is updated accordingly.

Management's Responses

In response to recommendation number 1, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will develop the policies and procedures.

In response to recommendation number 2, the Office of Administration concurs with this recommendation.

Contractor Personnel Did Not Receive Annual Privacy Training

In FY 2012, some of the contractors with access to PII did not receive annual privacy training. The methods that are used to identify contractor personnel and to provide annual privacy training are not effective in ensuring that every employee of the

contractor is trained. Generally, contractor personnel are only receiving initial training from the Chief Privacy Officer when the COR provides the contractor personnel list to the Chief Privacy Officer.

The controls in NIST SP 800-53, Revision 4 require that the RRB, at least annually, administer basic and roles-based privacy training to all personnel having responsibility for PII or activities that involve PII. This includes all contractor personnel. The Chief Privacy Officer provides annual privacy training to the RRB's contractors. The identification and distribution of the annual privacy training to contractor personnel is through the RRB's email system. However, not every contractor is assigned an RRB email address. Therefore, the emailed training notice is not released to all contractors.

The RRB is not adequately ensuring that annual privacy training requirements are met for all contractors. As such, the RRB faces an increased risk for a breach of PII by contractor personnel.

Recommendation

3. We recommend that the Bureau of Information Services revise their methods for identifying contractor personnel and distributing the annual privacy training, and implement a control to verify that all contractors receive annual privacy training.

Management's Response

In response to recommendation number 3, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will update the policies and procedures to ensure all contractors that have access to PII or work with privacy act systems of records will receive both initial and subsequent annual refresher privacy awareness training.

Outdated Training Materials Are Provided to New Employees

The initial training documents provided to new RRB employees for security awareness and privacy responsibilities are outdated and require revision. We interviewed Human Resources and reviewed the security and privacy training materials provided to new employees. We found that the combination of documents provided, which includes the G-15, *Information Systems Security Awareness Training for the Railroad Retirement Board*, meets the privacy training requirements of OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

OMB Memorandum 07-16 includes proper safeguards that should be in place to protect PII including privacy and security requirements. The security requirements require that agencies must initially train employees on their privacy responsibilities before permitting access to agency information and information systems. Thereafter, agencies must

provide at least annual refresher training to ensure employees continue to understand their responsibilities. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed.

In February 2013, the Chief Security Officer instructed Human Resources to remove the G-15 security and privacy awareness pamphlet from the training materials because it was obsolete and being retired. However, in July 2013, the RRB reconsidered their decision to retire the G-15, and the Chief Security Officer indicated that pamphlet could continue to be used for initial security and privacy training after it is updated.

In order to provide quality security and awareness training, the materials that are distributed to employees need to be current. Training is necessary to continue to safeguard the RRB's information and information systems.

Recommendations

4. We recommend that Bureau of Information Services revise and update the privacy and security awareness training documents and provide the Bureau of Human Resources with the updated documents.

5. We recommend that Office of Administration, Bureau of Human Resources, update the materials that are provided to new employees with the updated privacy and security awareness training documents.

Management's Responses

In response to recommendation number 4, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services has provided updated privacy awareness training documents to the Bureau of Human Resources and has established an interim working procedure for new RRB employees to certify that they understand their safeguarding responsibilities. These procedures will be documented.

In response to recommendation number 5, the Office of Administration concurs with this recommendation.

Administrative Circulars Are Outdated

The RRB has administrative circulars that are outdated and contain references to obsolete or outdated documents. The outdated circulars are Administrative Circular IRM-2, *Management of Information Privacy for Individuals,* and IRM-15, *Safeguarding Protected Information and Breach Notification Protocol*. The Chief Privacy Officer identified these administrative circulars as part of the policies and procedures for the privacy program.

The controls in NIST SP 800-53, Revision 4 require that the RRB update privacy policies and procedures at least biennially. In addition, Administrative Circular IRM-2 defines the responsibilities of the Senior Agency Official for Privacy, including a review of privacy procedures to ensure that they are comprehensive and up-to-date.

Management has not ensured that agency policy documents in the form of administrative circulars are correct and up-to-date. Administrative Circular IRM-2 was last updated on September 3, 2008. A review of this document identified references to Form IRM-1, *Information Privacy Certification by Contractor.* This document was replaced by Form G-511, *Information Privacy Certification by Contractor,* in November 2009. Administrative Circular IRM-15 was last updated on October 9, 2012. This document contains references to Form G-455X which was declared as obsolete by the RRB in April 2009.

Incorrect and outdated policy documents weaken the overall internal control structure of the agency.

Recommendation

6. We recommend that the Bureau of Information Services revise Administrative Circulars IRM-2 and IRM-15 to reflect current security and privacy documents and procedures.

Management's Response

In response to recommendation number 6, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will revise Administrative Circulars IRM-2 and IRM-15.

Privacy Considerations Need to be Included with Systems Development Requests

The RRB is requesting changes to systems without considering privacy requirements when the request is made. The RRB uses Form G-436A, *Request for Information Technology Development,* for systems development requests. This form does not contain any privacy related questions and does not require approval of the Chief Privacy Officer before systems development is started.

The controls in NIST SP 800-53, Revision 4 require that the RRB implement a process to embed privacy considerations into the development of programs, information systems, business processes, and technology.

The RRB uses Form G-436A to document information technology development requests for new projects and system modifications. While a prior version of that form included explicit privacy related questions, management revised the form in October 2008 and removed those questions.

When privacy considerations are not made when new systems are developed or changes are made to existing systems, the RRB's risk of noncompliance with privacy requirements increases, as well as the risk of unauthorized sharing of information protected by the Privacy Act.

Recommendation

7. We recommend that the Bureau of Information Services revise Form G-436A to include privacy related questions and, if necessary, an approval by the Chief Privacy Officer.

Management's Response

In response to recommendation number 7, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will revise Form G-436A to include review and approval, as necessary.

A Strategic Organizational Privacy Plan Needs to be Developed

The RRB does not have a comprehensive strategic organizational privacy plan. A strategic organizational privacy plan documents applicable privacy controls, policies, and procedures. It also presents the long-term objectives and goals the agency plans to achieve, the actions they will take to realize those goals, and how they will deal with the challenges and risks that may hinder achieving the planned results.

New controls in NIST SP 800-53, Revision 4 require that the RRB develop a strategic organizational privacy plan for implementing applicable privacy controls, policies, and procedures. The publication also details other new controls relating to the validation of PII, communication between bureaus regarding changes in PII, and the use and protection of PII for testing, training, and research purposes. A comprehensive strategic privacy plan was not previously required.[8]

Strategic planning is a valuable tool for communicating initiatives to agency managers and employees. By developing a strategic organizational privacy plan, the RRB will be able to align its resources and guide agency decision making for new or long-term privacy requirements and initiatives.

Recommendations

8. We recommend that the Bureau of Information Services develop a strategic organizational privacy plan that is multi-organizational and represents the RRB as a whole.

[8] NIST SP 800-53, Revision 4, was issued on April 30, 2013. The agency is required to implement any new controls within one year of that date.

9. We recommend that the Bureau of Information Services develop a policy for the validation of PII.

10. We recommend that the Bureau of Information Services develop a policy on communication between bureaus regarding changes in PII.

11. We recommend that the Bureau of Information Services develop a policy on the use and protection of PII in testing, training, and research.

Management's Responses

In response to recommendation number 8, the Bureau of Information Services concurs with this recommendation.

In response to recommendation number 9, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will work to develop a policy of validation of PII with the Privacy Act systems of records owners.

In response to recommendation number 10, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will work to develop a policy for coordination of changes to PII with the Privacy Act systems of records owners.

In response to recommendation number 11, the Bureau of Information Services concurs with this recommendation. The Bureau of Information Services will work to develop a policy for the use of PII and protection of PII in testing, training, and research with the Privacy Act systems of records owners.

UNITED STATES GOVERNMENT
MEMORANDUM

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

September 13, 2013

To: Diana Kruel, Assistant Inspector General for Audit

From: Ram Murthy, Chief Information Officer

Subject: BIS Response to Draft Report – Audit of the Railroad Retirement Board's Privacy Program

We have reviewed your draft audit report on the Railroad Retirement Board's Privacy Program, dated August 30, 2013. Here are our responses to the recommendations directed to the Bureau of Information Services (BIS).

Recommendations:

1. *We recommend that the Bureau of Information Services work with the Office of Administration, Division of Acquisition Management, and the agency's contracting officer's representatives to maintain a Contractor Security Control Log, ensure that it is continually updated to reflect all contractors and their staff that work at the RRB, and indicate whether the contractor staff will have access to PII or a system of records.*

   BIS Response: We concur. Office of Administration – Division of Acquisition Management has agreed to follow policies and procedures developed by BIS for the contractor security log. Acquisition Management will ensure that RRB contracting officer's representatives (COR's) are aware of their responsibilities for maintaining their portion of the contractor security log. BIS will develop the policies and procedures by December 31, 2013.

2. Recommendation directed to Office of Administration, Division of Acquisition Management.

3. *We recommend that the Bureau of Information Services revise their methods for identifying contractor personnel and distributing the annual privacy training, and implement a control to verify that all contractors receive annual privacy training.*

   BIS Response. We concur. We will update our policy and procedures to ensure all contractors that have access to PII or work with a privacy act systems of records will receive both initial and subsequent annual refresher privacy awareness training by December 31, 2013.

4. *We recommend that the Bureau of Information Services revise and update the privacy and security awareness training documents and provide the Bureau of Human Resources with the updated training documents.*

   BIS Response. We concur. We have provided updated privacy awareness training documents to the Bureau of Human Resources and have established an interim working procedure for new RRB employees to certify that they understand their privacy safeguarding responsibilities. We will have the procedures documented by December 31. 2013.

5. Recommendation directed to Office of Administration, Bureau of Human Resources.

6. *We recommend that the Bureau of Information Services revise Administrative Circulars IRM-2 and IRM-15 to reflect current security and privacy documents and procedures.*

   BIS Response. We concur. We will revise and submit for Board approval updated Administrative Circulars IRM-2 and IRM-15 by September 30, 2014.

7. *We recommend that the Bureau of Information Services revise Form G-436A to include privacy related questions and, if necessary, an approval by the Chief Privacy Officer.*

   BIS Response. We concur. We will review and revise Form G-436A as necessary to include review and approval for new or major changes to IT systems, as defined by the E-Government Act of 2002, to include review and approval as necessary by the following BIS officers who have a regulatory approval role: Chief Security Officer, Chief Privacy Officer, and the Chief Records Officer. We will also include the Supervisor of Data Management, who has role in ensuring data optimization and architecture. We will have the updated G-436A (or new form) developed and approved by September 30, 2014. We may need to adjust this projected completion date based on our gap-analysis findings and/or buy-in from agency stakeholders.

8. *We recommend that the Bureau of Information Services develop a strategic organizational privacy plan that is multi-organizational and represents the RRB as a whole.*

   BIS Response. We concur. Initial coordination with BIS managers indicate that we most likely will adopt a stand-alone strategic privacy plan that feeds into the Strategic IRM plan.

9. *We recommend that the Bureau of Information Services develop a policy for the validation of PII.*

   BIS Response. We concur. We will work to develop a policy for validation of PII with the privacy act systems of records owners by June 30, 2014.

10. *We recommend that the Bureau of Information Services develop a policy on communication between bureaus regarding changes in PII.*

    BIS Response. We concur. We will work to develop a policy for coordination of changes to PII with the privacy act systems of records owners by June 30, 2014.

11. *We recommend that the Bureau of Information Services develop a policy on the use and protection of PII in testing, training and research.*

BIS Response. We concur. We will work to develop a policy for the use of PII and protection of PII in testing, training, and research with the privacy act systems of records owners by June 30, 2014. Just like our response to audit finding #7, we may need to adjust this projected completion date based on our gap-analysis findings and/or buy-in from agency stakeholders.

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

UNITED STATES GOVERNMENT
MEMORANDUM

September 18, 2013

TO : Diana Kruel
Assistant Inspector General for Audit

FROM : Keith B. Earley
Director of Administration

SUBJECT: Draft Report – Audit of the Railroad Retirement Board's Privacy Program

Thank you for the opportunity to review the Office of Inspector General's draft audit report entitled "Audit of the Railroad Retirement Board's Privacy Program." We have reviewed the draft report and concur with both recommendations. Accordingly, we are providing the following comments to the recommendations directed to the Office of Administration:

OIG Recommendation #2

We recommend that the Office of Administration, Division of Acquisition Management, revise the instructions to the contracting officer's representative and implement a control to ensure the Contractor Security Control Log is updated accordingly.

The Office of Administration concurs with the recommendation.

Target Completion Date: September 30, 2014

OIG Recommendation #5

We recommend that the Office of Administration, Bureau of Human Resources, update the materials that are provided to new employees with the updated privacy and security awareness training documents.

The Office of Administration concurs with the recommendation.

Target Completion Date: June 30, 2014