OFFICE OF INSPECTOR GENERAL

Audit Report

Evaluation of the Railroad Retirement Board's Privacy Program

Report No. 07-06
July 30, 2007

RAILROAD RETIREMENT BOARD

INTRODUCTION

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

Background

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. These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid over $9.5 billion in benefits during fiscal year 2006.

The Privacy Act of 1974 (Privacy Act) addresses the government's obligation concerning the privacy of records maintained on individuals. It establishes requirements for the collection, maintenance, access, disclosure, and the accounting of records, as well as penalties and exemptions for all information about an individual that is maintained by the agency. Section 208 of the E-Government Act of 2002 (E-Government Act) applies the Privacy Act requirements to electronic environments. Primary components of the privacy provisions in the E-Government Act are privacy impact assessments, and the establishment of privacy policies on agency websites and in machine-readable formats.[1]

Throughout the years, the Office of Management and Budget (OMB) has issued guidance agencies must follow in implementing their privacy program. This guidance includes, but is not limited to, implementation of the Privacy and E-Government Acts, computer matching, periodic reviews, safeguards, privacy breaches/incidents, and reporting.

The mission of the RRB requires that it maintain detailed beneficiary records that include personal information. The agency reported a total of 35 systems of records in fiscal year 2006.[2]

In fiscal year 2005, the RRB appointed a new Chief Privacy Officer to oversee the privacy of beneficiary information. The Chief Privacy Officer reports to the Chief Information Officer in the Bureau of Information Services. The RRB also established two new committees during fiscal year 2007 to aid in privacy-related matters: the Security and Privacy Committee and the Agency Core Response Group. The Security and Privacy Committee generally meets on a quarterly basis and is comprised of agency employee representatives responsible for assisting in the establishment of

[1] 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.
[2] The Privacy Act defines a "system of records" as any record from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

policies, procedures, and training. The Agency Core Response Group is comprised primarily of agency managers responsible for determining whether privacy breaches pose identity theft problems.

This evaluation was conducted pursuant to Title III of the E-Government Act, the Federal Information Security Management Act of 2002 (FISMA). FISMA requires the RRB to conduct an annual evaluation of its information security program, including privacy. OMB has requested that the Inspectors General perform reviews of agency efforts to protect sensitive information. This evaluation of the privacy program at the RRB supports the FISMA evaluation for fiscal year 2007.

Objective, Scope and Methodology

The objective of this evaluation was to assess the adequacy of the RRB's privacy program. An adequate privacy program provides reasonable assurance that proper safeguards are in place to ensure the security and confidentiality of records. Our work included an assessment of the legal and regulatory requirements, as well as the management, operational, and technical controls, pertaining to the privacy program.

To accomplish our objective, we:

- reviewed pertinent legal and regulatory requirements including, but not limited to, the Privacy Act, the E-Government Act, FISMA, assorted OMB guidance listed in Appendix I of this report, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53;

- obtained and reviewed RRB policies and procedures pertaining to the privacy program;

- reviewed RRB privacy program practices, including systems of records; third party disclosures; privacy impact assessments; privacy breaches; agency committees, reviews, surveys, and reports; agency laptop inventory; data encryption and anti-theft mechanisms; contract language; training; users (including contractors) with access to agency systems; users (including contractors) with virtual private network connections; and contractor certifications;

- obtained and reviewed the RRB's Plan of Action and Milestones (POAM), an OMB designed tool for tracking remedial actions; and

- interviewed responsible management and staff.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objective. Fieldwork was conducted at RRB headquarters in Chicago, Illinois during October 2006 through April 2007.

RESULTS OF REVIEW

The RRB's privacy program is not fully effective in providing reasonable assurance that proper safeguards are in place to ensure the security and confidentiality of records. During our review, we noted that additional resources are needed to update policies and procedures, provide job-specific training, and effectively analyze and react to the results of periodic reviews performed by the Chief Privacy Officer.

We also noted weaknesses in the evaluation of risk and privacy impacts, safeguards over remote access and data removal, contract language and applicable clauses, contractor identification, identification and management of weaknesses, and explicit policies and procedures over privacy-related issues.

The details of our findings and recommendations for corrective action follow. Management has agreed to take the recommended corrective actions for all recommendations except Recommendation 4 which was considered and declined, and Recommendation 15 which has only been partially agreed. The full texts of management's responses are included in this report as Appendices II, III, and IV.

Resources are Needed for an Effective Privacy Program

The RRB has developed a privacy program designed to meet the requirements of the Privacy Act, the E-Government Act, and OMB requirements; however, additional staffing resources are needed to ensure the effectiveness of the program.

The Privacy Act, E-Government Act, and OMB guidance specifically require a privacy program that continually assesses the risks associated with handling personal information, and the implementation of safeguards to protect against those risks.

We found that many of the RRB's policies and procedures governing the privacy program are outdated and require revision to explicitly support legal and/or OMB requirements. We also found that the RRB needs to provide job specific privacy-related training to many of their employees who have increased responsibilities for handling personally identifiable information (PII).[3] Lastly, we found that the RRB needs additional resources to effectively analyze the results of their periodic reviews, and to develop and implement appropriate action plans to address the weaknesses identified.

The RRB appointed a new Chief Privacy Officer in fiscal year 2005 and two new committees during fiscal year 2007 to aid in privacy-related matters. Although the committees will be able to assist the Chief Privacy Officer in privacy-related activities, this assistance is supplemental to their regular job duties. Much of the above-

[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.

mentioned work will fall under the purview of the Security and Privacy Committee which is also tasked with assisting in the implementation of the RRB's security program. The committee's responsibilities include the resolution of existing significant deficiencies in risk assessments and periodic testing and evaluations, including certification and accreditation.

Without additional, managed resources, the RRB will continue to experience delays in achieving an effective privacy program that is fully compliant with the Privacy Act, the E-Government Act, and OMB requirements.

Recommendation

1. We recommend that the Bureau of Information Services acquire additional staffing resources to aid in the implementation of the privacy program.

Management's Response

The Bureau of Information Services concurs with the recommendation and will begin the process of adding an additional staff person.

Privacy Impact Assessments Need to be Prepared

The RRB is not preparing privacy impact assessments as required by the E-Government Act. A privacy impact assessment determines the risk and effects of collecting, maintaining, and disseminating information in identifiable form while examining and evaluating protections and alternate processes that can mitigate those potential risks.[4]

The E-Government Act requires agencies to conduct a privacy impact assessment before developing or procuring an information technology system or project that collects, maintains, or disseminates information in identifiable form, or before initiating a new electronic collection of information in identifiable form, from or about members of the public. Agencies are also required to make the privacy impact assessment publicly available whenever practicable.

OMB M-03-22 requires privacy impact assessments when new technologies are employed; business processes change such as when databases are merged, centralized, or matched with other databases; or when major system modifications occur such as when employing new relational database technologies.

[4] Information in identifiable form is information in a system or online collection that directly identifies an individual (e.g., name, address, social security or other identifying number or code, etc.), or by which the agency intends to indirectly identify specific individuals in conjunction with other data elements such as gender, race, date of birth, geographic indicators, etc.

The RRB began a major system modification involving the conversion to a relational database technology in October 2005, but did not consider the impact of the new privacy risks this project creates. For example, the conversion requirements/solicitation package did not specify the safeguards required of the contractor's work environment in which most of the work is being performed. We also found that while the RRB attempts to ensure all contractors are aware of their responsibilities in safeguarding PII by obtaining written certifications on Form IRM-1, many of the contractors involved in the database conversion had not been identified and certified by the Chief Privacy Officer. All data used in testing of the database conversion is acquired from the existing production databases containing PII about RRB beneficiaries.

The RRB has not implemented procedures for the completion of privacy impact assessments early in the systems development life cycle.[5] Additionally, the RRB has not provided privacy-related job-specific training to individuals responsible for systems development and/or contract administration. Although privacy issues are included in the RRB's general awareness training, the depth and breadth of this training is not sufficient to ensure they are adequately instructed about their responsibilities with respect to PII and the completion of privacy impact assessments.

A lack of risk identification when new technologies, business processes, or major system modifications are planned subjects the agency to potential exposure or compromise of PII and the resulting loss of assets.[6] For example, relational database technologies can create a more open environment and avenues for exposure of data that previously did not exist. Agencies can avoid expensive re-work and retro-fitting when the appropriate management, operational, and technical safeguards to ensure the security and confidentiality of records are considered before developing or procuring new information technology.

Recommendations

We recommend that the Bureau of Information Services:

2. implement procedures and guidelines for the completion of privacy impact assessments; and

3. conduct job-specific training on privacy impact assessments to individuals with responsibilities for performing those assessments.

[5] The Chief Privacy Officer and Security and Privacy Committee are in the process of developing procedures and guidelines for the completion of privacy impact assessments, although no target dates for implementation have been set.

[6] The resulting loss of assets can range from the use of additional resources to correct a pre-existing problem, to the costs that may be incurred when a breach has taken place and the agency needs to remedy the harm caused by that breach.

Management's Responses

The Bureau of Information Services concurs with the recommendations and will implement privacy impact assessment templates and guidelines, and conduct training.

Safeguards over Remote Access and Data Removal Need To Be Strengthened

Adequate safeguards are not in place to ensure the confidentiality of PII when remotely accessed or removed from agency premises. During our evaluation we found three situations where safeguards over PII need to be strengthened:

- PII is being handled when working at home,
- PII is accessed on agency laptops without encryption, and
- PII on mainframe tapes is transported and stored off site without encryption.

In June 2006, OMB issued memorandum M-06-16 which contained guidance for safeguarding PII that is accessed remotely or removed from agency premises. The guidance cites specific controls from the NIST SP 800-53 that agencies must comply with to properly safeguard PII. The guidance also specifies other requirements, including encryption, when PII is transported outside of the secure agency location or is stored offsite.[7]

Employees Working at Home

PII is not safeguarded when accessed in a work-at-home situation because employees use their own equipment, and the RRB is unable to control the configuration of the employee's equipment to enforce the confidentiality of PII. In an effort to provide some safeguards, the RRB has restricted certain job functions that regularly use PII from working at home. However, a recent survey of 240 employees who do work at home revealed some have used PII in work-at-home situations.[8]

In response to OMB M-06-16, the RRB issued a Rules of Behavior policy which states that RRB equipment should be used whenever possible for remote access. Additionally, the Rules of Behavior policy requires any downloaded PII stored on a remote system to be encrypted. This policy is inconsistent with the Work-At-Home policy which does not mention encryption. The Rules of Behavior policy is unenforceable regarding encryption because agency-owned laptops with encryption

[7] Other requirements include allowing remote access only with two-factor authentication, use of a time-out function, and logging and verification that sensitive data is erased when no longer needed. The agency will address the requirement for two-factor authentication after they implement the personal identity verification project for Homeland Security Presidential Directive 12. The RRB complies with the time-out function, and reported in September 2006 that they do not have a plan to implement logging and data erasure verification. The agency has previously rejected other audit recommendations for a formal audit log policy and the logging of user activity.

[8] As of February 15, 2007, the agency had a total of 451 employees and contractors with virtual private network connections and the ability to access PII remotely.

software are not available for work-at-home employees. Additionally, a lack of understanding about how PII that is accessed remotely can be exposed or accessed by unauthorized individuals in a work-at-home situation may contribute to additional risks for those employees who admitted to accessing PII at home.

Agency Laptops

In September 2006, the RRB purchased 96 new laptops and 100 licenses for encryption software. These purchases were made in order to secure PII in situations where employees need to access and store PII remotely. Deploying laptops with this encryption software adds an extra layer of security and strengthens the safeguards over PII because the encryption is performed automatically without user intervention. The RRB intends to replace the agency's existing laptops with the newly purchased and encrypted laptops. However, as of March 9, 2007 the agency had only deployed six of the newly purchased and encrypted laptops.

The agency's fixed asset inventory with respect to laptops was inaccurate and cannot support an analysis of whether all of the newly purchased laptops have been included, or whether the RRB purchased enough encryption licenses to support all agency-owned laptops.[9]

The RRB has not developed a formal deployment plan which considers the full inventory of laptops and the decommissioning of any laptop that does not have encryption software. In order to achieve full compliance with the encryption requirement in OMB M-06-16, the agency must ensure all laptops are encrypted. The Bureau of Information Services also advised us that a lack of staffing resources has prevented a fast and orderly deployment of the newly purchased laptops. Additionally, we were told that some of the agency's existing laptops are not compatible with the new encryption software.

Mainframe Data Tapes

The RRB does not have the means to encrypt mainframe data tapes containing PII. These tapes are transported to the Federal Records Center for storage. In order to properly safeguard the information, the tapes should be encrypted prior to their transport and storage. While other procedures are in place to protect data tapes during transport out of the building and when stored at the Federal Records Center, OMB M-06-16 requires that the tapes be encrypted.

The RRB considered the purchase of encryption hardware/software for mainframe tapes at the end of fiscal year 2006. However, management was unable to identify a compatible product that could be used in their information technology environment prior to fiscal year-end. Although the Bureau of Information Services has included mainframe encryption hardware/software in their fiscal year 2007 "Needs List", they have not yet recommended a suitable product for purchase.

[9] Exploration of this asset management issue is outside the scope of this evaluation.

The RRB has a fiduciary duty to protect personal information that has been entrusted to them. Inadequate safeguards over PII increases the RRB's risk for exposure, compromise, or loss of PII and can result in identity theft and/or other consequences for the beneficiaries of the RRB's programs.

Recommendations

4. We recommend that the Office of Administration revise the Work-at-Home policy to ensure its consistency with the recently adopted Rules of Behavior policy.

We recommend that the Bureau of Information Services:

5. ensure all employees are assigned an agency owned laptop with encryption software installed when they work at home;

6. develop a comprehensive plan for laptop deployment which addresses the surplus and removal of old laptops that cannot be adequately encrypted;

7. identify, purchase, and install the necessary hardware/software for mainframe data tape encryption and ensure its use on all mainframe data tapes transported off site; and

8. provide privacy and security training to all employees who have remote access to PII, or remove PII from the agency premises.

Management's Responses

The Office of Administration has considered and declined Recommendation 4, to revise the Work-at-Home policy, because they believe a Standards of Conduct clause contained within the Work-at-Home agreement sufficiently covers adherence to other agency policies released after the Work-at-Home policy was established.

The Bureau of Information Services concurs with the recommendations and will take actions to assign agency owned laptops, request the return of all old laptops, implement tape encryption, and will provide the required training.

OIG's Comments on Management's Response

The OIG agrees that the Standards of Conduct clause should be sufficient to cover policies released after the Work-at-Home policy was established. Therefore, Recommendation 4 will be closed without implementation.

Contracts Lack Privacy-Related Federal Acquisition Regulation Clauses and Language

The RRB is not consistently including privacy-related Federal Acquisition Regulation (FAR) clauses and language in their solicitations and contracts. In fiscal year 2006, the Office of Administration reviewed the language of 11 contracts for privacy related FAR clauses and found that 4 (including the contract for the agency's database conversion effort) did not include the required clauses. Additionally, the Office of Administration did not document their remedial action plans for noted deficiencies, as requested by the Chief Privacy Officer.

Our review of the contract file for the agency's database conversion effort showed that FAR language for privacy and security safeguards, including identification of the applicable system of records, was missing.

The FAR prescribes the insertion of three contract clauses pertaining to privacy. The Privacy Act Notification, consisting of two FAR clauses (52.224-1 and 52.224-2), must be included in solicitations and contracts when the contract activities include the design, development, or operation of a system of records, including the collection, use, and dissemination of records. The Privacy or Security Safeguards clause (52.239-1) must be included when the contract activity includes information technology which requires security, and/or is for the design, development, or operation of a system of records using commercial information technology services or support services.

The FAR also prescribes specific language when the contract activity includes information technology, including:

- agency rules of conduct that the contractor is required to follow;
- a list of the anticipated threats and hazards that the contractor must guard against;
- a description of the safeguards that the contractor must provide; and
- requirements for a program of Government inspection during contract performance to ensure continued efficacy and efficiency of safeguards, and the discovery and countering of new threats and hazards.

The agency has published an Administrative Circular (BSS-14) as guidance for the procurement of goods and services; however, that circular does not specify FAR requirements concerning privacy and security safeguards.

Poorly articulated privacy and security safeguards in contracts increase the risk that the RRB will be exposed to legal ramifications if PII is inappropriately exposed, compromised, or lost by contractor employees.

Recommendations

We recommend that the Office of Administration:

9. revise Administrative Circular BSS-14, Procurement of Goods and Services, to include consideration of the FAR requirements for privacy and security safeguards when contracts are established; and

10. obtain contract modifications to include the privacy and information technology related FAR clauses and language.

Management's Responses

The Office of Administration concurs with the recommendations and will initiate a revision to Administrative Circular OA-14 (which supersedes Administrative Circular BSS-14) and will obtain contract modifications.

Uncertified Contractors Encounter Personally Identifiable Information

Contractor staff handling PII are not always identified and certified by the Chief Privacy Officer prior to beginning work at the RRB. The RRB uses Form IRM-1 to document the contractor's certification that they were notified of their responsibilities when handling PII, and agree to adhere with the RRB's privacy protections. Our review of contractor staff that worked for the RRB, and had access to agency systems during fiscal years 2006 and 2007, disclosed 19 who did not sign a certification form.

The Privacy Act requires individuals involved in the design, development, operation, or maintenance of any system of records to be instructed regarding the rules of conduct and procedures adopted for the protection of the information involved. The Privacy Act also holds all government contractors and their employees to the same degree of compliance as any agency employee. The FAR clauses for privacy extend the provisions of the Privacy Act to any subcontract awarded under the initial contract. Form IRM-1 clearly states the RRB's expectations of contractor responsibility when handling PII. Contractor staff who may encounter PII must sign Form IRM-1 prior to beginning work at the RRB to ensure the safeguards are understood.

Additionally, the agency provides every RRB employee who serves as a Contracting Officer's Technical Representative an instructional letter describing their duties for ensuring contractor performance for individual contracts. However, the instructional letter does not specify any privacy or security safeguard requirements such as advising the Chief Privacy Officer whenever new contractor staff is assigned to the contract.

The Chief Privacy Officer is responsible for instructing each individual contractor employee of their responsibilities with regard to PII and for obtaining their signed certification via Form IRM-1. In this respect, the Chief Privacy Officer should be notified

of all contractor staff, and decide whether a certification is necessary. Currently, there is no control in place that would ensure the Chief Privacy Officer has been notified of any new contractor staff assigned during the life of the contract.

The RRB has provided PII access to some contractors who have not certified that they were instructed of their responsibilities for safeguarding the PII. As a result, the agency has incurred increased risk that the personal information entrusted to them may be lost, exposed, or compromised by the contractor employees.

Recommendations

We recommend that the Office of Administration:

11. develop procedures to ensure that the Chief Privacy Officer is informed of all contractors who may handle PII prior to their beginning work at the RRB; and

12. revise the Contracting Officer's Technical Representative instructional letter for privacy and security requirements, including informing the Chief Privacy Officer of all contractor staff assigned to the contract.

We recommend that the Bureau of Information Services:

13. obtain Form IRM-1 from current, uncertified contractor staff handling PII; and

14. implement a control to ensure the Chief Privacy Officer has been informed of all contractors and their assigned staff, thereby ensuring the proper contractor certifications have been obtained.

Management's Responses

The Office of Administration concurs with the recommendations and agrees to advise the Chief Privacy Officer of all contractors who may handle PII, and will review and revise the Contracting Officer's Technical Representative instructional letter to include the duty of informing the Chief Privacy Officer of contractor staff.

The Bureau of Information Services concurs with the recommendations and will obtain Form IRM-1 from current, uncertified contractor staff. The Bureau of Information Services will also propose a control for use by the Office of Administration to ensure continued contractor identification and certification.

OIG's Comments on Management's Response

While the OIG acknowledges that coordination between the Office of Administration and the Chief Privacy Officer is necessary to accomplish identification of contractor staff, the responsibility for ensuring contractor certification lies solely with the Chief Privacy Officer. As such, the OIG believes an effective process should include not only a

procedure by the Office of Administration to notify the Chief Privacy Officer of contractor staff, but a control administered by the Chief Privacy Officer to ensure that procedure is operating and producing the desired results. We urge the Chief Privacy Officer to revisit her decision to place implementation of such a control beyond her purview, thereby diminishing her effectiveness in fulfilling her responsibilities for obtaining contractor certifications.

Plan of Action and Milestones Does Not Include Privacy-Related Weaknesses

The RRB's Plan of Action and Milestones (POAM) does not reflect privacy-related weaknesses identified by the RRB in their fiscal year 2006 privacy reviews.[10]

OMB M-06-15 requested agencies to conduct reviews of their privacy-related policies and processes, and to take corrective action as appropriate. OMB also requested agencies to include any weaknesses identified in the existing security POAM required by FISMA. The Bureau of Information Services maintains the POAM and provides OMB with quarterly updates of corrective actions.

In September 2006, the Chief Privacy Officer reported four areas requiring improvement that were identified in the RRB's review for OMB M-06-15.[11] Our review of the RRB's POAMs as of September 2006 and March 2007, show that the above mentioned areas for improvement are not included; however, other required privacy-related reporting was present. When we questioned the Chief Privacy Officer in December 2006 regarding the omission of privacy-related weaknesses in the POAM, she said it did not occur to her to use the POAM and that she was not familiar with how the POAM was updated. She also indicated that resource constraints were keeping her from the in-depth analysis needed to determine what tasks were required to correct the weaknesses.

By not using the POAM as the effective tool it is meant to be, the RRB cannot provide reasonable assurance that proper safeguards are in place because weaknesses are not identified and managed efficiently.

Recommendation

15. We recommend that the Bureau of Information Services develop appropriate action plans and update the POAM for all privacy-related weaknesses.

[10] The OIG has cited the agency for an inadequate POAM in FISMA reviews since fiscal year 2003. The agency originally rejected the OIG's recommendation regarding the POAM in fiscal year 2003 (Audit Report No. 03-11, #1), but agreed to a recommendation made in fiscal year 2005 (Audit Report No. 05-11, #3). That recommendation is still pending.

[11] The Chief Privacy Officer cited the need for improvement in 1) privacy-related guidelines and training for remote users, 2) language in computer matching agreements, 3) privacy-related guidelines and training for contract officials and contractors, as well as language in contracts and memoranda of understanding, and 4) reviews of applications for access controls. Our current evaluation also reflects some of these weaknesses.

Management's Response

The Bureau of Information Services partially concurs with the recommendation and will include significant privacy related weaknesses in the POAM.

Policies and Procedures Should Explicitly Address Personally Identifiable Information

Many existing RRB policies and procedures require revision to explicitly include privacy-related issues and safeguards for PII. New procedures are also needed. For example, explicit policy and procedures on safeguarding PII during remote access or physical removal of data from the agency environment are not documented. Our review disclosed the following policies and procedures that require revision or development.

- Administrative Circular IRM-2. This document addresses the Privacy Act and the Freedom of Information Act but needs to be updated for recent OMB guidance. This document is currently undergoing revision.
- Administrative Circular IRM-5. This document is out of date concerning the destruction of sensitive information because it does not address all situations and methods in which sensitive information should be destroyed subsequent to remote access and storage on external devices.
- Field Operating Manual I. This manual contains instructions for employees in the Office of Programs for completing Form G-671. The instructions for completing this form are vague, and do not ensure that the form will contain the necessary information for the RRB's periodic review of routine use disclosures.[12]
- Personal Digital Assistant policy. This document is out of date and does not address PII safeguards.
- Laptop Loan policy. This document is out of date and does not address PII safeguards.
- No formal, documented policies and/or procedures were found to explain the scope and capabilities of the RRB's monitoring, analysis, and reporting of data extracts containing sensitive information.
- No formal, documented procedures were found to explain risk assessment updates and the criteria specifying the significant changes that prompt a risk assessment update.

[12] The term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which the record was collected. Each system of records specifies the routine use disclosures that are allowed for that system of records. The RRB uses Form G-671 to document disclosures made to third parties, which are governed by the record's routine use. As a result, Form G-671 is a primary source of information needed for the review of routine use disclosures.

OMB M-06-16 contains guidance for agencies to implement regarding sensitive information accessed remotely or removed from the agency. The guidance cites specific controls from the NIST SP 800-53, including formal, documented policies and procedures.

The Privacy Act defines routine use, conditions of disclosure, and the expected accounting of certain disclosures. OMB Circular A-130, Appendix I requires agencies to review their routine use disclosures every four years to ensure compatibility with the purpose for which the information was collected/disclosed. Our non-statistical review of several Form G-671s completed in January 2006 showed they did not always contain the information necessary to complete the routine use review required by OMB Circular A-130, Appendix I.

Although the Chief Privacy Officer has recognized that many of these policies and procedures require updates, the current lack of resources applied to the privacy program has adversely affected timely implementation.

Well documented and formulated policies and procedures help to ensure an effective program because they advise employees of management's expectations in a reliable and consistent manner. Without well documented and formulated privacy-related policies and procedures, the RRB's privacy program cannot provide reasonable assurance that PII will be safeguarded.

Recommendations

16. We recommend that the Bureau of Information Services update the policies and procedures for Administrative Circular IRM-2, Administrative Circular IRM-5, Personal Digital Assistants, Laptop Loans, audit scope and capabilities, and risk assessment updates.

17. We recommend that the Office of Programs revise the instructions for Form G-671 in the Field Operating Manual I.

Management's Responses

The Bureau of Information Services concurs with the recommendation and will update the above-mentioned documents.

The Office of Programs concurs with the recommendation and will revise the instructions for Form G-671.

List of OMB Guidance

OMB Circular A-130, Appendix I, “Management of Federal Information Resources, Federal Agency Responsibilities for Maintaining Records About Individuals,” November 28, 2000.

OMB M-03-22, “OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002,” September 26, 2003.

OMB M-05-08, “Designation of Senior Agency Officials for Privacy,” February 11, 2005.

OMB M-06-15, “Safeguarding Personally Identifiable Information,” May 22, 2006.

OMB M-06-16, “Protection of Sensitive Agency Information,” June 23, 2006.

OMB M-06-19, “Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,” July 12, 2006.

OMB M-06-20, “FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” July 17, 2006.

OMB M-07-04, “Use of Commercial Credit Monitoring Services Blanket Purchase Agreements,” December 22, 2006.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

July 24, 2007

TO : Letty Benjamin Jay
Acting Assistant Inspector General, Audit

FROM : Terri Morgan
Chief Information Officer

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

We have completed our review of the subject report dated June 22, 2007. Following are our responses to the recommendations directed to the Bureau of Information Services (BIS) for this program.

Recommendation 1

BIS: Acquire additional staffing resources to aid in the implementation of the privacy program.

BIS Response

Agree. We will begin the process to add an additional staff person for the short term by January 2008.

Recommendation 2

BIS: Implement procedures and guidelines for the completion of privacy impact assessments.

BIS Response

Agree. The draft PIA templates and guidelines introduced to the Information Security & Privacy Committee in April should be finalized and in effect by the end of this Fiscal Year September 2007

Recommendation 3

BIS: Conduct job specific training on privacy impact assessments to individuals with responsibilities for performing those assessments.

BIS Response

Agree to this from the perspective of training-the-trainer to provide the best combination of training to include program activities.

Recommendation 5

BIS: Ensure all employees are assigned an agency owned laptop with encryption software installed when they work at home.

BIS Response

Agree. Sept. 2008 for employees who handle PII and Business Sensitive Information and Sept. 2009 for all employees who work at home.

Recommendation 6

BIS: Develop a comprehensive plan for laptop deployment which addresses the surplus and removal of old laptops that cannot be adequately encrypted.

BIS Response

BIS is requesting the return of all old laptops for surplus.

Recommendation 7

BIS: Identify, purchase, and install the necessary hardware/software for mainframe data tape encryption and ensure its use on all mainframe data tapes transported off site.

BIS Response

We agree that BIS can implement tape encryption. Sept 2009.

Recommendation 8

BIS: Provide privacy and security training to all employees who have remote access to PII, or remove PII from agency premises.

BIS Response

Agree. BIS will provide this training after the WAH program is revised (#4 above). September 2008.

Recommendation 13

BIS: Obtain Form IRM-1 from current, uncertified contractor staff handling PII.

BIS Response

Agree. We will request that Acquisition Management provide us with a list of current contract employees and obtain Form IRM-1 from those who have not completed one. Sept 2007 BIS-IRMC

Recommendation 14

BIS: Implement a control to ensure the Chief Privacy Officer has been informed of all contractors and their assigned staff, thereby ensuring the proper contractor certifications have been obtained.

BIS Response

BIS-IRMC will propose a control by Dec 2007 for use by OA at which time this recommendation should be considered implemented. OA will need to assume responsibility for implementing it per recommendation 11.

Recommendation 15

BIS: Develop appropriate action plans and update the POAM for all privacy-related weaknesses.

BIS Response

BIS needs to focus its limited resources in significant areas that need attention. The POAM will include action plans for significant privacy related weaknesses.

Recommendation 16

BIS: Update the policies and procedures for Administrative Circular IRM-2, Administrative Circular IRM-5, Personal Digital Assistants, Laptop Loans, audit scope and capabilities, and risk assessment updates.

BIS Response

BIS-IRMC has developed a chapter in the handbook Chapter 22 –Protecting Sensitive Information that addresses PII and will make any additional changes needed by for the above-mentioned documents. March 2008

cc: Director of Administration
Director of Programs
Chief Privacy Officer

UNITED STATES GOVERNMENT

MEMORANDUM

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

July 3, 2007

TO : Letty Benjamin Jay
Acting Assistant Inspector General, Audit

FROM : Henry M. Valizlisar
Director of Administration/Senior Executive Officer

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

This is in reply to your June 22, 2007 memorandum regarding the above subject. The following are the Office of Administration's responses to the recommendations directed to our organization.

Recommendations

4. We recommend that the Office of Administration revise the Work-at-Home policy to ensure its consistency with the recently adopted Rules of Behavior policy.

Response -- The current Work-at-Home Program (WAH) already accomplishes the suggested recommendation. The Program includes an Agreement which each WAH participant signs and clearly states the following:

Standards of Conduct

"Employee agrees he or she is bound by agency standards of conduct while performing official duties at the home work site."

I believe that the statement covers any and all policies that the agency currently has or will have concerning employee conduct while working at home. I would hesitate to specifically address the Rules of Behavior Policy individually because to do so would require us to individually address all other policies that deal with employee conduct. The purpose of the above statement was not only to cover any policy on conduct that might be applicable at the time that the Agreement was written but to also cover any future policies that might be applicable.

Additionally, the WAH Program and the WAH Agreement has been negotiated with the AFGE. To make any revisions to the Agreement or the program would require negotiations with the union. I don't believe that renegotiating the WAH Agreement is necessary because the Rules of Behavior Policy is covered by the current standards of conduct statement.

9. Revise Administrative Circular BSS-14, Procurement of Goods and Services, to include consideration of the FAR requirement for privacy and security safeguards when contracts are established.

Response -- The Acquisition Management Division (AM) will initiate the suggested revision to Administrative Circular OA-14. This circular was just recently updated but will be revised by the end of the year.

10. Obtain contract modifications to include the privacy and information technology related FAR clauses and language.

Response -- AM will provide the Chief Privacy Officer (CPO) with a list of contracts by July 15, 2007 for review and concurrence and will complete modifications by August 15, 2007. AM will work with the CPO to develop appropriate language for provisions when required by the FAR, but not specified in the FAR clause proper, that shall set forth Contractor and Government responsibilities.

11. Develop procedures to ensure that the Chief Privacy Officer is informed of all contractors who may handle PII prior to their beginning work at the RRB.

Response -- AM will identify planned acquisitions to the CPO that may involve PII during the preparation stage. The program office or bureau designated official nominated as the Contracting Officer's Technical Representative (COTR) will, in conjunction with the CPO, inform AM staff that a planned acquisition will involve PII and request inclusion of relevant clauses and provisions in the contract.

12. Revise the Contracting Officer's Technical Representative instructional letter for privacy and security requirements, including informing the Chief Privacy Officer of all contractor staff assigned to the contract.

Response -- AM will review the COTR appointment and instructional letter to include that duty in the next COTR appointment letter issued.

cc: Executive Assistant
Director of Human Resources
Supervisory Contract Specialist

UNITED STATES GOVERNMENT

MEMORANDUM

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

JUL 17 2007

TO: Letty Jay
Acting Assistant Inspector General, Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

THROUGH: Dorothy Isherwood
Director of Programs

SUBJECT: **Draft Report – Evaluation of the RRB's Privacy Program**

Overall Comments

There is one recommendation that impacts the Office of Programs. Our response is below.

Recommendation 17

We recommend that the Office of Programs revise the instructions for Form G-671 in the Field Operating Manual.

OP Response

We concur. Based on the OIG's evaluation of the Railroad Retirement Board's Privacy Program, the instructions for completing the G-671 will be clarified to ensure that the form requests the necessary information, as required, for RRB's periodic review of routine use disclosure. The revised form requires additional identifying information, such as, the type of information being requested, the name of the requestor, and how and why the information is needed.

Policy and Systems requested comments on a revision to FOM1 1720 to include more complete and detailed instructions for completing the G-671 (which has also been revised and will be made available on RRAILS) on July 2, 2007. Once the comments have been received and incorporated, the revision will be loaded to PRISM production. The expected completion date is August 30, 2007.

---

cc: Director of Policy and Systems