# PRIVACY IMPACT ASSESSMENT

| | |
|---|---|
| **SYSTEM OR APPLICATION NAME:** | Railroad Service and Compensation Reports<br>(Forms AA-12, BA-6a, G-88A.1 and G-88A.2) |
| **DATE:** | October 17, 2007 |
| **SYSTEM OWNER & TITLE:** | Ronald Russo, Director<br>Policy & Systems |
| **CONTACT POINT:** | Kimberly Price-Butler (312) 751–4383<br>Pauline Coleman-Sutton (312) 751-4508 |
| **ORGANIZATION:** | Office of Programs<br>Policy & Systems |
| **REVIEWING OFFICIAL NAME & TITLE** | Ronald J. Hodapp, Chief |
| **ORGANIZATION:** | Information Resources Management Center<br>Bureau of Information Services |

## Overview

The primary function of the U. S. Railroad Retirement Board (RRB) is to determine and pay retirement-survivor and unemployment-sickness benefits under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA) to the nation's railroad workers and their families. The benefit payments administered by the RRB are based on earnings credits with covered railroad employers ("employers"), called creditable service and compensation. Service and compensation information is collected from employers via service and compensation reports. The RRB maintains lifetime records of creditable service and compensation for each railroad employee for purposes of determining eligibility for and amount of, benefits due under the laws it administers.

The RRB is authorized to require an employer to submit service and compensation information by RRB Regulation (20 CFR 209.2) and by RRA sections 7(b)(6) and 9, and RUIA sections 6 and 12(l). Both Acts make provision for enforcement of reporting requirements, as well as providing authority to collect the social security account numbers associated with the earnings.

In order to achieve that goal, employers file the following service, compensation and address reports which contain personally identifiable information (PII) on behalf of its employees:

- Form AA-12, Notice of Death and Request for Service Needed for Eligibility;
- Form BA-6a, Form BA-6 Address Report;
- Form G-88A.1, Request for Verification of Date Last Worked; and
- Form G-88A.2, Notice of Retirement and Request for Service Needed for Eligibility.

Forms AA-12, G-88A.1 and G-88A.2 are used by the RRB to secure lag service and compensation for former and deceased employees when information is needed to determine benefit eligibility from railroad employers. Lag service is defined as the period of time between the date of the last record of employment processed by the RRB from Form BA-3, Annual Report of Creditable Compensation and the employee's death or retirement. Form BA-6a is used by railroad employers to report the addresses of newly hired employees. The forms contain employee name, social security number, address, calendar year service and compensation data, dates of birth and death (if applicable) as well as the employer identification number. In order to reduce the risk of exposure of PII, completed Forms AA-12, G-88A.1 and G-88A.2 are received at the RRB via facsimile. A new electronic method of submitting Form BA-6a has also led to a reduction of risk of exposure of PII. The addition of File Transfer Protocol (FTP) offers an alternative to employers that previously mailed electronic media to the RRB. The paper reporting of Form BA-6a still exists with privacy and security methods in place to protect the data. All paper reports are kept in a secure location and disposed of properly.

## Section 1.0 -- The System and the Information Collected and Stored within the System

1.1 What information is to be collected?

Covered railroad employers submit the following data to the RRB on the forms listed below:

- Form AA-12, Notice of Death and Request for Service Needed for Eligibility - The tax year, railroad employer number, payroll number, corporate name of the railroad employer, employees' social security numbers, employees' names, creditable RUIA compensation, RUIA maximum benefit amount, creditable service months, total creditable service months, employees' street address, city, state, zip code, Tier 1 compensation, Tier 2 compensation, miscellaneous compensation, sick pay, last daily pay rate and effective date of address.
- Form BA-4, Report of Creditable Compensation Adjustments – Railroad employers use this form to submit corrections or adjustments to every data element submitted on Form BA-3 with the exception of address data.
- Forms G-88A.1, Request for Verification of Date Last Worked and Notice of Retirement and Request for Service Needed for Eligibility, respectively – Railroad employer's name, address and employer number, employee's social security number, name, payroll number, job title, work location, department or division, date last worked or paid for time lost, date rights relinquished and creditable service months for the current and prior year.

1.2 From whom is the information collected?

The information is collected from employers covered under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA).

1.3 Privacy Impact Analysis: What are the privacy risks associated with the information collected?

The railroad service and compensation reports contain sensitive information which needs to be protected while being collected from railroads and stored by the RRB. All methods of submission by employers are processed in a secure manner to ensure employee privacy.

## Section 2.0 -- The Purpose of the System and the Information Collected and Stored within the System

2.1 Why is the information being collected?

The information is collected to determine entitlement to and amount of benefits payable under the RRA, the RUIA and the Social Security Act (SSA), if applicable. Forms AA-12, G-88A.1 and G-88A.2 are only used if lag service is needed for a particular employee's benefit eligibility. The records are updated daily based on earnings reports received from railroad employers and the SSA and are stored in the Employment Data Maintenance (EDM) database.

2.2 What specific legal authorities, arrangements, agreements authorize the collection of information?

To enable the RRB to establish and maintain the record of creditable service and compensation, employers are required under Sections 6 of the RUIA and Section 9 of the RRA to file with the RRB, in such manner and form and at such times as the RRB prescribes, reports of compensation of employees. The reporting requirements are identified in 20 CFR 209.

2.3 Privacy Impact Analysis: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

Privacy Risk: Collection of extraneous information
Mitigation: The Employment Data Maintenance (EDM) database contains only those data elements needed to accomplish the mission of the agency which is the payment of benefits under the two acts it administers – the RRA and the RUIA.

Privacy Risk: Inaccurate information is attributed to the individual
Mitigation: The identity of the social security number holder is verified by through an exchange with the Social Security Administration. Once verified, active employees are sent an annual Certificate of Service Months and Compensation (Form BA-6). The BA-6 is the basis for filing a protest if the employee disagrees with the service and or compensation that has been reported on his behalf by his railroad employer(s) for the previous tax year.

## Section 3.0 -- Uses of the System and the Information

3.1 Describe all uses of the information.

The purpose of this system is to store railroad earnings of railroad employees which are used to determine entitlement to and amount of benefits payable under the RRA, the RUIA and the Social Security Act, if applicable. The records are updated daily based on earnings reports and/or subsequent adjustment reports received from railroad employers and the SSA; the results of which are stored in the Employment Data Maintenance Application database.

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

The information collected is derived from various earnings reports which are submitted by covered employers not “individuals”. The reports are checked for accuracy by editing programs that identify illogical data entries. The editing programs prevent erroneous data from being posted to an individual’s record. If the earnings reports pass the initial editing programs, the data within the report it is subsequently checked for accuracy through the release of an employee’s Form BA-6 described above.

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

| **Type** | **Retention** |
|---|---|
| Magnetic Tape/Disk | Permanent retention; updated annually |
| Paper | Retained for five years and destroyed. Prior year ledger placed in storage when current year ledger is complete. |
| Database Records | Retained Indefinitely |

3.5 Privacy Impact Analysis: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

The earnings data stored within EDM is used internally by RRB systems to pay benefits under the RRA and RUIA once a properly executed application for such benefits has been filed by the employee and/or other qualified individual. Until such time as an application for benefits is filed, the earnings data is stored for future entitlement. Established rules of behavior exist for those persons who must access the information to perform their jobs in the payment of those benefits.

| **Input Type** | **Risk** | **Mitigation** |
|---|---|---|
| Magnetic Tape | Unauthorized Disclosure | Handled by authorized personnel on a need to know basis. Computer and computer storage rooms are restricted to authorized personnel. |
| Paper Form | Unauthorized Disclosure | Delivered in a sealed envelope; handled by authorized personnel on a need to know basis. Mainframe processing. Paper is bound in hard covers and stored in on steel shelving accessible to only authorized personnel. |
| Secure FTP (future use) and Secure Email | Unauthorized Disclosure | Encrypted, password protected secured email or FTP; accessible by only authorized personal. Direct mainframe processing. |
| Diskette, CD/ROM | Unauthorized Disclosure | Delivered in a sealed envelope; handled by authorized personnel on a need to know basis. Mainframe processing. Disk//CD's are stored in a secured location that is only accessible by authorized personnel. |
| Internet/ERS | Unauthorized Disclosure | Encrypted, password and PIN protected secured transmission residing behind multi--layer firewall protection in an environment controlled by security software and technology based upon a need to know access and least privilege policy. |

## Section 4.0 -- Internal Sharing and Disclosure of Information within the System

4.1 With which internal components of the RRB is the information shared?

The data is shared and used by all internal RRB components and processes involved in the payment of benefits under the RRA and the RUIA and other authorized users on a need to know basis. Access is restricted to only those authorized employees and officials who need it to perform their official duties. Established rules of behavior exist for those persons who must access the information to perform their jobs in the payment of those benefits.

4.2 For each recipient component or office, what information is shared and for what purpose?

The information shared is the same as what is collected and stored within EDM which is used to determine eligibility for, and amount of, benefits payable under the RRA and the RUIA.

4.3 How is the information transmitted or disclosed?

The data received from covered employers on Form BA-6a is transmitted via paper, magnetic tape, diskette, CD Rom, secure email and the Internet. We are now proposing the use of FTP as additional means of transmittal. The data received from covered employers on Forms AA-12, G-88A.1 and G-88A.2 is received via facsimile.

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

The RRB has established security and privacy awareness training; quarterly access reviews; and standard rules of behavior for users to mitigate unauthorized access.

## Section 5.0 -- External Sharing and Disclosure

5.1 With which external (non-RRB) is the information shared?

The earnings data stored within EDM is proprietary information provided to the RRB by covered employers. As such, earnings information is frequently exchanged between the RRB and said covered employer who is the owner and source of the data. Information is also shared with the Social Security Administration (SSA) to determine which agency (either the RRB or SSA) has jurisdiction for the benefit payment. In many cases, SSA is the source agency of some of the data maintained in EDM.

5.2 What information is shared and for what purpose?

The System of Records (SOR) RRB-5, RRB-22 and the Memorandum of Understanding (MOU) with SSA describes the routine disclosures of information with external users.

5.3 How is the information transmitted or disclosed?

Information may be disclosed in any form, provided the release of information is authorized under RRB-5, RRB-22 or the MOU with SSA.

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

In order to prevent theft or accidental use, RRB has established MOUs with SSA. Confidentiality and Privacy Act Statements are also included within contracts for work performed by approved vendors which provide standard rules of behavior to mitigate the redisclosure of the data once accessed.

5.5 What type of training is required for users from agencies outside RRB prior to receiving access to the information?

External users do not have direct access to the information; instead, it is provided to them in a manner and format that is defined by a MOU, contract or written request that falls within the acceptable uses in the SOR.

5.6 Are there any provisions in place for auditing the recipients' use of the information?

No.

5.7 Privacy Impact Analysis: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

Data is only shared with the individual owner of their employment data, covered railroad employers, and those external agencies and individuals who have a need to know such data or are authorized to receive such data as established by MOU, SOR or other agreement. The RRB uses standard safeguards, security measures and rules of behavior to mitigate risks of unauthorized use and redisclosure.

## Section 6.0 – Notice

6.1 Was any form of notice provided to the individual prior to collection of information?

In compliance with the Paperwork Reduction Act of 1995, a notice of collection is posted in the Federal Register regarding the obligation of covered employers to provide the requested data on behalf of the individual employees. A notice is also published on the RRB.GOV web site under RRB Privacy Act System of Records using text link RRB-5 and RRB-22.

6.2 Do individuals have an opportunity right to decline to provide information?

No. Covered employers (not individuals) are obligated to provide the information to the RRB or risk penalties and or prosecution for failure to report.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Yes. Individuals can provide written authorization to have information released to a third party that falls outside of the routine uses of information as provided under the Privacy Act or as described in SOR RRB-5 and RRB-22.

6.4 Privacy Impact Analysis: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The RRB Privacy Act System of Records RRB-5 and RRB-22 authorizes the release of information to certain entities. Disclosure of information to an entity not previously identified in RRB-5 and RRB-22 is prohibited without the written authorization of the individual employee. Access to employee's earnings data is restricted to only those authorized RRB users and officials who need it to perform their official duties.

## Section 7.0 -- Individual Access and Redress

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Active employees are annually provided a Form BA-6, Certificate of Service Months and Compensation, which details the earnings data provided by their employer(s) for the previous calendar year.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

If a person disagrees with the earnings data that has been reported to the RRB by their employer(s), Form BA-6 includes instructions on how to file a protest regarding the disputed earnings data. A person may also request reconsideration of any adverse benefit determination based on the reported earnings. Instructions for filing a request for reconsideration are included in the RRB benefit denial or award letter. Individuals may also request to review and amend information maintained in the Privacy Act systems of records RRB-5 and RRB-22 as described in the notice published on RRB's website and in the Federal Register.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives to the individual?

N\A

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

If a person disagrees with the earnings data that has been reported to the RRB by their employer(s), Form BA-6 includes instructions on how to file a protest regarding the disputed earnings data. A person may also request reconsideration of any adverse benefit determination based on the reported earnings. Instructions for filing a request for reconsideration are included in the RRB benefit denial or award letter.

## Section 8.0 -- Technical Access and Security

8.1 Which user will have access to the system?

Access is restricted to only those authorized employees and officials on a need- to-know basis to perform their official duties. Authorization procedures not only authorize access, but also determines what information a covered employers; agency or individual can have access to, once access is authorized.

8.2 Will contractors to the RRB have access to the system? If so, please submit a copy of the contract describing their role with this PIA?

Contractors are not provided direct access to the system; rather data is provided to them in a limited format. See attached contract for RRB Tax Statements, BA-6 Forms and Rate Letters.

8.3 Does the system use "roles" to assign privileges to users of the system?

Role-based access is granted by the system administrator. Systems owners have established access/security profiles for the authorized users. Access is granted based on established profiles which identify the user's name, position and job title. System owners conduct regular periodic reviews to mitigate unwarranted access. User access is granted on a need-to-know basis.

8.4 What procedures are in place to determine which users may access the system and are they documented?

The system administrator/owner reviews and or changes previously approved access based on any change in roles or job responsibilities. Access/security profiles are established for all authorized users. Access is granted based on established profiles which identify the user's name, position and job title. Periodic reviews are conducted to mitigate unauthorized access. User access is granted on a need-to-know basis.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

The system administrator/owner review approved access on a quarterly basis based on any change in roles or job responsibilities Access/security profiles are established for the authorized users. Access is granted based on established profiles which identify the user's name, position and job title. Periodic reviews are conducted to mitigate unauthorized access. User access is granted on a need-to-know basis. System audit trails are reviewed periodically and maintained and stored offsite.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

EDM creates an electronic audit trail for each transaction that posts or edits data within an individual record that identifies the person or process that initiated the transaction. The system audit trails can not be compromised and are maintained offsite. Rules of behavior are established to prohibit misuse of data.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Security and privacy awareness training is provided to all RRB system users and owners. Once approved, new users receive the appropriate training on how to access the database and are trained on the need to protect the confidentiality of the records accessed. Users are required to complete the appropriate access authorization form before access is granted.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification and Accreditation last completed?

The data is secured with comparable requirements to those of FISMA.

8.9 Privacy Impact Analysis: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

Periodic reviews are conducted to mitigate unwarranted privacy risks and unauthorized access. User access is granted on a need-to-know basis. System audit trails are created for each transaction that posts or edits data within an individual record that identifies the person or process that initiated the transactions. The system audit trails can not be compromised and are maintained offsite. Rules of behavior are established to prohibit misuse of data.

## Section 9.0 -- Technology

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

The RRB applies standard computer security system controls to protect the data stored on EDM. Network monitoring and intrusion detection systems monitors all user traffic for various, worms, spy ware; etc and utilizes encryption technology, where appropriate. Network access monitors user attempts to gain access and allows or denies access based on preset parameters.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

Standard computer security business rules are applied based on systems rated at medium risk.

9.3 What design choices were made to enhance privacy?

Transmission alternatives, including secure email and FTP, rather than design choices were implemented to enhance privacy. Both alternatives offer an alternative to employers who previously mailed either electronic or paper reports to the RRB.

9.4 Privacy Impact Analysis: Given the technology and design choices, what privacy risks were identified and describe how they were mitigated?

Offering transmission alternatives to railroad employers decreases the privacy risks for electronic and/or paper reports that had been previous mailed. This change in reporting methods minimized the number of points of vulnerability by decreasing manual handoffs during the posting process. These reports contain PII, which could possibly be exposed in delivery. The proposed use of FTP by railroad employers will replace the US Postal Service mailing of these reports in an effort to further protect privacy for reports that were previously mailed to the RRB.