



PRIVACY IMPACT ASSESSMENT

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service
(Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

CONTACT POINT: Ronald Russo, Director
Policy & Systems

PREPARER NAME & TELEPHONE: Kimberly Price-Butler (312) 751-4383
Pauline Coleman-Sutton (312) 751 - 4508

ORGANIZATION: Office of Programs
Policy & Systems,

REVIEWING OFFICIAL NAME & TITLE Ronald J. Hodapp, Chief

ORGANIZATION: Information Resources Management Center
Bureau of Information Services

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

Overview

Under Section 2 of the Railroad Unemployment Insurance Act (RUIA), one of the primary functions of the U. S. Railroad Retirement Board (RRB) is to determine and pay unemployment and sickness benefits to the nation's railroad workers. These benefits are generally payable for each day of unemployment or sickness in excess of four during a registration period (normally a period of 14 calendar days). Section 12 of the RUIA provides that the RRB establish, maintain and operate free employment facilities, directed toward the reemployment of railroad employees. In order to apply for unemployment benefits, employees must file Form UI-1, Application for Unemployment Benefits and Employment. If the employee is qualified based on minimum earnings and proves to be otherwise entitled, the employee is subsequently provided Form UI-3, Claim for Unemployment Benefits. The procedures for applying for the unemployment benefits and employment service and registering and claiming benefits by mail are prescribed in RRB regulation 20 CFR 325.

Prior to 2004, the application and claim procedures were paper-based processes submitted via the United States Postal Service to their local RRB field office. While the paper-based processes are still available, in keeping with the Government Paperwork Elimination Act (GPEA), the RRB developed an application called RUIAnet which provided unemployed railroad workers the option of applying for railroad unemployment benefits (Form UI-1) over the Internet. The ability to file unemployment claims (Form UI-3) over the Internet was launched later that same year.

RUIAnet is a web-based application for unemployment benefits that collects essentially the same information and serves the same basic function as the paper-based Forms UI-1 and UI-3. Employees can access these services by visiting the RRB's website at www.rrb.gov after establishing an Internet Services account. In order to establish an RRB Internet Services Account, employees must apply for a Password Request Code (PRC) to ensure security. After receiving the PRC, employees instructed to create a personal identification number (PIN) that is used in conjunction with their password.

The data that is collected from Forms UI-1 and UI-3 via RUIAnet or paper is the same and includes the following:

- Form UI-1, Application for Unemployment Benefits and Employment Service – Personally identifiable information including name, social security number, date of birth, address, telephone number and gender; employment information including name of last railroad employer, job title, location of last railroad job and reason for not working; other information including school information, other benefits a person may be receiving and direct deposit information.
- Form UI-3, Claim for Unemployment Benefits – The dates claimed as days of unemployment within the designated claim period, the gross amount of any wages/pay received for the days within the designated claim period, the name of employee's last railroad employer, the last railroad job, the reason not working and other questions pertaining to benefits and employment since the employee last worked.
-

Data from both paper or Internet filed unemployment applications and claims is entered on the Railroad Unemployment Claims System (RUCS).

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

1.1 What information is to be collected?

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

The following data is collected on the forms listed below:

- Form UI-1, Application for Unemployment Benefits and Employment Service – Personally identifiable information including name, social security number, date of birth, address, telephone number and gender; employment information including name of last railroad employer, job title, location of last railroad job and reason for not working; other information including school information, other benefits a person may be receiving and direct deposit information.
- Form UI-3, Claim for Unemployment Benefits – The dates claimed as days of unemployment within the designated claim period, the gross amount of any wages/pay received for the days within the designated claim period, the name of employee's last railroad employer, the last railroad job, the reason not working and other questions pertaining to benefits and employment since the employee last worked.

1.2 From whom is the information collected?

The information is collected from railroad employees who want to file for and claim unemployment benefits payable under the Railroad Unemployment Insurance Act (RUIA).

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

The unemployment and claim data collected from employees contain sensitive information which needs to be protected while being collected. All methods of submission by employees (both Internet and paper) 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 support the payment of unemployment benefits to qualified railroad employees under the RUIA. The information from the forms is entered into the Railroad Unemployment Claim System (RUCS) and is extracted for batch processing which may result in the issuance of a claim or payment for a previously filed claim.

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

Sections 2 of the RUIA provided unemployment benefits for qualified railroad employees. The procedures for applying for the unemployment benefits and employment service and registering and claiming benefits by mail are prescribed in RRB regulation 20 CFR 325. The procedure for applying and claiming RUIA benefits via the Internet is in RRB regulation 20 CFR 321.

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 Railroad Unemployment Claim System (RUCS) database contains only those data elements needed to accomplish the mission of the agency which is the payment of benefits under the RUIA.

Privacy Risk: Inaccurate information is attributed to the individual

Mitigation: RUIAnet includes a front-end authentication system using a PIN/password process that can only be established by the employee. Both processes (paper-based or Internet) will generate an acknowledgement letter and claim form(s) to be mailed to the claimant and prepayment notices to the person's employer for additional verification.

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

Privacy Risk: Risk of intrusion.

Mitigation: The risk of intrusion is dealt with by security requirements that the RRB imposes on the web host. Application and claims data are kept on the RUCS mainframe database, which is not modifiable by the public.

Section 3.0 -- Uses of the System and the Information

3.1 Describe all uses of the information.

RUCS is an interactive database used by RRB offices to input RUIA benefit applications and claims, and perform other functions related to the maintenance of unemployment and sickness beneficiary rolls.

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?

RRB claims examiners adjudicate applications and claims for unemployment benefits by entering data from Forms UI-1 and UI-3 onto RUCS which also has built-in edits for certain logical entries. Subsequent reviews of data occur by multiple entities (RRB and Office of Inspector General staff as well as railroad employers) through program integrity activities to ensure that the right amount of benefits are both paid and recovered.

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)?

<u>Type</u>	<u>Retention</u>
RUCS Database	Purged upon request based on RRB parameters
Paper	Retained for six years and 3 months before it destroyed

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 unemployment application and claims data stored within RUCS is used internally by RRB systems to pay benefits under the RUIA once a properly executed application for such benefits has been filed by the employee and/or other qualified individual. Established rules of behavior exist for those persons who must access the information to perform their jobs in the payment of those benefits.

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 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?

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

The information shared is the same as what is collected and stored within RUCS, an interactive database used by RRB offices to input RUIA benefit applications and claims, and perform other functions related to the maintenance of unemployment and sickness beneficiary rolls.

4.3 How is the information transmitted or disclosed?

The unemployment and claim data received from railroad employees on Forms UI-1 and UI-3 BA-3 and BA-4 is transmitted via paper or Internet.

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 help mitigate improper disclosure.

Section 5.0 -- External Sharing and Disclosure

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

Information may be shared with any number of entities provided that the employee has provided written authorization of its disclosure or the disclosure is covered under the Privacy Act System of Records (SOR) RRB-6, Unemployment Insurance Record File and RRB-7, Applications for Unemployment Benefits and Placement Service under the Railroad Unemployment Insurance Act.

5.2 What information is shared and for what purpose?

The SOR RRB-6 and RRB-7 describe 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 the SOR.

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

No.

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 the written request or is considered acceptable by 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 the data, their railroad employer(s), and those external agencies and individuals who have a need to know such data or are authorized to receive such data as established by the SOR or employee authorization. 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?

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

The Privacy Act Notice, the Computer Matching and Privacy Protection Act Notice and the Paperwork Reduction Act Notice are provided in Form UB-10, Unemployment Benefits for Railroad Employees, a booklet that includes Form UI-1. Form UI-3, Claim for Unemployment Benefits, also includes a reminder to employees to check Form UB-10 for such notices. Links for the notices are also available within the RUIAnet application on the RRB.GOV web site. Links to the SOR RRB-6 and RRB-7 are also available.

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

Individuals have the right to decline to provide information. However, the RRB cannot pay benefits without such information.

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. Other than information that may be disclosed routinely under the Privacy Act or as described in SOR RRB-6 and RRB-7, no other information about an employee's application or claims for benefits may be disclosed without that person's written consent.

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-6 and RRB-7 authorizes the release of information to certain entities. Disclosure of information to an entity for a purpose not previously identified in RRB-6 and RRB-7 is prohibited without the written authorization of the individual employee. Access to employee's application and claims 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?

An employee may request reconsideration of any adverse benefit determination based on information received from numerous sources which may affect the payment of a claim. Instructions for filing a request for reconsideration are included in the RRB benefit denial letter. Individuals may also request to review and amend information maintained in the Privacy Act systems of records RRB-6 and RRB-7 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.

An employee may request reconsideration of any adverse benefit determination based on information received from numerous sources which may affect the payment of a claim. Instructions for filing a request for reconsideration are included in the RRB benefit denial letter.

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

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?

No

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?

RUCS contains a 'transaction history' of every adjudicative determination that is input into the database which identifies the RRB employee who entered the transaction as well as the date. RUCS entries are extracted daily for batch processing and once extracted, transactions can not be altered. 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.

SYSTEM OR APPLICATION NAME: Application and Claim for Unemployment Benefits and Employment Service (Forms UI-1, UI-1 (Internet), UI-3 and UI-3 (Internet))

DATE: October 17, 2007

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 entered on RUCS that identifies the person who initiated the transaction. The RUCS transactions are extracted daily for batch processing and once extracted, the entries can not be compromised. 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 RUCS. 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 Internet filing, rather than design choices were implemented to enhance privacy. This option offers an alternative to employees who previously mailed paper forms 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 this transmission alternative to railroad employees decreases the privacy risks for paper forms that had been previously mailed. This change in filing methods minimizes the number of points of vulnerability by decreasing manual handoffs during the adjudicative and mailing processes. These forms contain PII, which could possibly be exposed in delivery.