PRIVACY IMPACT ASSESSMENT

SYSTEM OR APPLICATION NAME:	Financial Management Integrated System (FMIS)
DATE:	October 28, 2015
SYSTEM OWNER & TITLE:	Thomas M. McCarthy Chief, Treasury, Debt Recovery and Financial Systems Division
CONTACT POINT	Kristofer Garmager Financial Management and Program Analyst
ORGANIZATION:	Bureau of Fiscal Operations U.S. Railroad Retirement Board 844 North Rush Street Chicago, IL 60611-2092
REVIEWING OFFICIAL NAME & TITLE	Charles P. Mierzwa Chief of Information Resources Management
ORGANIZATION:	Bureau of Information Services Information Resources Management Center U.S. Railroad Retirement Board 844 North Rush Street Chicago, IL 60611-2092

SYSTEM OR APPLICATION NAME:	Financial Management Integrated System
DATE: OCTOBER 28, 2015	

Overview

The RRB Financial Management Integrated System (FMIS) utilizes a contractor provided, (CGI Federal) cloud based Infrastructure-as-a-Service (IaaS). CGI Federal IaaS cloud based FMIS system is Federal Risk Authorization Management Program (FedRAMP) approved for data at the 'Moderate' security level as defined by guidance provided by OMB Federal Enterprise Architecture Program Management Office Business Reference Model 2.0, and FIPS Pub 199, *Standards for Security Categorization of Federal Information and Information Systems* which is based on NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*. CGI Federal received FedRAMP certification and approval from the Joint Authorization Board (JAB) as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DOD) and Department of Homeland Security (DHS).

Overview of CGI Federal Infrastructure-as-a-Service (IaaS):

The CGI IaaS Cloud service provides Virtual Machine and Web Hosting services in the cloud enabling scalable, redundant, dynamic computing services. The CGI IaaS Cloud service allows Federal agencies, local and state governments, and tribal organizations to procure and provision computing services and Web hosting services online via the Internet.

The CGI IaaS Cloud is designed to be scalable to permit a customer to request computing services and capacity on-demand and provision services and capacity dynamically. The CGI IaaS Cloud provides a high-availability infrastructure through hardware with redundant internal components and a redundant architecture that enables automatic failover of the infrastructure components that operate the CGI IaaS Cloud.

RRB FMIS Applications hosted on the CGI Federal Infrastructure as a Cloud based Service (IaaS):

Automated FMIS Applications:

- Central Contractor Registration Connector (CCRC). The CCRC is used to upload and process daily System Award management (SAM) files which then update the vendor records in FMIS
- Cost Accounting. The Cost Accounting application produces accurate and timely information for RRB management and other Federal government agencies to permit cost comparison and analysis.
- Employer Contribution & Collection System (ECCS). ECCS is an RRB internal application used for tracking employer contributions and collections.
- Electronic Government Travel (E-Gov Travel). E-Gov Travel is government wide, web-based, world-class travel management service. It was launched in April 2002 to save significantly on costs and improve employee productivity.
- Federal Business Opportunities (FedBizOps). FedBizOps is where we post solicitations for services and products.

- Federal Procurement Data System – Next Generation (FPDS-NG). FPDS is the system where we report all procurements over $3K and provide information such as the vendor, description of products/services, services dates, whether it was competed and how it was competed. FPDS is the government site that transmits all government spending information to the usaspending.gov site to provide information to taxpayers on government spending.

- GSA Payroll & Transit Benefits. RRB employee payroll and transit benefits are managed through the GSA national payroll and transit benefits application.

- Government wide Treasury Account Symbol (GTAS). GTAS is the application we use to provide Department of the Treasury with accounting information.

- Program Accounts Receivable (PAR). PAR is an RRB internal application that is used to track program accounts receivable.

- System for Award Management (SAM). Vendors that do business with the government must be registered on SAM. Their registration on SAM includes their business information, TIN, DUNS, address, banking information, Representations and Certifications, as well as contact information. We log into SAM in order to check vendor records and also to download daily SAM files which provide updates on the vendors in SAM. We take those daily files and upload and process them in CCRC which then updates our vendor records in FMIS.

- Transaction Reporting System (TRS). TRS is a system used to collect deposit data for the RRB.

Manual FMIS Applications (Applications that require RRB staff interaction):

- Actuarial and Research Reports. Data supplied by the Office of Actuary to support various accounting functions and financial statements.

- Bureau of Public Debt. This is a shared government service that is used to pay for employee change of station moves.

- Government wide Treasury Account Symbol (GTAS). GTAS is the application we use to provide Department of the Treasury with accounting information.

- Railroad Retirement Act (RRA) and Railroad Unemployment Insurance Act (RUIA) Awards Processing. Multiple RRB specific applications used to pay RRA and RUIA benefits.

- Secure Payment System (SPS). SPS is the application that we use to certify payments for the Department of the Treasury to make on our behalf.

Section 1.0 – The Nature of the Information in the FMIS System and Its Source.

In general the Financial Management Integrated System does not process RRB beneficiary information since its core purpose is financial management. However, FMIS does work with the following personal information:

- Personal information of the RRB annuitants and beneficiaries - The following information is collected by the Programs Account Receivable (PAR) application as needed to process billing and dunning (collection) notices:
    - Name (First name, Last name, Middle name),
    - Home Address (of record), and
    - Taxpayer Identification Number (TIN) / Social Security Number (SSN).
- RRB Employee - The following RRB employee information is collected to process monetary transactions with employees such as travel, relocation and medical reimbursements. The FFS application contains the following Personally Identifiable Information (PII) and other sensitive employee information to allow for the proper financial accounting of funds disbursed to employees:
    - Name (Last name, First name, Middle name),
    - Social Security Number (SSN), and
    - Bank information
- Other – All other information collected or distributed to the Financial Management Integrated System is for used for accounting and financial processing as designed by the core functional capabilities of the system and does not specifically identify any person or organization specifically. Other data includes:
    - Budget execution data,
    - Receipt and receivable data,
    - Cost management data,
    - Procurement data and vendor information, and
    - General Ledger data.

Section 2.0 – The Uses of the Information.

We collect the information so we can provide services for RRB program beneficiaries with outstanding accounts receivable and to reimburse our employees for their travel and related expenses.

Our authority to collect and use this information for each of these programs comes from United States Code, Executive Orders, and our agency regulations:

United States Code:

- 5 U.S.C., Government Organization and Employees:
    - § 1302 - Special Authority for Office of Personnel Management to make rules, etc,
    - § 2951 - Submission of Reports to the Office of Personnel Management,
    - § 3301 - Examination, Certification and Appointment of Civil Service Members,
    - § 3372 - Assignments to and from States,
    - § 4118 – Training, and
    - § 8347 - Civil Service Retirement

- 45 U.S.C § 231f, Railroad Retirement Act, and
- 45 U.S.C. § 362 Railroad Unemployment Insurance Act

Executive Orders:
- Executive Order 13478 – Amendment to Executive Order 9397 Relating to Federal Agency Use of Social Security Numbers Persons (i.e. Social Security Numbers)

Railroad Retirement Board Regulations:
- 20 CFR, Employees' Benefits, Chapter II, Railroad Retirement Board.

Section 3.0 – Retention of Information

We base our need to retain information on what is required to provide the service for which it is collected. The National Records and Archives Administration reviews and approves our retention schedules. When the information is no longer required, we securely dispose of it.

Section 4.0 – Internal Sharing and Disclosure of Information

Sensitive information that we store and process on the Financial Management Integrated System major application is shared internally only to those authorized RRB staff members that have a valid business requirement for it. We share information on our annuitants and beneficiaries to support our debt collection actions. We share information about our employees to support payroll and travel payment claims. We have established security and privacy policies and procedures, awareness training programs and rules that our staff must follow when using our systems and accessing sensitive data. Our rules also cover what is required to disclose information and the penalties for improper disclosure.

Section 5.0 – External Sharing and Disclosure

We only share information as required to provide for debt recovery actions, employee payroll and payment of employee travel claims. Our Privacy Act Systems of Records Notices list who those parties are and under what routine uses that we may disclose that information.

Section 6.0 – Notice

We publish our Privacy Act Systems of Records Notices both in the *Federal Register* and on our web site (http://www.rrb.gov/bis/privacy_act/SORNList.asp).

These notices explain:
- What system collects and uses the information,
- What information is collected,
- Under what routine uses we may release that information,
- How we store, retrieve, retain and safeguard that information,
- What RRB official is the manager of that system, and
- The procedures to follow if you want to see or request corrections made to any information that system may have about you.

We also publish a Privacy Act Notice and a Paperwork Reduction Act Notice on any form that we use to collect personal information from you.

The Financial Management Integrated System uses information that is collected and used as outlined in

the Privacy Act System of Records Notices (SORN) listed here:

RRB-8…Railroad Retirement Tax Reconciliation System (RR Employee Representatives),
RRB-18…Miscellaneous Payments Posted to General Ledger,
RRB-19…Transit Benefit Program Records System (RRB Employees), and
RRB-42…Overpayment Accounts

Our Privacy Act Systems of Records Notices list who those parties are and under what routine uses that we may disclose that information.

We only share that information needed to provide and manage RRB annuitants and beneficiary's debt collections, or RRB employee payroll and travel payments with those RRB staff members or other organizations that we listed under our routine disclosures in our Privacy Act Systems of Records Notice on a strict need-to-know basis. We also have management, operational and technical control measures in place to mitigate risks to the information you provide us.

Section 7.0 – Individual Access and Redress

If you wish to review or request a change to the records and benefits that we maintain on you, please contact the nearest RRB field office for assistance.

You may also file a request for information regarding your records in writing, including your full name, social security number and railroad retirement claim number (if any). Before information about any records will be released, you will be required to provide proof of identity, or authorization from the individual you are requesting records for, before we release that information.

Send your request to:

- For RRB annuitants and beneficiaries:
    - Benefit overpayments: Chief Financial Officer, U.S. Railroad Retirement Board, 844 North Rush Street, Chicago, Illinois 60611-2092, and
    - Requests for information regarding an individual's or business' benefit overpayment record should be in writing addressed to the System Manager identified above, including the full name, claim number, and social security number of the individual.

- For RRB Employees:
    - Salary overpayments: Director, General Services Administration National Payroll Center, Attention: 6BCY, 1500 Bannister Road, Kansas City, Missouri 64131-3088, and
    - Requests for information regarding an RRB employee's salary overpayment record should be in writing addressed to the Director, General Services Administration National Payroll Center at the address above.

Before information about any record will be released, the System Manager may require the individual to provide proof of identity or require the requester to furnish an authorization from the individual to permit release of information.

Section 8.0 – Technical Access and Security

Our greatest privacy risk is unauthorized access or modification of records containing sensitive

information. We mitigate this risk by following Federal security and privacy guidance and directives. An independent contractor evaluated the RRB portion of the Financial Management Integrated System as part of its Certification and Accreditation process to ensure we are compliant with the appropriate security standards. We also have a contractor perform an independent security test and review of the RRB portion of the Financial Management Integrated System annually as part of our continuous monitoring program. The CGI-Federal portion of the information system is also independently reviewed as part of their FedRAMP certification and continuous monitoring program.

We provide security and privacy awareness training annually to all agency system users. Before granting access to the Financial Management Integrated System, new users receive training on proper use of the system and protecting the confidentiality of the data. Our users also are required to receive additional training from other Federal Agencies (Department of the Treasury, General Services Administration, or the Internal Revenue Service) if they are accessing information that is owned by those agencies.

Before we grant or modify access to the Financial Management Integrated System, management reviews the request and approves it if the employee or contractor requires that level of access to perform their assigned job duties. Once approved by management, they forward the request to our network access control staff, which assigns the appropriate roles and security profile for that authorized user. We use established role based access control rules and follow our internal agency operating procedures.

We have extensive auditing and technical safeguards in use with the Financial Management Integrated System. The auditing system contains a complete 'transaction history' for every input one of our staff members or contractors makes on the system. This transaction history cannot be modified and records among other things: The user who accessed the record, the date, time, the connecting computer address and what activity was performed.

We use extensive technical measures in order to provide electronic and physical defense-in-depth for your information. Some of our safeguards are:

- Internal policies and training addressing proper handling of sensitive information,
- Access is limited to those staff members who have a business requirement to that information,
- Information systems secured in accordance with Federal Law, National Institute of Standards and Technology (NIST) and other Executive Agency guidance and directives,
- Role based access controls used to control access to electronic data records and applications enforcing need to know and least privilege policies,
- Transaction histories are maintained to track any changes to individual records,
- Encryption of all data on systems that are located outside of RRB facilities,
- Complete hard drive encryption on all portable media (laptops, tablets, smart phones, backup media, etc.),
- Encryption of all data that transits to or from the RRB network,
- Secure disposal of electronic media when it is no longer required,
- Logging of local, network, mainframe and database usage,
- In-Depth electronic security monitoring and incident response technologies and dedicated security staff,
- Systematic data backups performed with the backup media securely transported to, and stored at a Federal records holding center and/or stored as electronic disk images at a Federally owned and operated data center, and
- The CGI-Federal portion of Financial Information Management System is FedRAMP certified.

Section 9.0 – Technologies Used by the FMIS System

The Financial Management Integrated System is comprised mainly of external Federal applications that

are provided for shared Federal government financial services.

The CGI Federal IaaS received and maintains FedRAMP approval to process information rated at the 'Moderate' risk level. The Authorizing Official (AO) or Designated Approving Authority (DAA) for this information system is the Federal Risk Authorization Management Program (FedRAMP), Joint Authorization Board (JAB) as comprised of member representatives from the General Services Administration (GSA), Department of Defense (DOD) and Department of Homeland Security (DHS).

The contractor connection for the travel application underwent a complete evaluation by the General Services Administration and was certified and accredited for operation by them. Additionally, we validated that our responsible sections of the Financial Management Integrated System meets all current Federal guidelines and directives through the use of an independent evaluation.

Additionally, our Privacy and Security staff review all information system proposals in accordance with the E-Government Act of 2002 (Public Law 107-347) and Office of Management and Budget directives.

Conclusion

Our Financial Management Integrated System (FMIS) includes components for budget formulation and execution, general ledger accounting, revenue accounting, procurement, accounts payable, travel, and inventory control, which is essential for the day to day financial operations of our agency.

We take our obligation seriously to protect all data that we use for our daily financial operations. We do this by complying with Federal information and privacy laws, directives and guidance, by providing technical network defenses in depth, and by having established management and operational controls in place to manage our information systems.

Certification of Responsible Officials

Preparer Signature & Title	Kristofer Garmager Financial Management and Program Analyst
System Owner Signature	Thomas M. McCarthy Chief, Treasury, Debt Recovery and Financial Systems Division
Approved Signature & Title	Charles P. Mierzwa Chief of Information Management Resources Center
PTA Control Number (if a PTA was submitted prior to PIA)	PTA-20150611-001
PIA Control Number	PIA-20151028-001