PRIVACY IMPACT ASSESSMENT

SYSTEM OR APPLICATION NAME:	Financial Management System
DATE:	June 24, 2011
SYSTEM OWNER & TITLE:	John M. Walter Chief, Accounting, Treasury and Financial Systems
CONTACT POINT	Kristofer Garmager Financial Systems Manager
ORGANIZATION:	Bureau of Fiscal Operations U.S. Railroad Retirement Board 844 North Rush Street Chicago, IL 60611-2092
REVIEWING OFFICIAL NAME & TITLE	Patricia Henaghan 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 System
DATE: JUNE 24, 2011	

Overview

The Railroad Retirement Board's (RRB) Financial Management System (FMS) includes components for budget formulation and execution, general ledger accounting, revenue accounting, procurement, accounts payable, travel, and inventory control. It also includes a Program Accounts Receivable (PAR) component which centralizes accounts receivable activities. Because the RRB has a benefit payment mission, the Financial Management System is used to post accounting information from systems authorizing (vouchering) benefit payments, recovery of benefit overpayments, and management of large trust funds, including investment of funds and inter-fund transfers.

The Federal Financial System (FFS) is a software package purchased from American Management Systems, Incorporated. The system is used throughout the agency for purchasing, inventory, and budget preparation (on-line data entry from terminals in headquarters and field offices). All batch processing is automatically initiated by mainframe computer scheduling software and subsequently reviewed by the system administrator (or his designee).

Personal computer spreadsheets and database management programs are used extensively to process and reconcile information received electronically from Treasury and downloaded from FFS. Downloads are done through EXTRA!'s personal client file transfer facility and is password protected through RACF.

In addition, personal computers are used to transmit data to the Office of Management and Budget (OMB), using OMB's Budget Preparation System and to transmit data to Treasury using Treasury's Government Online Accounting Link System (GOALS II). Both systems are accessible only by password through secure card IDs.

Access to the system is controlled by RACF, a system security software package from IBM. Additional security at the transaction and reference table levels is controlled by CORE software provided by the financial system vendor.

Financial Management System consists of the CORE Foundation Software system. CORE provides standard protocols for communicating with users. These protocols define how a user requests information from the system, how a user updates information in the system, and the basic formats of the display screens that are used to retrieve or update information. The protocols are designed for processing documents, for maintaining tables, and for accessing screens in a predetermined sequence.

CORE Security includes options that can be used to enforce site policies about the use of system functions, access to system data, and authorization of transactions. CORE security software controls system access by checking whether or not users are authorized to perform requested actions or access requested records.

FFS and PAR are applications that utilize the CORE system functionality. FFS has the following subsystems:

- **Accounts Payable:** Used to authorize and record payments for goods and services. It also supports Prompt Payment Act requirements and provides for direct or manual disbursement of funds,
- **Budget Execution:** Automates the budget execution process by recording online all financial activity associated with the execution of the agency's budget. These activities include distributing funds and monitoring the spending of funds at all budget levels,

- **General Ledger:** The functions of the General Ledger (GL) subsystem encompass all other FFS subsystems. These functions include automatically posting entries (debits and credits) for FFS transactions to the FFS GL and journals, maintaining account balances in the GL and journals, and maintaining an audit trail of FFS budget and financial transactions. FFS uses this audit trail to produce reports that are in compliance with the US Standard General Ledger. The GL subsystem is also used to record miscellaneous accounting transactions that are typically not handled by other FFS subsystems,
- **Budget Preparation:** Provides tools to assist the agency in all phases of the budget preparation process, from input of initial estimates through final approval of an operating plan. The subsystem maintains budget data through multiple phases of preparation and at different funding levels, and is designed to support three types of budget preparation: FTE budget preparation, workload budget preparation, and object of expense budget preparation. The subsystem is closely linked to the Budget Execution subsystem. The Budget Execution subsystem provides input to the Budget Preparation subsystem in the form of actual budget data from a previous year on which the new budget can be based. The Budget Preparation subsystem provides input to Budget Execution in the form of allotment data which can be transferred into the Budget Execution subsystem,
- **Purchasing:** Combined with the Accounts Payable and Automated Disbursements subsystems, Purchasing records, monitors, and controls all activities in the purchasing process. These purchasing activities include requesting goods and services, ordering goods and services, recording the receipt of goods and services and recording the receipt of vendor invoices. It also performs all financial, cost accounting, and reporting functions associated with the purchase of goods and services,
- **Automated Disbursements:** This subsystem records, monitors, and controls all activities associated with the disbursement of funds. These activities include generating GL entries, disbursing funds by printing checks or generating Treasury disbursement tapes, and reconciling all disbursements with Treasury's records, and
- **Inventory:** Combined with the Purchasing subsystem, the Inventory subsystem supports the main functions of inventory management, including requisition processing, purchasing, and physical inventory reconciliation. This is accomplished by:
    - Providing information on the availability of stocked items and the status of stocked requisitions, facilitating timely requisition process, and automatically recording and servicing back orders,
    - Minimizing inventory investments by basing purchasing decisions on actual usage history,
    - Providing automated tools to purchase and manage the inventory, and
    - Improving financial control of the inventory by charge backs to the user organizations and by periodic reconciliation of inventory balances with physical accounts.

Program Accounts Receivable (PAR) is used to perform the following functions:

- Record the collection of funds as revenue (billed or received),
- Bill customers for overpayments incurred,
- Calculate and post interest, administrative charges, and penalty charges for overdue receivables, and
- Select receivables for write-off or referral to collection agencies.

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

In general the Financial Management System does not process RRB beneficiary information since its purpose is core financial management.

We do however process Personally Identifiable Information (PII) in these two business activities:

- RRB annuitants and beneficiaries: Our Programs Account Receivable (PAR) application as needed to process billing and dunning (collection) notices, and
- RRB Employees – We collect and use RRB employee information to process monetary transactions with employees such as travel, relocation and medical reimbursements.

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

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 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 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 put management, operational and technical control measures into 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 Financial Management 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 Financial Management System annually as part of our continuous monitoring policy.

We provide security and privacy awareness training annually to all agency system users. Before granting access to the Financial Management 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 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 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 of our notebook computers,
- 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
- Financial applications owned by other Federal agencies also have their own unique management and security controls, in addition to ours.

Section 9.0 – Technologies Used by the FMS System

The Financial Management System is comprised mainly of external Federal applications that are provided for shared Federal government financial services. The one 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 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 System (FMS) 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 Systems Manager and Information Systems Security Officer
System Owner Signature	John M. Walter Chief, Accounting, Treasury and Financial Systems
Approved Signature & Title	Patricia Henaghan Chief of Information Management Resources Center
PTA Control Number (if a PTA was submitted prior to PIA)	PTA-20110503-001
PIA Control Number	PIA-20110624-001