Review of Mainframe Access Controls at the Application Level
Program Accounts Receivable System
Report No. 04-09, September 9, 2004

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) audit of the effectiveness of access controls in ensuring security over the Program Accounts Receivable (PAR) system, a component of the Railroad Retirement Board's (RRB) financial management application system.

Background

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act (RRA) and the Railroad Unemployment Insurance Act (RUIA). These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid out nearly $9 billion in benefits during fiscal year (FY) 2003.

The RRB's information system environment consists of two general support systems and seven major application systems. The two general support systems are the data processing system, which supports all mainframe computing activity, and the end-user computing system, which supports the agency's local and wide area networks. The major application systems correspond to the RRB's critical operational activities: payment of RRA and RUIA benefits, maintenance of compensation and service records, administration of Medicare entitlement, financial management, personnel/payroll, and the RRB's financial interchange with the Social Security Administration.

The agency's Chief Information Officer, who is also the director of the Bureau of Information Services, has overall responsibility for administration of both data processing and end-user computing as well as in-house systems development. Within the Bureau of Information Services, the Chief Security Officer has primary responsibility for coordinating, evaluating and reporting on information security for the agency.

The PAR system is a mainframe application that supports debt recovery management and reporting for the RRA and RUIA programs. Access to the mainframe environment is password protected. The PAR system includes an additional system of security functions that controls user accesses, document approval processing procedures and logging features.

The Bureau of Fiscal Operations is the owner-of-record for the PAR system and has responsibility for system administration. The system administrator maintains the security settings within the PAR system, including the access privileges of new and existing users. The PAR system is also used extensively by Office of Programs' personnel which has responsibility for debt recognition and coordination of debt

recovery and benefit payments. The RRB recognized approximately $90 million in new program debt during FY 2003.

Information security is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability. Access controls limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Previous OIG security evaluations cited the agency with material weaknesses due to significant deficiencies in access controls in both the mainframe and end-user computing environments and in the training provided to staff with significant security responsibilities.

The Office of Management and Budget (OMB) has published guidance to assist Federal managers in meeting the management control and computer security requirements of the Computer Security Act of 1987, the Chief Financial Officers Act of 1990, and the Clinger-Cohen Act of 1996. OMB Circular A-130, "Management of Federal Information Resources," Appendix III, dated November 30, 2000, establishes policy for the management of Federal information resources and establishes a minimum set of controls to be included in Federal automated information security programs.

This evaluation was conducted pursuant to the E-Government Act of 2002 (P.L. 107-347), Title III, the Federal Information Security Management Act of 2002 (FISMA), which requires annual Inspector General security evaluations.

Objective, Scope and Methodology

The objective of this evaluation was to assess the effectiveness of access controls in limiting and detecting access to the PAR system. In order to accomplish our objective, we

- identified users of the PAR system as of December 2003 and documented their system privileges;
- obtained an understanding of the security configuration of the PAR system;
- obtained an understanding of the policies and procedures through which system access is requested, authorized, granted and maintained;
- obtained an understanding of the access re-authorization process through discussions with responsible management and staff, and reviews of supporting documentation as available; and
- used statistical and non-statistical sampling to assess the effectiveness of controls in limiting access to the PAR system.

The details of the sampling methodology and results are presented in Appendix I to this report.

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 December 2003 through May 2004.

RESULTS OF REVIEW

Our audit tests disclosed that access controls are not adequate to ensure that PAR system users are limited to the system privileges required for the performance of their current job. In addition, we observed that PAR system features designed to ensure accountability for changes to certain security settings have not been implemented, and that the approval settings that control transaction processing and data entry are not consistent across programs.

The details of our findings and recommendations follow. Management has agreed to take the recommended corrective action. The full text of the responses of the Bureaus of Information Services and Fiscal Operations are included in this report as appendices II and III respectively.

Controls Are Not Effective in Limiting Access to Requirements of Position

The RRB's existing control framework is not adequate to ensure that the access privileges granted to users of the PAR system are limited to those required for performance of their current job. Our conclusion is based on our evaluation of the system privileges of 115 system users who can process transactions and/or data which identified 28 users (24%) whose privileges exceeded the requirements of their current position.

OMB Circular A-130 requires Federal agencies to limit a user's access (to data files, processing capability, or peripherals) or type of access (read, execute, delete) to the minimum necessary to perform his or her job. Current RRB policy calls for periodic system re-authorization reviews, an internal control process designed to identify changes in user needs. During the re-authorization, supervisors have the opportunity to review the current access privileges of their staff and identify any needed changes or corrections.

The Bureau of Fiscal Operations, the system owner, is responsible for ensuring that re-authorization reviews are scheduled and completed. The Bureau of Fiscal Operations had not performed a re-authorization review for the PAR system since FY 1998; the review scheduled for FY 2003 was not performed.

Although a re-authorization review was performed during FY 2004, the information provided to supervisors did not include sufficient detail about the specific privileges granted to individual employees to provide a basis for re-authorization. In most cases, the information about staff privileges included only the name of a pre-defined security

profile, but not the privileges associated with that profile. In some cases, the pre-defined security profile had not been updated to modify user privileges when the responsibilities of a job were changed.

During the period of our review, the agency's Chief Security Officer, organizationally within the Bureau of Information Services' Risk Management Group, had not assumed any direct oversight responsibility for this process. The lack of effective procedures and controls to ensure that PAR system user accesses are limited to the requirements of their current job weakens the overall structure of information security.

Recommendations

We recommend that:

1. The Bureau of Information Services implement a quality assurance program to ensure the timeliness and effectiveness of the re-authorization process for the PAR system. Such a process should include:

    - a review for completeness of documentation;
    - periodic testing to verify the effectiveness of the process;
    - issuance of an annual report communicating to the Chief Information Officer the results of the annual re-authorization process including an objective assessment of its overall effectiveness.

2. The Bureau of Fiscal Operations, as the system owner, coordinate a review of pre-defined security profiles to ensure that they properly reflect current job requirements.

Management's Response

The Bureau of Information Services concurs with the recommendation for implementation of a quality assurance program and state that they have already submitted a personnel request to assign staff; however, due to limited resources, the implementation of the program will be a multi-phased approach.

The Bureau of Fiscal Operations agrees that predefined security profiles for PAR system users should reflect their current job requirements and will conduct a review of PAR system security profiles.

Accountability for Changes to Core Security Not Ensured

Existing controls do not provide adequate accountability for changes to the PAR systems' core security tables. As a result, the system audit trail is not adequate to identify individuals who initiated changes to security settings.

OMB Circular A-130 requires Federal information systems provide accountability. Accountability is defined as the existence of a record that permits the identification of an individual who performed some specific activity so that responsibility for that activity can be established. We would have expected to see an audit trail, in the form of transaction logs, for changes to all core security tables to ensure accountability as well as separation of duties between those system users who initiate/approve changes to the logs and agency personnel who review them.

The PAR system has the capability to provide accountability through the creation of logs that capture date, time and initiator of changes to security tables. However, this feature has not been implemented for the tables that control security within the PAR system.

Only PAR system administrators can initiate changes to system security settings. The system administrators also determine which changes will be logged. The need for logging changes to core security tables was overlooked because of the small number of individuals within the agency who can make such changes and the strong trust relationship among them.

Recommendation

We recommend that:

3. the Chief Security Officer work with the system administrator to determine which security-related transactions should be logged, and identify the appropriate level of management to receive and review the logs.

Management's Response

The Bureau of Information Services concurs with the recommendation and has agreed that the Chief Security Officer will work with the PAR system administrator to determine which security-related transactions should be logged and the appropriate level of management to receive and review them.

Approvals Settings Are Inconsistent and May Be Ineffective

Document approval requirements have not been established consistently among like transactions. It is not clear whether the approval privileges, as granted to system users, are effective in achieving management's internal control objectives.

Transactions, such as document approvals, should be executed in accordance with management's directives.[1] However, we observed that like transactions do not always require like approvals. For example, an RUIA debt can be established by any individual authorized to enter billing documents, but an RRA billing document cannot be

[1] "Standards for Internal Control in the Federal Government," General Accounting Office, November 1999, GAO/AIMD-00-21.3.1

processed without an additional level of approval. In addition, approval privileges have been granted to many users so that most individuals who can enter an RRA billing document can also add the required additional approval.

As a result, the security settings for individual transactions within the PAR system imply a level of control which, in reality, has not been achieved.

Recommendation

We recommend that:

4. the Bureau of Fiscal Operations coordinate a review of the core security settings to ensure that the configuration of document approvals and award of approval privileges has properly implemented management's intentions with respect to transaction processing.

Management's Response

The Bureau of Fiscal Operations agrees with the recommendation and will conduct a review of the core security settings.

Sampling Methodology and Results

We used statistical sampling to assess the effectiveness of controls designed to limit PAR system user access to those privileges required in performance of their assigned duties. Because more than 80% of PAR system users have been limited to "View Only" access, we supplemented our sampling test with reviews of selected user groups who are able to process transactions or enter data.

Audit Objective

The objective of our tests was to determine whether the agency has been effective in restricting the privileges of users of the PAR system to only those required for their current job.

Scope

We selected the sample from the population of 669 PAR System users as of December 2003.

Review Methodology

Acceptance Sample

We used statistical acceptance sampling using a 95% confidence and 5% tolerable error which directed a sample size of 145. The threshold for acceptance was three errors. Three exceptions would permit the auditors to infer, with 95% confidence, that controls were adequate to ensure that no fewer than 95% of PAR system users had only the access privileges required for performance of their current job.

Any user who had privileges that exceeded the requirements of their current position was counted as an exception.

Non-Sampling Test

We reviewed the security profiles that granted privileges to the 115 system users who can process transactions and/or input data. Based on an initial inspection of their privileges and the auditor's knowledge of agency operations, we identified selected users whose privileges appeared to be at highest risk of exceeding the needs of their current job. We asked the system users and/or their supervisors to determine whether the privileges granted were required by the responsibilities of their current position.

Sampling Methodology and Results

Results of Review

Random Sample

Our evaluation of 145 randomly selected PAR user access profiles identified three users whose access profile included privileges that were not required to perform current job responsibilities.

Non-Sampling Test

Among the 115 individuals who had been granted privileges other than "View Only," we identified 28 (24%) who had system privileges that were not required by their current position.

Audit Conclusion

Based on our evaluation, the RRB has not achieved an adequate level of compliance with least privilege principles. Our tests disclosed a high percentage of users who have the ability to enter and/or modify system data but who do not need that access.

FORM G-115i (1-92)

UNITED STATES GOVERNMENT

MEMORANDUM

RAILROAD RETIREMENT BOARD

SEP 0 2 2004

TO : Henrietta Shaw
Assistant Inspector General, Audit

FROM : Terri Morgan
Acting, Chief Information Officer

SUBJECT: Draft Report - Review of Mainframe Access Controls at the Application Level Federal Financial System and Program Accounts Receivable System

We have completed our review of the subject reports dated August 20, 2004 and August 23, 2004 respectively, and submit to you our response to the recommendations for these systems.

Recommendation 1

We recommend that the Bureau of Information Services implement a quality assurance program to ensure the timeliness and effectiveness of the re-authorization process for Program Accounts Receivable and Federal Financial Systems. Such a process should include:

- A review for completeness of documentation;
- Periodic testing to verify the effectiveness of the process; and
- Issuance of an annual report communicating to the Chief Information Officer the results of the annual re-authorization process including an objective assessment of its overall effectiveness.

BIS Response – We concur with the recommendation for implementation of a quality assurance program for the reauthorization process. We have already submitted a request to the Bureau of Human Resources to create a temporary "Statement of Duties" position within the Architecture and Planning Group. The person selected will be responsible for the development, and preparation for the implementation, of the quality assurance program. Due to the limited number of resources that can be committed to the project, implementation of the program will be a multi-phased approach. The processes identified in the recommendation will be incorporated into the program. The tentative target date for completing the initial report of the results of the annual re-authorization process is six months from when the position is filled.

Recommendation 3

We recommend that the Chief Security Officer work with the system administrator to determine which security-related transactions should be logged, and identify the appropriate level of management to receive and review the logs.

BIS Response

We concur with the recommendation. The Chief Security Office will work with the system administrators of the Federal Financial and Program Accounts Receivable Systems, as well as business managers, to determine which security-related transactions should be logged, and will identify the appropriate level of management to receive and review the logs. These activities will be conducted, we will document which transactions are logged and identify the managers who will received and review the logs by December 31, 2004.

cc : Chief Financial Officer
Chief, Accounting, Treasury, Financial Systems and Financial Management

UNITED STATES GOVERNMENT
MEMORANDUM

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

AUG 25 2004

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Kenneth P. Boehne
Chief Financial Officer

SUBJECT: Draft Report –
Review of Mainframe Access Controls at the Application Level
Program Accounts Receivable System

Thank you for the opportunity to review and comment on the above draft report dated August 20, 2004. Our comments on the recommendations are as follows:

Recommendation 2: We agree that the pre-defined security profiles for users of the Program Accounts Receivable System should reflect their current job requirements. We will conduct a review of these profiles and implement any needed changes by December 31, 2004.

Recommendation 4: We agree that the configuration of document approvals and the delegation of approval privileges should properly reflect management's intentions with respect to transaction processing. We will conduct a review of the core security settings and implement any needed changes by December 31, 2004.

We have no comments on the other recommendations in this draft report. If you have any questions concerning our comments, please advise.