Review of Mainframe Access Controls at the Application Level
RRB-Developed Applications Controlled by ACF2 and IDMS
Report No. 04-08, September 7, 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 mainframe applications developed by programmers at the Railroad Retirement Board (RRB).

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 RRB has set forth agency-specific information security requirements in its administrative circulars. The agency's Chief Information Officer, also the director of the RRB's 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 within the agency.

The RRB maintains a staff of software programmers and system analysts to develop applications that support the agency's various program operations. Access to in-house developed applications is controlled by commercial access control software products marketed by Computer Associates International, Inc: CA-ACF2, an access control software package, or IDMS a database management system. The Bureau of Information Services has responsibility for security administration for in-house developed systems controlled by CA-ACF2 and IDMS.

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 for material weaknesses due to significant deficiencies in access controls in the mainframe and end-user computing environments and in the training provided to staff who have 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 appropriately limiting access to systems for which security is controlled by CA-ACF2 or IDMS. In order to accomplish our objective, we:

- identified users of RRB-developed applications as of November 2003 and documented their system privileges.
- obtained an understanding of the security configurations established by CA-ACF2 or IDMS;
- obtained an understanding of the policies and procedure 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 RRB-developed applications.

We limited our testing to the approximately 45 systems that support the RRB's program operations. Our 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 during December 2003 through May 2004.

RESULTS OF REVIEW

Existing controls are not effective in appropriately limiting access to RRB-developed mainframe systems. Our testing disclosed that existing controls are not effective in ensuring that system users are limited to only those privileges required for the performance of their current job. We also identified weaknesses in the implementation of segregation of duties that permit some users to perform too many key activities.

The details of our findings and recommendations follow. Although management generally agreed with our findings and agreed to take corrective action, some changes may be delayed pending availability of resources or implementation of changes to the data processing environment. The full text of the responses of the Bureau of Information Services and the Office of Programs are included in this report as appendices II and III respectively.

Access Not Limited to the Needs of Current Position

The RRB's existing control framework is not adequate to ensure that the access privileges granted to users of RRB-developed applications are limited to only those required by their current employment. Our conclusion is based on the results of a statistical sample that indicates the agency has not ensured that, at minimum, the access privileges of 95% of users have been appropriately restricted.

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. A re-authorization review is 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.

Based on our evaluation, the RRB has not adequately restricted user privileges to only those required by their current position. The results of the sample evaluation indicate that the number of users whose privileges exceed the requirements of their current job exceed 5%. We reviewed the access profiles of 186 randomly selected system users and found that 66 users (35%) had at least one privilege not required for the performance of their job.

The existing review and re-authorization process is not adequate to ensure that system users retain only those privileges required for their current employment. The current process is not effective because:

- all re-authorization reviews are not performed;
- re-authorization reviews do not include non-RRB employees;

- all changes requested during re-authorization reviews are not made;
- the process does not include all levels of access for systems with security features controlled by a separate security system in addition to IDMS or ACF2; and
- the process is not well documented with respect to timeliness and accountability for actions taken by system owners and administrators.

In addition, some systems were initially developed without a "Read-Only" access option for those who do not require higher-level privileges. In these cases, access cannot be appropriately restricted.

The lack of effective procedures and controls to ensure that system access is limited to the requirements of each user's 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 all agency-developed applications. 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.

2. The Office of Programs consider modifications to provide "Read-Only" access to those systems for which such access is not currently available.

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 Office of Programs concurs with the recommendation and has advised us they have reviewed list of their systems and requested modification of the only system that should, but does not, offer "Read-Only" access.

Inadequate Segregation of Duties Among User and Programmer Analysts

The RRB has not ensured adequate segregation of duties among users of RRB-developed applications because a large number of system analysts have been granted access to all three systems environments: development, test, and production to facilitate performance of their jobs.[1]

Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud. No one individual should control all key aspects of a transaction or event.[2]

Our review of the access profiles of 186 randomly selected system users disclosed seven users who have access to all three systems environments. The sample results indicated that the number of users who have privileges giving them access to all three systems development environments exceeds 5% of the total.

We performed additional non-sampling tests that disclosed that:

- 40 of the 173 employees (23%) in the Bureau of Information Services have access privileges that permit them to process transactions within the production environment; and
- 68 of the 85 user analysts (80%) in the Bureau of Information Services and the Office of Programs have access to the development environment and regularly perform system testing in this environment.

Data processing personnel who build and modify systems should not be able to enter or process transactions in the production environment. System users should not be able to access systems being developed or modified in the development environment. Such accesses are incompatible because they permit individuals to control all aspects of transaction processing, increasing the agency's risk that errors or wrongful acts could go undetected.

Recommendation

We recommend that the Bureau of Information Services:

3. review the responsibilities and related system accesses of individuals who have been granted access to all three systems development environments, and take action to appropriately restrict system privileges.

[1] The "development environment" is used by programmers to build or modify applications. The "test environment" is used by programmers and user analysts to test the operational capability of new applications and modifications before making them available to all users in the production environment. The "production environment" is the system as accessed by general users to view, enter and process transactions.

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

Management's Response

The Bureau of Information Services generally concurs with the finding; however, they are not currently prepared to fully implement the recommendation.

At the present time, the Bureau of Information Services does not plan to modify the accesses of user analysts to support segregation of duties because to do so would disrupt procedures and practices that have been followed for a number of years and would cause delays in testing and implementation. They believe that other controls effectively mitigate the agency's risk. Future conversion of IDMS databases to a DB2 environment will require revision of the existing test environment and they plan to address segregation of duties at that time.

With respect to programmer analysts, the Bureau of Information Services responded that they have reviewed their access privileges to production applications and made changes to individual's access based on application use and job responsibilities.

Former RUCS and FAST System Administrators Retain Privileges

Users of the RUCS and FAST systems, who are required to enter transactions for processing as part of their regular duties, are also able to administer the systems' security features. The RUCS and FAST systems support critical activities within the agency's benefit payment operations.

As discussed earlier in this report, a system user's access should be restricted to the minimum necessary to perform his or her job and key duties and responsibilities need to be divided among different people.

In February 2002, the OIG recommended that the Bureau of Information Services implement independent reviews of system administrator functions throughout the agency.[3] That recommendation was intended to address the internal control weakness created by RUCS and FAST system administrators in the Office of Programs who were also required, as part of their duties, to enter transactions for processing.

As a result of the OIG's recommendation, responsibility for RUCS and FAST system administration was re-assigned from the Office of Programs to the Bureau of Information Services. However, the high-level privileges of the former RUCS and FAST system administrators in the Office of Programs were not revoked. The corrective action taken by management replaced one control weakness with another by permitting the former systems administrators to retain privileges that they no longer required.

[3] "Review of Information Security at the Railroad Retirement Board," OIG Audit Report # 02-04, February 5, 2002.

Recommendation

We recommend that the Bureau of Information Services:

4. revoke the administrator-level privileges held by Office of Programs personnel who enter transactions in the RUCS and FAST systems.

Management's Response

The Bureau of Information Services concurs and has reported revoking the questioned privileges.

Sampling Methodology and Results

We used statistical sampling to assess the effectiveness of controls designed to limit the access privileges of users of RRB-developed mainframe applications.

Audit Objective

The objective of the sample review was to assess the adequacy of internal control over the access privileges granted to users of RRB-developed systems.

Scope

We selected the sample from the population of 1,104 users of RRB-developed applications as of November 2003.

Review Methodology

We used statistical acceptance sampling using a 95% confidence and 5% tolerable error which directed a 186 case sample. The threshold for acceptance was four exceptions. Four exceptions would permit the auditors to infer, with 95% confidence, that controls were adequate to ensure that no fewer than 95% of 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. Similarly, we considered whether the privileges held by system users indicated an inadequate segregation of duties that would increase the risk of errors or fraud by permitting some users to control too many key activities.

We also performed non-sampling tests of selected user groups to supplement the sampling tests of controls.

Results of Review

Our evaluation of the system privileges of 186 randomly selected users identified 66 users whose access profile included privileges that were not required to perform current responsibilities.[4] We identified:

- 51 individuals retained authorization privileges that had been made obsolete by the implementation of modifications/enhancements that transferred some functions to another system;
- 13 individuals required "Read-Only" access, but had been granted data/transaction entry privileges because the systems did not support "Read-Only" access. In 12 of the 13 cases, the questioned privileges were in the same system.

[4]We ended the sample evaluation of system accesses with respect to job responsibilities after 66 exceptions were identified. Accordingly, our review may not have disclosed all of the possible exceptions among system users in the audit sample.

- 2 users retained privileges that had been made unnecessary by changes in position or the end of a temporary duty assignment.

We also questioned the adequacy of the segregation of duties in the access privileges of 108 programmer and user analysts who had been granted access, other than "Read Only," to all three systems environments: development, test, and production.

Audit Conclusion

The number of exceptions identified exceeds the sample acceptance threshold. As a result, we cannot conclude that controls are adequate to ensure that at least 95% of users whose access privileges are controlled through CA-ACF2 or IDMS hold only the access privileges required for performance of their current job or that adequate segregation of duties is being maintained.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115i (1-92)

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 RRB-Developed Applications Controlled by ACF2 and IDMS

We have completed our review of the subject report dated August 17, 2004, and submit to you our responses to the recommendations.

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 all agency-developed 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 2

We recommend that the Bureau of Information Services review the responsibilities and related system accesses of individuals who have been granted access to all three systems development environments, and take action to appropriately restrict system privileges.

BIS Response – We concur with the recommendation as it pertains to established government standards and generally accepted best practices for systems development. Resolutions for the recommendation have been provided for each of the two categories of employees reviewed.

User Analysts - We are not currently prepared to modify their access to the development environment to support segregation of duties. To do so would disrupt procedures and practices that have been followed for a number of years and would cause delays in testing and implementation. Other system controls and life cycle procedures effectively mitigate any risk to data integrity, errors or undetected wrongful acts. The preferred practice of developing and/or modifying an application and conducting initial integration tests within the work environment has provided the most effective and productive means of assuring that IDMS applications function as expected and are validated by system owners.

The established "work environment" was developed to facilitate testing a system that requires additional data records from other IDMS based systems to complete and/or validate processing. This supported the concept of the "integrated" database. Initial testing is conducted using test beds established in the work area. Multiple test beds were established to enable simultaneous development/testing of the many new and existing mainframe on-line systems. After this testing is performed subsequent testing is conducted after promoting the application system to the "test environment". The additional integrated testing is coordinated and conducted with all user analysts of those systems that will interface during the process. If the results of that test are not satisfactory to all user analysts involved, the system is demoted to the "work environment" for additional modifications and the process is repeated until all users accept the results. At that time the system(s) is readied for promotion to the "production environment".

The required resources needed to replicate the functionality of the work environment would not be a cost effective solution based on risks. The procedures and practices that have been developed have adequately mitigated those risks. User analysts do not have access to modify code. They can only create and modify test data. Conversion of the IDMS databases to a DB2 environment will require revision of the existing test environment. At that time, we will work with system owners to include in the development of environments that will ensure segregation of duties, thus adhering to both acceptable security practices and government standards.

We have reviewed the type of access provided to user analysts and have validated the need for access to the work environment based on current job functions. Those who use the "work environment" for system testing are granted this access based on that need. This review was completed August 31, 2004.

Programmer Analysts - We have reviewed the type of access the programmer analysts have to production applications. Appropriate changes have been made to an individual's access based on application use and job responsibilities. Only 12 of the original 40 programmer analysts have access to the production environment. The function for rate history is solely for the purpose of printing database records and/or obtaining counts of the total of rate history records on file, these functions therefore are not associated with transactional processes. The access provided to programmer analysts for the RUIA database (RUCS) does not have a browse only feature and is used to facilitate identification and resolution of production problems. The review and all changes were completed August 30, 2004.

Based upon our reviews and action taken, as well as the justification provided we request that this recommendation be closed.

Recommendation 3

We recommend that the Bureau of Information Services revoke the administrator-level privileges held by Office of Programs personnel who enter transactions in the RUCS and FAST systems.

BIS response – We concur with the recommendation. Action has already been taken to revoke administrator-level privileges of personnel from Office of Programs who previously had been granted this access to RUCS (BASS) and FAST (SECUTAB).

cc: Robert LaBerry, Chief Enterprise Architect
Ron Russo, Chief of Policy and Systems
Catherine Leyser, Chief of Assessment and Training
Pat Henaghan, Supervisory Data Manager

UNITED STATES GOVERNMENT

MEMORANDUM

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

AUG 3 1 2004

TO: Henrietta Shaw
Assistant Inspector General, Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

THROUGH: Dorothy Isherwood
Director of Programs

SUBJECT: Draft Report – Review of Mainframe Access Controls at the Application Level – RRB-Developed Applications Controlled by ACF2 and IDMS
Your memo of August 17, 2004

Recommendation 2 We recommend that:
The Office of Programs consider modifications to provide a "Read-Only" access to those systems for which such access is not currently available.

OP Response We concur. The Office of Programs reviewed a list of the available access levels for all of its systems and determined that OLDDS was the only system without an Inquiry level that would require one. Two of the other three systems cited in the audit (SCAMP and SPOC) provide real-time calculation capabilities; the results of which are not retained for viewing. The other system (RUIACALC) is used to update and maintain user tables that are referenced by automated systems in daily RUIA processing; the system is not used for inquiry purposes. OLDDS modifications are in progress and are expected to be completed by December 31, 2004.

---

cc: Acting Chief Information Officer
Chief Security Officer
Director of Policy and Systems
Chief of Systems Technology and Development
Chief of Program Evaluation (Ret/Surv/Medicare/Tax)