OFFICE OF INSPECTOR GENERAL

Audit Report

Audit of the General and Application Controls in the Financial Management Major Application System

Report No. 09-05
September 30, 2009

RAILROAD RETIREMENT BOARD

TABLE OF CONTENTS

Introduction

Results of Evaluation

Appendices

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) audit of general and application controls over the financial management major application system using the methodology contained in the Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM).[1]

Background

The Railroad Retirement Board (RRB) administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and the Railroad Unemployment Insurance Act. These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid over $10.1 billion in benefits during fiscal year (FY) 2008.

The RRB's financial management major application includes two mainframe components, the Federal Financial System (FFS) and the Program Accounts Receivable (PAR) system, which support budget formulation and execution, general ledger accounting, accounts payable, cost accounting, payroll, and accounts receivable activities. Access to the financial management major application is controlled by ACF2, a commercial access control software product, with additional security at the transaction level provided by core security within FFS or PAR. The core security controls user activities such as document preparation and table entries, and their associated approvals. On-line data entry from personal computers in headquarters and field offices allows for updates to FFS and PAR, with overnight batch update processing and reporting.

The Bureau of Fiscal Operations (BFO) is the owner-of-record for FFS, PAR and the Automated System to Recover Overpayments (ASTRO), and has responsibility for system administration of FFS and PAR. The BFO system administrator maintains the security settings within FFS and PAR, including the access privileges for new and existing users.

The Office of Programs is the owner-of-record for the RRB's benefit payment systems, including the Railroad Unemployment Claims System (RUCS) and the Field Address Suspension Termination System (FAST). The Office of Programs includes the RRB's Field Service Office organizational component.

The Bureau of Information Services (BIS) is the owner-of-record for the Payment, Rate and Entitlement History System (PREH) and the Employment Data Maintenance System (EDMA). Additionally, BIS has responsibility for the security administration of ACF2, which controls access to all mainframe systems and provides the initial access

[1] *Federal Information System Controls Audit Manual*, GAO/AIMD-12.19.6 (January 1999), and revision GAO-09-232G (February 2009).

gateway to FFS, PAR, RUCS, FAST, and ASTRO. BIS also maintains two separate security systems that provide for the transaction level activities within RUCS and FAST.

The FISCAM provides a methodology for evaluating internal controls over the confidentiality, integrity, and availability of data maintained in financial information systems that support agency business operations. The FISCAM methodology aligns with the internal control standards promulgated by the National Institute of Standards and Technology (NIST) in Special Publication (SP) 800-53, which makes it an ideal tool for assessing agency progress in meeting requirements established by the Federal Information Security Management Act of 2002 (FISMA).[2]

FISMA requires agencies to develop, document, and implement an agency-wide information security program. The OIG has the responsibility of evaluating the information security at the RRB. Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity 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.

This audit was conducted pursuant to FISMA, which requires annual OIG security evaluations. This audit also supports the RRB's strategic goal of serving as responsible stewards of the agency's trust funds and financial resources, and its objective to ensure the effectiveness, efficiency, and security of operations.

Objective

The objective of this review was to determine the adequacy of the general and application controls over the financial management major application system.

Scope

The scope of this evaluation was FY 2008 and included the financial management major application and the general support system environment in which it operates. Due to the impact of the benefit payment systems upon the financial management major application, the access control and emergency program change portions of our general support system review included all component applications regardless of whether or not they were specific components of the financial management major application.

Our scope for the evaluation of software development was expanded to include projects as far back as FY 2005, the date when the last major modification of the financial management major application took place. The scope for our evaluation of personnel security included individuals hired by the RRB during calendar year 2007 in order to

[2] *Recommended Security Controls for Federal Information Systems*, NIST SP-800-53 (December 2007); *Federal Information Security Management Act of 2002*, Title III of the E-Government Act of 2002, P.L. 107-347 (December 2002).

allow for the completion of the Office of Personnel Management background checks and references that were performed into FY 2008, following employment.

Methodology

To accomplish our objective, we:

- reviewed pertinent laws and guidance;
- obtained and reviewed documentation to support software development projects from FY 2005 through FY 2007 that impacted the financial management major application;
- obtained and reviewed documentation to support all emergency program changes that occurred in FY 2008;
- compared the RRB's password policy with the settings within the mainframe and LAN general support systems and Federal Desktop Core Configuration, and performed validation testing of major password rules;
- obtained and reviewed documentation to support background investigation and reference checks for employees hired during calendar year 2007;
- obtained job descriptions for several employees with access to sensitive areas or the financial management application, and determined through interview whether those job descriptions were reasonably accurate and current;
- obtained and reviewed documentation to support authorized key-card access as of November 15, 2007, to sensitive areas including the data center, and determined whether the access was appropriate to job function;
- obtained and reviewed procedures for the removal and return of electronic media, and conducted independent tests to verify backup tape delivery to, and receipt from, the Federal Records Center;
- obtained and reviewed documentation to support disaster recovery testing of the financial management major application performed at the RRB's offsite test facility during FY 2008;
- obtained and reviewed listings of all mainframe and LAN user account identifications (IDs) as of January 30, 2008 and February 15, 2008, and verified that each user was a current RRB employee or an authorized non-RRB user;
- selected a statistical random sample of PAR application users with access greater than read-only as of December 10, 2008, and obtained and reviewed their individual access profiles to determine if their access was appropriate to job function;
- obtained and reviewed documentation to support access to FFS and PAR dataset files as of February 8, 2008 (and February 13, 2008, to determine

- selected a statistical random sample of mainframe application users as of January 30, 2008, and obtained and reviewed their individual access profiles to determine if their access was appropriate to job function;
- obtained and reviewed documentation to support the periodic reauthorization of mainframe application users performed in FY 2008, to confirm that all applications had been considered, and to evaluate the effectiveness of the reauthorization process;
- obtained and reviewed the access profiles as of February 12, 2009 and job descriptions for field service employees to determine if their access was appropriate to job function;
- obtained and reviewed documentation to support special privilege access provided through ACF2 as of January 30, 2008, to determine whether the access granted was appropriate to job function and periodically reauthorized; and
- interviewed responsible agency management and staff.

The primary criteria for this evaluation included:

- GAO's FISCAM;
- FISMA;
- NIST SP 800-53;
- GAO *Standards for Internal Control in the Federal Government*;[3]
- Office of Management and Budget (OMB) Circular A-130;[4] and
- RRB policies and procedures.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Fieldwork was conducted at RRB headquarters in Chicago, Illinois from December 2007 through May 2008, and October 2008 through June 2009.

[3] *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (November 1999).
[4] *Management of Federal Information Resources*, OMB Circular A-130 (November 2000).

RESULTS OF EVALUATION

Our review of the financial management major application determined that the general and application controls over entity-wide security program planning and management, data center access, non-emergency systems development, and service continuity/data recovery and backup procedures are adequate. However, the general and application controls are not adequate to ensure:

- proper segregation of duties,
- least privilege access control,
- contractor account management,
- authorized emergency program changes, and
- consistent password management and implementation.

The details of our findings and recommendations for corrective action follow. Agency management has agreed to take the recommended corrective actions except for recommendations five, nine, and ten. The full texts of management's responses are included in this report as Appendices III, IV, and V.

Segregation of Duties for Accounts Receivable Transactions is Not Enforced

Security settings within the PAR component application allow some employees the ability to both enter and approve their own accounts receivable documents or table entries, and therefore, do not support proper segregation of duties.

GAO *Standards for Internal Control in the Federal Government* requires key duties and responsibilities to be divided or segregated among different people, including the responsibilities for processing, recording, and authorizing transactions. It states, “[n]o one individual should control all key aspects of a transaction or event.”

Our review of security profiles for a statistical random sample of 49 individuals with PAR access greater than read only, disclosed 24 who are able to both enter and approve their own transactions.[5] We were advised by BFO management that supervisory review is performed for some PAR transactions processed in the debt recovery unit, but other transactions are processed without review. Likewise, in the Office of Programs Medicare unit, management advised that their users may or may not approve their own transactions based on the type of transaction processed. The Office of Programs has implemented other "no authorization" transactions throughout their processes and has performed validation studies to assess continued accuracy; however, no validation study has been performed for the types of Medicare transactions that are currently self-processed.

When management has implemented policy decisions that eliminate or forego certain controls without implementing a compensating control, the risk for fraud or abuse increases and management cannot ensure their control objectives will be achieved.

[5] See Appendix I for details of our testing methodology.

Recommendations

We recommend that the Bureau of Fiscal Operations:

1. implement a control to ensure supervisory review of transactions that are self-processed.

We recommend that the Office of Programs:

2. implement regular reviews of Medicare option cases for accuracy; and

3. perform a validation study to assess the accuracy of other types of Medicare self-processed transactions.

Management's Response

The Bureau of Fiscal Operations will implement a control to ensure supervisory review of transactions that are self-processed.

The Office of Programs has agreed to initiate quarterly reviews of Medicare option cases in FY 2010, and will complete a validation study and issue a report that will determine the need for any additional studies.

Access Control over Dataset Rules Needs to be Improved

Dataset rules governing FFS and PAR do not enforce least privilege.

OMB Circular A-130 requires agencies to incorporate controls such as least privilege into applications and application rules. Appendix III "Security of Federal Automated Information Resources" defines least privilege as "the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job."

Our review of FFS and PAR dataset access rules disclosed three individuals with access to FFS datasets and five individuals with access to PAR datasets who do not need the access for their current positions. All of the FFS users and one of the PAR users identified here have full control over the datasets (read, write, execute, and allocate), while the other four PAR users have read, write, and execute privileges. One user with full control to both FFS and PAR datasets has not required that access since at least March 2005.

We observed that BIS does not routinely request reauthorization of dataset accesses. We also found that a review of the FFS and PAR dataset privileges has not been performed since we previously identified a problem with those dataset rules in 2002.[6]

Excessive rights and privileges to data and sensitive system programs weaken the overall information security program, and prevent management from ensuring that their information systems are protected from intentional or unintentional modification.

Recommendations

We recommend that the Bureau of Fiscal Operations:

4. perform a review of FFS and PAR datasets, and initiate actions to remove the unnecessary access privileges.

We recommend that the Bureau of Information Services:

5. ensure that dataset privilege reviews are performed by system owners on an annual basis to enforce least privilege.

Management's Response

The Bureau of Fiscal Operations will perform a review of FFS and PAR datasets, and initiate actions to remove the unnecessary access privileges.

The Bureau of Information Services disagrees with recommendation five because they believe that enforcement of the security principle of least privilege with regard to data access is not a management function for BIS and that they provide dataset access based upon documented requests issued by data owners.

OIG's Comments on Management's Response

In our opinion, the RRB Security Handbook places this responsibility for enforcing least privilege with BIS security personnel because their responsibilities include:

- defining the access control strategy for RRB security management,
- modifying component users or dataset profiles to control ACF2 privileges and access to protected resources,
- assessing systems security requirements of group-level datasets,
- monitoring the component's datasets to ensure proper protection of sensitive data,
- assisting users in their assessment of user-identification-level datasets, and
- assisting users in determining proper level of protection.[7]

[6] *Review of Information Security at the Railroad Retirement Board,* OIG Report No. 02-04, February 5, 2002, Recommendation 9.
[7] *RRB Information Systems Security Policy, Standards and Guidelines Handbook (RRB Security Handbook),* Chapter 10.2.6, June 15, 2007.

Additionally, the RRB has implemented a procedure for periodic reviews to reauthorize users' access rights to component applications which are initiated by BIS security personnel, but no similar reviews exist for application datasets. This inconsistency in the RRB's access control strategy creates unnecessary vulnerability to sensitive RRB data.

Access Controls that Enforce Least Privilege Need Improvement

Mainframe access controls, including the reauthorization process, are ineffective in ensuring least privilege for all systems.

OMB Circular A-130 requires agencies to incorporate controls such as least privilege into applications. The RRB has implemented an annual reauthorization review of mainframe system accesses to enforce least privilege.

Our review of access privileges for a statistical random sample of 45 mainframe users disclosed 4 users who had inappropriate access based on his or her job function.[8] We also reviewed the reauthorization process for the mainframe systems which were identified as inappropriate for those four users. Our reviews of the reauthorization process revealed problems in the following three areas:

- Various system owners apply inconsistent methodologies in determining whether a user should retain their current access privileges.
- The reauthorization request for one system, EDMA, did not contain accurate base-line information.
- Reauthorization responses for two systems, FAST and RUCS, were not made or fully made by BIS.

Inconsistent Methodology Used

Each year BIS provides the RRB system owners with a reauthorization request to validate current access privileges, but the methodology used by those system users is not consistent. The system owner reviews the access privileges shown on the reauthorization request and instructs BIS in their reauthorization response to leave the access privilege alone, modify the access privilege to a new transaction level, or delete the access privilege. When the owner-of-record was in the Office of Programs, inquiries were routinely made of the individual user’s supervisor to determine whether the current access privileges were appropriate. However, when the owner-of-record was in BIS, such inquiries were not made and the owners attempted to determine access appropriateness themselves. Since users of RRB systems are dispersed throughout the agency, it is unrealistic to assume that a system owner can know the specific job functions of every user.

[8] See Appendix II for details of our testing methodology.

Inaccurate Base-Line Information Provided

Transaction level access provided in the EDMA system involves multiple programmed codes. Most job functions require various combinations of these programmed access codes, and each combination is translated to a generally known level of access that is easily identified by the system owner. However, the actual transaction level access of the user is the individual programmed codes and not the translated generally known level of access. When BIS prepares the reauthorization request for EDMA, the combinations of programmed codes for each user are translated to the generally known level of access. Only the generally known level of access is provided to the system owner for review. Our sample included one user for which the translation of programmed codes by BIS was not accurate, and the wrong level of access was provided to the system owner for reauthorization. We found that the individual programmed codes for this user did not equate to any generally known level of access. Instead, the individual programmed codes for this user included one additional code beyond the combination of codes required for her appropriate level of access.

Reauthorization Responses Not Implemented

Reauthorization responses requesting access modifications were not always made for two systems, FAST and RUCS. Both of these systems have transaction level access provided by separate security systems other than ACF2. In our expanded testing of the reauthorization process for the mainframe systems which were identified as inappropriate for our sample selection, one of the modification requests for FAST was not made and five users who were marked as no longer requiring RUCS access continued to be included in the separate security system that controls RUCS transaction level access.

Other Access Issues Noted for RUCS

We noted five RUCS users who had been assigned access levels that were inappropriate to their job function. These users were not identified during the reauthorization process as having inappropriate access because the system owner generally validates, through a user's supervisor, whether RUCS access is necessary and not what level of access is appropriate. As a result, all of these users were given more access than they required. We also noted four users with access specified in the separate security system, but not on the RUCS ACF2 access list. These users do not have RUCS access, but the system owner believes access is necessary for these users. Since these four users were not on the RUCS ACF2 access list, their supervisors were not asked to validate whether or not RUCS access is necessary. Access for these users is currently questionable and may include old, outdated information in the separate security system.

Ineffective reauthorization of an individual’s rights and privileges prevents management from ensuring that their information systems are protected from intentional or unintentional modification, or inappropriate viewing of privacy-related information.

Outdated security rules that clutter the security management systems weaken the overall information security structure and require additional, unnecessary, work efforts during the reauthorization process as those rules must be repeatedly identified when requests for removal are ignored.

Recommendations

We recommend that the Office of Programs:

6. review the questionable RUCS access identified in our review and ensure only appropriate access is allowed;

7. ensure the inappropriate ASTRO, FAST, and RUCS access identified by our review, and the outdated information in the separate security system that controls RUCS transaction level access, are removed; and

8. validate with a user's supervisor the RUCS transaction level access maintained in the separate security system when reauthorizations of RUCS access are performed.

We recommend that the Bureau of Information Services:

9. ensure the inappropriate PREH Correction and EDMA access identified in our review is removed;

10. develop procedures to be used by all BIS system owners in conducting system reauthorizations which includes validation of user access by the user's supervisor; and

11. provide the EDMA system owner with a reauthorization request that lists the users and their individual programmed access codes, rather than one that lists the users and their generally known translated access levels.

Management's Response

The Office of Programs agrees with the recommendations and advises that they have taken corrective action to implement recommendations six and seven. Additionally, the Office of Programs has advised that a security access audit for RUCS and BASS is planned for the first quarter of calendar year 2010, at which time recommendation eight will be addressed.

The Bureau of Information Services agrees with recommendation 11 and advises that the conversion of access control to RACF will eliminate the use of individual access codes. However, they disagree with recommendations nine and ten because the identified employees are considered to have appropriate PREH Correction and EDMA access, and because position-level roles are adequate indicators for access requirements and role-based access has been used.

OIG's Comments on Management's Response

Our finding was based on interviews with employees or their immediate supervisors to determine the appropriateness of the employee's access with relation to job function. In all cases, we were advised that the employee did not have any job functions that required the use of the application or the level of functionality they held for the application. We stand by our conclusion that the access for 4 of 45 employees, as cited in Appendix II, is inappropriate.

With respect to role-based access strategies and the principle of least privilege, it is important to address how roles change over time. We do not disagree with the use of role-based access strategies; however, supervisors need to be periodically interviewed to ascertain the continued appropriateness of the access privileges assigned each role. During our interviews, we were advised that employees in one unit no longer performed the job duties for which they held access privileges, and had not performed those job duties for several years. Without a change in the procedure used by BIS when reauthorizing access privileges, least privilege access rights will never be achieved.

Field Service Access Profile Needs Updating

The Field Service access profile has not been consistently applied in accordance with management's assertion, nor does it enforce least privilege.

OMB Circular A-130 requires agencies to incorporate controls such as least privilege into applications. The RRB designed a Field Service profile in 1992 to be used for granting application access to all Field Service employees. This profile has been modified throughout the years to allow for new systems and functions required by Field Service employees; but it has not been reviewed by RRB management to ensure its accuracy.

Our review of access privileges for a statistical random sample of 45 mainframe users disclosed 3 Field Service employees with different access privileges compared to other Field Service employees in our sample.[9, 10] This is in conflict with management's assertion (through use of an access profile) that all Field Service employees should have the same access privileges, regardless of the job position they hold.

Since we disagree with management's assertion that all Field Service positions require the same access privileges, we reviewed the job descriptions for many of the full-time Field Service staff and for the six temporary Field Service staff employed at the time of

[9] See Appendix II for details of our testing methodology.

[10] The difference in access granted to these three Field Service employees resulted in lesser privileges than the other Field Service employees in our sample. Therefore, we did not consider the differences noted as errors in our statistical sample evaluation.

our review.[11] We found that none of the six contractual agreements for temporary employment listed job duties that would require the individual to have identical access to most full-time RRB Field Service employees. We also found that one full-time Field Service position did not reflect the job duties that required the Field Service access profile.

Access profiles designed to allow the same rights and privileges to all individuals increase the risk for inappropriate disclosure of privacy-related information and prevent management from ensuring their information systems are protected from intentional or unintentional modification.

Recommendation

We recommend that the Office of Programs:

12. review the Field Service access profile and restrict its use to only those positions that require access to all system privileges contained in that profile.

Management's Response

The Office of Programs has agreed to review the access profiles for the different job types and their access levels to make sure they have appropriate read/update capabilities.

Controls over ACF2 Special Privileges Can be Improved

Internal control over ACF2 special privileges need improvement.

OMB Circular A-130 requires agencies to incorporate controls such as least privilege into applications. GAO's FISCAM guidance further states “[b]road or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or manage emergency situations. Such special privileges may be granted on a permanent or temporary basis. However, any such access should also be approved by a senior security manager, written justifications should be kept on file, and the use of highly sensitive files or access privileges should be routinely reviewed by management.” ACF2 special privileges provide the type of access described by GAO's FISCAM, above.

Our review of the ACF2 special privileges disclosed the following internal control deficiencies:

[11] The RRB Field Service employs temporary workers through separate contractual agreements with non-Federal employment agencies when workloads require additional staffing. These temporary employees generally perform clerical duties in individual Field Service offices, and are not RRB employees.

- Segregation of duties and least privilege is not enforced. We identified ten individuals, including one contractor, who have the ability to create, modify, or delete user accounts and the ability to assign access privileges to those accounts. The contractor also has the ability to read all data files, and to submit jobs for mainframe processing.

- Special privilege reviews and reauthorizations are performed by the system administrator who also enters the privilege rights, rather than a senior security manager. Such reviews have not always identified unnecessary IDs with special privileges for timely deletion. During the course of our review we requested additional information regarding one “started task” ID with a special privilege, and were informed that the ID had never been used and should be removed from the system. We noted that the ID had been active for about three years.

- Documentation to support reauthorization reviews of special privileges is not created or kept. We were advised that BIS only creates documentation for the creation, modification, or deletion of special privilege rights granted outside the reauthorization process. This procedure originated in response to problems we previously identified with documentation to support the granting of special privileges in 2002.[12]

The risk of inappropriate access to data and sensitive system programs, as well as the disruption of services is greater when high-level special privileges are not adequately controlled.

Recommendations

We recommend that the Bureau of Information Services:

13. review all assigned special privileges, including started tasks; and ensure proper segregation of duties and least privilege is maintained for all users with special privileges; and

14. implement a fully documented reauthorization review process of all special privileges by a senior security manager, at least annually. Such reviews should consider the identification and timely removal of unnecessary IDs with special privileges.

Management's Response

The Bureau of Information Services agrees with recommendations 13 and 14 and advises that the special privileges, as designed within ACF2, will be reviewed as part of the conversion to RACF and that the Chief Security Officer will implement a fully-documented annual reauthorization review process of all special privileges.

[12] *Review of Information Security at the Railroad Retirement Board,* OIG Report No. 02-04, February 5, 2002, Recommendation 9.

Contractor Account Management Can be Improved

The controls to ensure timely deletion of inactive contractor user accounts are not fully effective.

OMB Circular A-130 requires agencies to incorporate controls such as least privilege into applications. This includes the deletion of accounts that are no longer required. The RRB has implemented policies for the management of user accounts that include promptly deleting the account from the system when services are no longer provided, and identifying and reviewing accounts that have not been used in the past year.

During our review of all mainframe and LAN user accounts to verify that each user was a current employee or an authorized non-employee, we noted one user account for a contractor whose LAN account had not been used in three months.[13] We also noted that the contractor's LAN account did not allow for temporary usage because it was set to "never expire."

During interviews, BIS advised us that the contractor was no longer performing services for the RRB and that they had previously deleted the LAN account. BIS proceeded to delete the mainframe account in our presence. Two months later, however, we discovered that the LAN account was still active and brought that information to BIS' attention. BIS then deleted the LAN account. As a result, the LAN user account deletion took place nearly two months after BIS had become aware that the contractor was no longer working, and evidence suggests that the contractor may have ceased services as much as five months prior to account deletion.

When a contractor continues to have access to systems after they have ceased employment, the risk of unauthorized access is increased, which weakens the overall security program.

<u>Recommendation</u>

We recommend that the Bureau of Information Services:

15. implement a policy to provide for earlier identification and review of inactive contractor accounts by utilizing the LAN account expiration setting, and timing it to coincide with individual contract expectations.

[13] The contractor was a computer programmer hired to assist in a systems development project.

Management's Response

The Bureau of Information Services agrees with the recommendation and has advised that all contractor accounts will be established using the LAN account expiration setting, timed to coincide with individual contract expectations.

Emergency Program Change Controls Can be Improved

Controls designed to ensure that emergency program changes are made in accordance with proper supervision and authorization need improvement.

GAO *Standards for Internal Control in the Federal Government* require the proper authorization and execution of transactions and events by persons acting within the scope of their authority, as well as the segregation of those duties. GAO's FISCAM guidance further states that emergency program changes should be promptly tested and approved; and integrated into change control, retroactively, as soon as possible after the emergency change is made.

The RRB has designed a control for managing emergency changes by promptly notifying BIS management of the emergency program change, and providing for a means to document the supervisor’s subsequent authorization by deleting the source program code. This deletion automatically writes the program code to a separate file for audit purposes. There is no written procedure or formal time standard for performing this activity. We were also advised by BIS that a program developer could not delete their own program code; only a supervisor can delete the source program code.

Our review of emergency program changes showed that the timeframes for supervisory deletion of source program code varied, many of which were unduly delayed. Of 22 emergency program changes that occurred in FY 2008, 11 showed evidence of supervisory review and approval within 2 business days of the emergency change.[14] However, the program code for the other 11 was deleted between 7 and 109 days after the emergency change took place. We also noted that on one occasion, the emergency program change was made by a supervisory-level employee, and that person was able to delete his own program code.

Processing errors or unauthorized program modifications can be introduced into the information system when adequate supervision and approvals are not present or unduly delayed.

[14] Of the 22 emergency program changes, 19 were for the same system and occurred prior to May 2008.

Recommendations

We recommend that the Bureau of Information Services:

16. establish a formal, written, procedure for executing emergency program changes. The procedure should specify a formal time standard for the review and authorization of the emergency change; and

17. implement a control to prevent a single individual, including supervisory personnel, from preparing an emergency program change and subsequently deleting the program code themselves.

Management's Response

The Bureau of Information Services agrees with the recommendations and advises that they will create a formal written procedure for executing emergency program changes which specifies a formal time standard for the review and authorization of emergency changes. The procedure will also specify that the individual who prepares an emergency program change will not be permitted to delete his or her own program code.

Password Rules Are Inconsistent and Do Not Enforce Written Policy

The RRB password rule settings are not consistently applied among agency platforms and do not enforce the written policy.

NIST SP-800-53 requires agencies to manage information system authenticators. Passwords are used to identify and authenticate users. Identification distinguishes one user from all others, and provides the means by which specific access privileges are assigned and recognized by the computer. The most widely used method of authentication is with a password. As such, passwords must be controlled to reduce the risk of unauthorized user access. Password rules are the means through which passwords are controlled, and include settings that stipulate character length and use, minimum and maximum age, password reuse, and account lockout when inaccurate authentication attempts are made.

NIST has also developed the Federal Desktop Core Configuration (FDCC) security configurations which include password rule settings for workstations. OMB has directed all agencies to implement the FDCC. The RRB has also established a written password policy, and has implemented password rules using global settings in both the LAN and mainframe platforms, as well as for agency workstations.[15]

[15] The global settings have been implemented through separate Group Policy Objects for the LAN servers and the FDCC regulated workstations, as well as through ACF2 Global Systems Options for the mainframe.

We observed that the RRB's written password policy is out of date, and has not been adjusted to conform to the FDCC security configurations. Our reviews of the RRB's password settings within the mainframe and LAN general support systems, including those for agency workstations, showed that the various settings are inconsistent and do not fully enforce the NIST FDCC security configurations.[16]

Our test of the effect of these inconsistencies showed that the FDCC password settings established in the FDCC Group Policy Object are not being applied. In the RRB's LAN general support system, user authentication is a function performed at the server level and not locally on the user's workstation. Although the FDCC security configurations apply to the workstations, and not the servers, the FDCC password settings must be implemented at the server level in order for them to take effect. In addition, during our validation testing of major password rules, we observed that the RRB does not routinely apply the LAN password setting to enforce single use of a temporary password when the user is assigned a new password by the system administrators.

Weak password rules increase the risk of unauthorized access to information systems.

Recommendations

We recommend that the Bureau of Information Services:

18. update the written password policy in the Security Handbook and ensure its conformance to the FDCC security configurations;

19. apply the FDCC password settings in the LAN server Group Policy Object; and

20. instruct the system administrators to begin using the temporary LAN password setting.

Management's Response

The Bureau of Information Services agrees with the recommendations and advises that to the extent practicable, the written password policy in the RRB Security Handbook will be updated in conformance with the FDCC security configuration. They will also apply the FDCC password settings in the LAN server Group Policy Object, and will instruct Customer Support Help Desk personnel to begin using the temporary LAN password setting.

[16] The inconsistent settings are, in some instances, necessary due to software constraints. However, in other instances, the RRB has decided to deviate from the FDCC security configuration setting.

METHODOLOGY AND RESULTS
Effectiveness of Controls over Access Provided to PAR

We evaluated the access controls designed to ensure that individual user access to PAR is appropriate for their current job position.

Objective

The objective of our test was to determine whether existing controls are effective to ensure that the authorized individuals have appropriate access to the PAR system.

Scope

We selected our sample from the population of 84 PAR users with greater than read-only access as of December 10, 2008.

Review Methodology

We used statistical attribute acceptance sampling using a 90% confidence and 6% tolerable error rate which directed a sample size of 49 users. The threshold for acceptance was one. If one or fewer errors were identified, the auditors may infer with 90% confidence that control errors would not exceed 6%, and the controls were operating and effective.

We obtained and reviewed the individual access profiles for each user in our sample to determine if the accesses specified were appropriate to their job function. An error was defined as:

- A control that was not operating;
- An operating control that could not be evidenced; or
- An unacceptable outcome, such as inappropriate access, indicated that the control was not effective.

Results of Review

Our evaluation of 49 randomly selected PAR users with greater than read-only access identified 24 who are able to both enter and approve their own transactions. As a result, the access control designed to enforce segregation of duties is not operating and it does not restrict a user's actions based on their job function.

Conclusion

The 24 exceptions exceed the sample acceptance threshold. As a result, we cannot conclude that controls are effective to ensure that individual user access is appropriate and only allows access that is required for the performance of current job functions.

METHODOLOGY AND RESULTS
Effectiveness of Controls over Access Provided by ACF2

We evaluated the access controls designed to ensure that individual user access is appropriate to their current job position.

Objective

The objective of our test was to determine whether existing controls are effective in ensuring that the authorized individuals have appropriate access to RRB information systems through an ACF2 user ID.

Scope

We selected the sample from the population of 946 ACF2 mainframe users as of January 30, 2008.

Review Methodology

We used statistical attribute acceptance sampling using a 90% confidence and 5% tolerable error rate which directed a sample size of 45 users. The threshold for acceptance was zero. If no errors were identified, the auditors may infer with 90% confidence that control errors would not exceed 5%, and the controls were operating and effective.

We obtained and reviewed the individual access profiles for each user in our sample to determine if the accesses specified were appropriate to their job function. An error was defined as:

- A control that was not operating;
- An operating control that could not be evidenced; or
- An unacceptable outcome, such as inappropriate access, indicated that the control was not effective.

Results of Review

Our evaluation of 45 randomly selected mainframe users identified 4 users whose access profile included privileges that were not required to perform their current job responsibilities, as follows.

User No.	Type of Errors Identified
1	• Has access to PREH Correction without job duties dependent on that system.

User No.	Type of Errors Identified
2	• Has access to PREH Correction without job duties dependent on that system. • Reauthorization requested removal of RUCS access, but removal was only applied to the RUCS user list in ACF2 and not the RUCS user list in the separate security system.
3	• Has access to PREH Correction without job duties dependent on that system. • Has access to FAST without job duties dependent on that system.
4	• Has access to ASTRO without job duties dependent on that system. • Has excessive access to EDMA without job duties for that function. • Reauthorization request for EDMA did not include accurate base-line information.

Conclusion

The four exceptions exceed the sample acceptance threshold. As a result, we cannot conclude that controls are effective to ensure that individual user access is appropriate and only allow access that is required for the performance of current job functions.

UNITED STATES GOVERNMENT

FORM G-115f (1-92)

MEMORANDUM

RAILROAD RETIREMENT BOARD

SEP 21 2009

TO : Letty Benjamin Jay
Assistant Inspector General for Audit

FROM : Kenneth P. Boehne Kenneth P. Boehne
Chief Financial Officer

SUBJECT: Draft Report – Audit of the General and Application Controls in the Financial Management Major Application System

Thank you for the opportunity to review and comment on the above draft report dated September 11, 2009. Our comments are as follows:

We recommend that the Bureau of Fiscal Operations:

1. implement a control to ensure supervisory review of transactions that are self-processed.

We will implement a control to ensure supervisory review of transactions that are self-processed. Target date: March 31, 2010.

4. perform a review of FFS and PAR datasets, and initiate actions to remove the unnecessary access privileges.

We will perform a review of FFS and PAR datasets, and initiate actions to remove the unnecessary access privileges. Target date: February 26, 2010.

cc: John Walter, Chief of Accounting, Treasury and Financial Systems
Kristofer Garmager, Financial Systems Manager
Tom McCarthy, Debt Recovery Manager
Bill Flynn, Executive Assistant
Jill Roellig, Management Analyst

UNITED STATES GOVERNMENT

MEMORANDUM

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

SEP 23 2009

TO: Letty Benjamin Jay
Assistant Inspector General, Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

Catherine A. Leyser

THROUGH: Dorothy Isherwood
Director of Programs

D Isherwood

SUBJECT: **Draft Report – Audit of the General and Application Controls in the Financial Management Major Application System**

FINANCIAL MANAGEMENT MAJOR APPLICATION SYSTEM

Overall comments

We have reviewed the draft report and appreciate the fact that the review determined that the general and application controls over entity-wide security program planning and management, data center access, non-emergency systems development, and service continuity/data recovery and backup procedures are adequate.

We concur with the recommendations and will take action on those directed to the Office of Programs as follows.

Recommendation 2

The OIG recommends that the Office of Programs:

Implement regular reviews of Medicare option cases for accuracy.

OP Response

We agree. The Chief of Unemployment and Program Services Division will initiate quarterly reviews in FY 2010. We plan to close out this recommendation by May 31, 2010 after the second review has been completed.

Recommendation 3

The OIG recommends that the Office of Programs

Perform a validation study to assess the accuracy of other types of Medicare self-processed transactions.

OP Response

We concur. We will complete a validation study and issue a report by September 30, 2010. That report will determine the need for additional studies, if any.

Recommendation 6

The OIG recommends that the Office of Programs

Review the questionable RUCS access identified in our review and ensure only appropriate access is allowed.

OP Response

We concur. In fact, we have already taken corrective action which we documented in an email to your office on Sept. 22, 2009.

Recommendation 7

The OIG recommends that the Office of Programs

Ensure the inappropriate ASTRO, FAST, and RUCS access identified by our review, and the outdated information in the separate security system that controls RUCS transaction level access, are removed.

OP Response

We concur. In fact, we have already taken corrective action which we documented in an email to your office on Sept. 22, 2009.

Recommendation 8

The OIG recommends that the Office of Programs

Validate with a user's supervisor the RUCS transaction level access maintained in the separate security system when reauthorizations of RUCS access are performed

OP Response

We concur. The next security access audit for RUCS and BASS is planned for the first quarter of calendar year 2010. Our target date for closing out this audit recommendation is April 30, 2010.

Recommendation 12

The OIG recommends that the Office of Programs

Review the Field Service access profile and restrict its use to only those positions that require access to all system privileges contained in that profile.

OP Response We concur. Field Service and Policy and Systems will work together to review the access profiles for the different job types and their access levels to make sure they have appropriate read/update capabilities. This review will be completed by March 31, 2009.

cc: Chief Information Officer
Chief Financial Officer
Director of Policy and Systems
Director of Operations
Director of Field Service

Appendix V

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

September 28, 2009

TO : Letty B. Jay,
Assistant Inspector General for Audit

FROM : Terri S. Morgan,
Chief Information Officer

SUBJECT: Draft Report – Audit of General and Application Controls over the Financial Management Major Application System

Thank you for the opportunity to review and respond to the subject draft report. The following are the responses to the recommendations included in the report that were addressed to the Bureau of Information Services.

Recommendation #5

We recommend that the Bureau of Information Services ensure that dataset privilege reviews are performed by system owners on an annual basis to enforce least privilege.

Response

BIS disagrees with this recommendation. In general, we believe that enforcement of the security principle of least privilege with regard to data access is not a management function for BIS. BIS provides dataset access based upon documented requests issued by data owners. BIS is not responsible for determining least privilege or defining the least amount of privileges needed by users to perform their business functions. Business analysts in the owner bureaus/offices are granted the least privilege read access to datasets relevant to the work of the bureau/office. Elevated access required to write to production data files generally is not allocated to individuals. System owners can enforce least privilege by limiting dataset access privileges to the minimum number of employees needing access to data.

Recommendation #9

We recommend that the Bureau of Information Services ensure the inappropriate PREH Correction and EDMA access identified in our review is removed.

Response

BIS disagrees with this recommendation. The identified employees are considered to have appropriate PREH Correction and EDMA access. No further action is necessary.

Recommendation #10

We recommend that the Bureau of Information Services develop procedures to be used by all BIS system owners in conducting system reauthorizations which includes validation of user access by the user's supervisor.

Response

BIS disagrees with this recommendation. BIS rejects this recommendation on the basis that role based access control (RBAC) is within NIST guidelines. The RRB has chosen the position as the role for access, as this is the practical level of control for BIS' staffing. While more granular choices can be made, business and technical experts have agreed in the past that position level roles are adequate indicators of access requirements. The next scheduled reauthorization of the PREH and EDM application is scheduled to be conducted by Data Management Group in the 3rd calendar quarter of 2010.

Recommendation #11

We recommend that the Bureau of Information Services provide the EDMA system owner with a reauthorization request that lists the users and their individual programmed access codes, rather than one that lists the users and their generally known translated access levels.

Response

BIS agrees with this recommendation. As part of the conversion of access control to RACF, individual access codes are being eliminated. When conducting the reauthorization review of the EDMA system, Systems Assurance Group will provide the owner with a report of users and their access level descriptor. The next reauthorization review for the EDMA system is scheduled for the 3rd calendar quarter 2010.

Recommendation #13

We recommend that the Bureau of Information Services review all assigned special privileges, including started tasks; and ensure proper segregation of duties and least privilege is maintained for all users with special privileges.

Response

BIS agrees with this recommendation. As part of the conversion to RACF, special privileges as designed within ACF-2 are being reviewed by Infrastructure Services Center. The conversion will be completed on or before December 1, 2009.

Recommendation #14

We recommend that the Bureau of Information Services implement a fully documented reauthorization review process of all special privileges by a senior security manager, at least annually. Such reviews should consider the identification and timely removal of unnecessary IDs with special privileges.

Response
BIS agrees with this recommendation. The Chief Security Officer will implement a fully documented annual reauthorization review process of all special privileges. The first such annual review will be conducted in January 2010.

Recommendation #15
We recommend that the Bureau of Information Services implement a policy to provide for earlier identification and review of inactive contractor accounts by utilizing the LAN account expiration setting, and timing it to coincide with individual contract expectations.

Response
BIS agrees with this recommendation. Effective immediately, all contractor accounts will be established using the LAN account expiration setting, timed to coincide with individual contract expectations. Systems Assurance Group will require the form G-455, Computer Access Authorization Request, when used for temporary contractors, to be notated with the expected account expiration date.

Recommendation #16
We recommend that the Bureau of Information Services establish a formal, written, procedure for executing emergency program changes. The procedure should specify a formal time standard for the review and authorization of the emergency change.

Response
BIS agrees with this recommendation. Application Design Center will create a formal, written procedure for executing emergency program changes that specifies a formal time standard for the review and authorization of the emergency change. This procedure will be produced by April 1, 2010.

Recommendation #17
We recommend that the Bureau of Information Services implement a control to prevent a single individual, including supervisory personnel, from preparing an emergency program change and subsequently deleting the program code themselves.

Response
BIS agrees with this recommendation. Application Design Center will specify in the emergency program change process that the individual who prepares an emergency program change will not be permitted to delete their own program code. This procedure will be produced by April 1, 2010.

Recommendation #18
We recommend that the Bureau of Information Services update the written password policy in the Security Handbook and ensure its conformance to the FDCC security configurations.

Response

BIS agrees with this recommendation. To the extent that is practicable, the Risk Management Group will update the written password policy in the Security Handbook in conformance with the FDCC security configuration by January 1, 2010.

Recommendation #19

We recommend that the Bureau of Information Services apply the FDCC password settings in the LAN server Group Policy Object.

Response

BIS agrees with this recommendation. Infrastructure Services Center will take action to apply the FDCC password settings in the LAN server Group Policy Object. This will be completed by January 1, 2010.

Recommendation #20

We recommend that the Bureau of Information Services instruct the system administrators to begin using the temporary LAN password setting.

Response

BIS agrees with this recommendation. The Customer Support Help Desk personnel will be provided with instructions to begin using the temporary LAN password setting by November 1, 2009.