OFFICE OF INSPECTOR GENERAL

Audit Report

Audit of the Railroad Retirement Board's Medicare Major Application System

Report No. 09-06
September 30, 2009

RAILROAD RETIREMENT BOARD

TABLE OF CONTENTS

Introduction

Background 1

Objective 2

Scope 2

Methodology 2

Results of Review

Dataset Rules Do Not Enforce Least Privilege 4

Access Controls that Enforce Least Privilege Need Improvement 6

Accountability over ACF2 Audit Logs Needs Improvement 7

Audit Log Content Needs Expansion 9

Audit Log of Security Violations is Misleading 10

Appendices

Appendix I Bureau of Information Services Management's Response 11

Appendix II Office of Programs Management's Response 13

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) audit of the Railroad Retirement Board's (RRB) Medicare major 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 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 Medicare program is a Federal health insurance program for people age 65 or older and certain disabled people. The program is run by the Centers for Medicare and Medicaid Services and the U.S. Department of Health and Human Services. Persons covered under the Railroad Retirement system participate in Medicare on the same basis as those under the Social Security system. The RRB enrolls railroad retirement beneficiaries in the program and deducts Medicare premiums from their monthly benefit payments.

The RRB's Medicare major application system includes the Medicare Information Recorded, Transmitted, Edited and Logged (MIRTEL) system. MIRTEL is a batch file system that is run daily. It establishes and maintains records for the RRB's Medicare beneficiaries. The Medicare major application system also includes the:

- MIRTEL On-Line Inquiry (MOLI) database that allows view-only access to select data for Medicare records in MIRTEL;
- Medicare Correction (MEDCOR) database system which allows on-line data input used in updating MIRTEL;
- Medicare Referral (MEDREF) database system which allows on-line viewing of MIRTEL rejects and referrals, which can be corrected using MEDCOR; and
- Monthly Adjustment of MIRTEL Master (MAMMA) which adjusts MIRTEL for changes in the RRB's beneficiary payment master file used to produce monthly benefit checks. Like MIRTEL, MAMMA is also a batch file system.

The Office of Programs is the owner-of-record for the RRB's Medicare and benefit payment applications. They also have responsibilities for all of the RRB's Medicare activities. These activities include eligibility determinations, enrollment processing, the collection of premiums, the recovery of overpayments, and the payment of Canadian claims.

The Bureau of Information Services (BIS) has responsibility for the security of all Medicare applications and data files. BIS maintains the security for these applications and data files using ACF2, a commercial access control software product. Using ACF2, access to MEDCOR and MEDREF is provided through one or more access privileges

for the combined systems. The first level of access acts as a gateway to the two database systems and allows view-only privileges. Any additional levels of access provide transaction-level privileges such as create, update, or delete.

This audit was conducted pursuant to the Federal Information Security Management Act of 2002 (FISMA) which requires annual OIG security evaluations.[1] 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 perform a system-level assessment of the Medicare major application to determine if security controls were in place, operated as intended, and met the requirements established by FISMA. The security controls reviewed in detail include access controls, audit and accountability, identification and authentication, and system and information integrity.

Scope

The scope of this evaluation was FY 2009 and included the Medicare major application and the general support system environment in which it operates.

Methodology

To accomplish our objective, we:

- reviewed pertinent laws and guidance;
- obtained and reviewed listings of all user accounts associated with the Medicare major application as of January 14, 2009 and February 5, 2009, and verified that each user was a current employee or an authorized non-RRB employee user, and was uniquely identified;
- obtained and reviewed documentation as of February 5, 2009, to support the individual access profiles of all users that had access to the MOLI, MEDCOR, and MEDREF databases to determine if their access was appropriate to job function;
- obtained and reviewed documentation from December 2, 2008 through January 9, 2009, to support access to all Medicare major application dataset files, including those associated with database and batch processes, to determine whether the access granted was appropriate to job function;

[1] *Federal Information Security Management Act of 2002,* Title III of the E-Government Act of 2002, P.L. 107-347 (December 2002).

- obtained and reviewed documentation to support the periodic reauthorization of user access privileges to the MOLI, MEDCOR, and MEDREF databases performed in August 2008, to evaluate the effectiveness of the reauthorization process;
- verified the filing and retention of information system media, both digital and non-digital, to determine whether access was appropriately restricted;
- obtained and reviewed documentation to support the audit of, and accountability over, Medicare output/production reports, audit logs, and information system violation reports;
- obtained and reviewed documentation to support the existence and operation of system and information integrity controls which include information input restrictions; accuracy, completeness, and validity; error handling; and information output handling and retention; and
- interviewed responsible agency management and staff.

The primary criteria for this evaluation included:

- FISMA;
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53;[2]
- Government Accountability Office (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 November 2008 through July 2009.

[2] *Recommended Security Controls for Federal Information Systems,* NIST SP 800-53 (December 2007).
[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 REVIEW

Our review of the Medicare major application determined that the identification and authentication, and system and information integrity controls were in place, operated as intended, and met the requirements established by FISMA. However, we found that the security controls over access, and controls over audit and accountability, need improvement.

The details of our findings and recommendations for corrective action follow. Agency management has agreed to take the recommended corrective actions except for recommendations one and two. The full texts of management's responses are included in this report as Appendices I and II.

Dataset Rules Do Not Enforce Least Privilege

Rules that govern dataset file access 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 approximately 386 dataset rules that provide users' access to Medicare data files showed that the RRB has written many dataset rules using a "wildcard" designator recognized by ACF2. Wildcard designators allow the substitution of any character in place of the wildcard. As a result, a wildcard designator will allow a user access to <u>any</u> dataset which matches the preliminary dataset name. For example, "P.BRC.-" (where "-" is the wildcard designator) allows access to any dataset that begins with "P.BRC.". We observed that the RRB has over 10,250 datasets that begin with "P.BRC.", the majority of which are for non-Medicare applications and include personally identifiable information such as names and social security numbers.[5]

We also identified six users with excessive rights to Medicare dataset files; the access privileges provided were more than the users required for the current job function. Four of the six individuals had full access (read, write, execute, and allocate) to the dataset files involved. These datasets (not "P.BRC.") were also assigned using a wildcard designator. The other two individuals did not require any access at all, and had the ability to read and execute all "P.BRC." dataset files.

We found that the RRB has not established standards to address how wildcard designators will be used when providing dataset access. Although the use of a wildcard designator can be an efficient method of providing access as each individual dataset

[5] There are 79 users with "P.BRC.-" access, and approximately 175 Medicare dataset files that begin with "P.BRC.". Dataset files are used in both database systems and batch file systems.

does not need to be enumerated for every user, overly broad wildcard usage can allow far greater access privileges than intended.

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, or inappropriate viewing of privacy-related information.

Recommendations

We recommend that the Bureau of Information Services:

1. establish a standard for the use of wildcard designators when preparing dataset access rules; and

2. evaluate current dataset access rules and enforce the principle of least privilege by restricting overly broad wildcard access use.

Management's Response

The Bureau of Information Services disagrees with the recommendations because wildcard designators are used whenever they facilitate the administration of resources and dataset access is allocated upon request as authorized and instructed by system owners.

OIG's Comments on Management's Response

With respect to the use of wildcard designators, we acknowledge their efficiency in facilitating the administration of resources and the difficulties that would arise if their use were fully restricted. However, because large volumes of sensitive data for many beneficiaries is easily accessible via dataset accesses, we strongly believe that wildcard designators should be used judiciously and in a manner that does not unreasonably increase the RRB's risk for a breach of personally identifiable information. Therefore, we seek improvement in the RRB's access control strategy by recommending that BIS, as the experts in access control, examine ways to reduce system owner's reliance on overly broad wildcard use. This includes establishing a standard for wildcard usage, and reviewing the current accesses provided via wildcard use and enforcing the principle of least privilege by restricting overly broad wildcard access use.

Access Controls that Enforce Least Privilege Need Improvement

Mainframe access controls, including the reauthorization process, are ineffective in ensuring least privilege for Medicare 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 systems accesses to enforce least privilege.

Our review of user access privileges for Medicare database systems disclosed users who have inappropriate access based on their job functions. Additionally, our review of the reauthorization process for Medicare database systems showed that it was ineffective in removing all users with inappropriate access, identifying potentially inappropriate access, and did not include contractors with access privileges. Our reviews revealed problems in the following areas:

	Number of Users MOLI	Number of Users MEDCOR/MEDREF
Inappropriate Access Based on Job Function	1	4
Reauthorization Response Not Addressed by BIS	5	2
Reauthorization Response Partially Addressed by BIS[6]		11
Reauthorization Did Not Consider Contractor	8	3
Other Questionable Access		22

We previously reported problems with the RRB's reauthorization process and made a recommendation for BIS to implement a quality assurance program to ensure timeliness and effectiveness.[7] That recommendation is pending corrective action. We were advised by the Chief Security Officer that an attempt was made to perform a quality assurance assessment of the reauthorization process included in our review, and that he was unable to complete that assessment and attest to the user access due to documentation problems he encountered during his review. He also advised that he did not keep records of his quality assurance attempt, but stated that he made a recommendation for improved retention of access authorizations to facilitate future assessments.

Excessive rights and privileges to applications and ineffective reauthorization of an individual's rights and privileges weaken the overall information security program. As a result, management cannot ensure that their information systems are protected from intentional or unintentional modification.

[6] Actions taken by BIS pursuant to these reauthorization responses resulted in only the deletion of the initial level of MEDCOR access, and not the users' higher level of access. In effect, the higher level of access is not operational, but represents old, outdated information that clutters the ACF2 security system.
[7] *Review of Mainframe Access Controls at the Application Level RRB-Developed Applications Controlled by ACF2 and IDMS*, OIG Report No. 04-08, September 7, 2004, Recommendation 1.

Recommendations

We recommend that the Bureau of Information Services:

3. remove the old, outdated information identified in our review; and

4. ensure contractor access is reauthorized annually.

We recommend that the Office of Programs:

5. review the inappropriate and questionable accesses identified in our review and initiate access modification requests, based on that review.

Management's Responses

The Bureau of Information Services agrees with the recommendations and advises that the data will be modified, and contractor access will be reauthorized annually as part of the regularly scheduled reauthorization process.

The Office of Programs agrees with the recommendation and advised that they have taken corrective action.

Accountability over ACF2 Audit Logs Needs Improvement

The RRB has not enforced proper segregation of duties over, or maintained adequate retention of ACF2 audit log reviews.

GAO's *Standards for Internal Control in the Federal Government* require key duties and responsibilities to be divided or segregated among different people, including the responsibilities for processing, recording, and reviewing transactions. It states, "[n]o one individual should control all key aspects of a transaction or event." These key aspects would include the production of ACF2 audit logs of system administrator actions, and their subsequent review.

The RRB has defined auditable events as "failed user authentication attempts, changes to users' systems security information, and organization- and application-specific systems security-relevant events" such as system administrator actions.[8] ACF2 provides the means to produce administrative reports, including audit logs of administrator activities, electronically or in hard-copy paper format. Special privileges held by the system administrator allow for the production of these reports. ACF2 also allows a user with the "AUDIT" special privilege to produce these reports. Currently, the RRB's ACF2 system administrator produces the reports in hard-copy paper format, and hand delivers the audit logs to the responsible manager for review. The RRB has

[8] *RRB Information Systems Security Policy, Standards and Guidelines Handbook*, Chapter 11 (June 2007).

advised us that the various reports cannot be separated into separate print jobs, and the responsible manager has not been granted the "AUDIT" special privilege in order to produce the audit logs themselves.

In addition, the RRB has not specified a specific retention period for audit logs other than that which is needed to support after-the-fact investigations. Rather, they have designated a three-year retention period for the source data from which the audit logs are produced. However, due to a change in tape processing specifications for the retention of source data, the RRB did not have a full three years of data available that could be used for the recreation of audit logs.[9] We were told that the responsible manager retains the hard-copy ACF2 audit logs until his two designated binders are full, and then he purges the logs on a first-in first-out basis, regardless of the log's age.

As a result, the audit log of administrator actions that is produced for review is vulnerable to mishandling through loss or unauthorized alteration, and management cannot ensure their control objectives will be achieved.

Recommendations

We recommend that the Bureau of Information Services:

6. provide the responsible manager with the "AUDIT" special privilege so he can electronically produce and review the audit logs of system administrator activities; and

7. establish a retention period for the audit logs of administrator actions, and maintain the electronically produced audit logs in accordance with that retention period.

Management's Response

The Bureau of Information Services agrees with the recommendations and advises that the responsible manager will be provided the "AUDIT" special privilege as part of the conversion to RACF, and that electronically produced audit logs of administrator actions will be maintained for three years by the Infrastructure Services Center.

[9] The RRB has modified their tape processing specifications from retaining a year's worth of data separately on tapes for 3 years, to retaining a month's worth of data separately on tapes for 36 months. At the time of our review, the RRB had 19 monthly tapes and no yearly tapes.

Audit Log Content Needs Expansion

The content of the ACF2 audit logs of administrative actions is not detailed enough to allow meaningful review.

NIST SP 800-53 requires information systems to produce "audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events."[10] Audit log reports are useful in ensuring that the system or resources have not been harmed by hackers, insiders, or technical problems. As previously discussed, the RRB has defined specific auditable events for security-related data and has implemented procedures for the review of those events.

Previously, we recommended that the RRB begin reviewing logs of administrator actions.[11] However, management's corrective action to address this recommendation is not sufficient to meet NIST requirements because the content of the audit records is not sufficient to allow meaningful analysis. We found that two of the three audit logs produced for management's review contain only summary data of system administrator actions.[12] This summary data only states that an action took place, not the actual setting that was changed. A "before and after" image of the modified record or access rule is available in a detailed report, which is not currently being produced.

As a result, the RRB systems are vulnerable to misuse or abuse without early detection and management cannot ensure their control objectives will be achieved.

Recommendation

We recommend that the Bureau of Information Services:

8. produce the logs of system administrator activities using the detailed format for review by the responsible manager.

Management's Response

The Bureau of Information Services agrees with the recommendation and advises that detailed format logs will be produced for review by the responsible manager.

[10] *Recommended Security controls for Federal Information Systems,* NIST SP 800-53, Appendix F, Security Control AU-3 Content of Audit Records (December 2007).
[11] *Fiscal Year 2004 Evaluation of Information Security at the Railroad Retirement Board*, OIG Report No. 04-11, September 30, 2004, Recommendation 7.
[12] The two ACF2 audit logs that are produced in summary format are the Information Storage Update Log and the Rule Modification Log.

Audit Log of Security Violations is Misleading

The RRB's audit log of security violations is misleading because it produces many false positive occurrences of unsuccessful user attempts to access the Medicare component applications.

NIST SP 800-53 requires information systems to produce "audit records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events."[13] Audit trails, or logs, maintain a record of system or user activity and can assist in detecting security violations, performance problems, and flaws in applications.

The RRB's ACF2 systems administrator performs daily on-line reviews of the unsuccessful user attempts. However, the report of these security violations includes many false positive occurrences of unsuccessful user attempts. BIS management has advised this is because of the manner in which user access attempts are recognized by the Medicare application program code. We were advised that when an authorized user accesses MEDCOR, the programming code attempts to log the user into all possible levels of MEDCOR access, regardless of what level of access the user has been granted and tried to use. These occurrences are known as false positive security violations, because it appears a violation occurred, when one did not.

The RRB's ACF2 systems administrator stated that several of the RRB's systems produce similar false positive security violations. As a result, the review of unsuccessful user attempts is greatly hampered, and ultimately ineffective in ensuring RRB systems are not misused or abused without early detection. The RRB is currently in the process of modernizing their legacy systems. This IT Capital Plan Element is to be performed over the next 10 years with individual systems modernized based on a "high value/high risk" assessment and is to include improved accuracy and security of the systems and their transactions. The modernization of the RRB's Medicare major application is currently underway. This effort provides an opportunity to introduce programming changes that will eliminate the false positive security violations discussed above.

Recommendation

We recommend that the Office of Programs:

9. request analysis and programming revisions of the Medicare major application to ensure that only true security violations will be identified and reported.

Management's Response

The Office of Programs agrees with the recommendation and will submit a request for analysis and programming.

[13] *Recommended Security controls for Federal Information Systems,* NIST SP 800-53, Appendix F, Security Control AU-3 Content of Audit Records (December 2007).

FORM G-115f (1-92)

UNITED STATES GOVERNMENT

MEMORANDUM

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 the RRB's Medicare 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 #1
We recommend that the Bureau of Information Services establish a standard for the use of wildcard designators when preparing dataset access rules.

Response
BIS disagrees with the recommendation. The RRB dataset logical access control is being converted from the CA-ACF2 program to the IBM-RACF product for securing computer data. Although RACF will change the control strategy from that of focusing on an individual's data access to that of group access, the use of wildcard designators within the RACF environment will be similar to its use within CA-ACF2. Wildcard designators are used whenever they facilitate the administration of resources as prescribed by the instructions of the data owners.

Recommendation #2
We recommend that the Bureau of Information Services evaluate current dataset access rules and enforce the principle of least privilege by restricting overly broad wildcard access use.

Response
BIS disagrees with this recommendation. Dataset access is allocated upon request as authorized by system owners. BIS administers data access as instructed by system owners and is not responsible for determining least privilege or defining the least amount of privileges needed by users to perform their business functions.

Recommendation #3
We recommend that the Bureau of Information Services remove the old, outdated information in our review.

Response
BIS agrees with this recommendation. The Systems Assurance Group is responsible for modification of this data, which will be changed by September 30, 2009.

Recommendation #4
We recommend that the Bureau of Information Services ensure contractor access is reauthorized annually.

Response
BIS agrees with this recommendation and the Systems Assurance Group will ensure that contractor access is reauthorized annually as part of the regularly scheduled re-authorization process. The next round of re-authorizations is scheduled to occur in the 1st calendar quarter of 2010.

Recommendation #6
We recommend that the Bureau of Information Services provide the responsible manager with the "AUDIT" special privilege so he can electronically produce and review the audit logs of system administrator activities.

Response
BIS agrees with this recommendation and will make this change to provide the Chief of Operations Services and Systems Assurance in Infrastructure Services Center with the "AUDIT" special privilege as part of the conversion to the IBM-RACF system that is scheduled for implementation on or before December 1, 2009.

Recommendation #7
We recommend that the Bureau of Information Services establish a retention period for the audit logs of administrator actions, and maintain the electronically produced audit logs in accordance with that retention period.

Response
BIS agrees with the recommendation. A three year retention period for the source data from which the audit logs are produced is already in place. On or before December 1, 2009, after the logical access control is changed to the IBM RACF utility, electronically produced audit logs of administrator actions will be maintained for three years by Infrastructure Services Center.

Recommendation #8
We recommend that the Bureau of Information Services produce the logs of system administrator activities using the detailed format for review by the responsible manager.

Response
BIS agrees with this recommendation. On or before December 1, 2009, after the logical access control is changed to the IBM RACF utility, detailed format logs will be produced for review by the Chief of Operations Services and Systems Assurance in Infrastructure Services Center.

UNITED STATES GOVERNMENT

MEMORANDUM

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

SEP 11 2009

TO: Letty Benjamin Jay
Assistant Inspector General, Audit

FROM: Catherine A. Leyser
Director of Assessment and Training

THROUGH: Dorothy Isherwood
Director of Programs

SUBJECT:

Draft Report – Audit of the Railroad Retirement Board's Medicare Major Application System

MEDICARE MAJOR APPLICATION SYSTEM

Overall comments

We have reviewed the draft report and appreciate the fact that the review determined that identification and authentication, and system and information integrity controls were in place, operated as intended, and met the requirements established by FISMA.

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

Recommendation 5

The OIG recommends that the Office of Programs:

Review the inappropriate and questionable access identified in our review, and initiate access modification requests, based on that review.

OP Response

We agree. In fact we have already taken corrective action. Documentation of our corrective action was provided as a separate submission on September 3, 2009. We believe that this recommendation can be considered implemented.

Recommendation 9

The OIG recommends that the Office of Programs

Request analysis and programming revisions of the Medicare major application to ensure that only true security violations will be identified and reported.

OP Response We concur. A request for analysis and programming will be submitted by December 31, 2009. At that point we expect that this audit recommendation would be considered implemented.

Because the recommendation does not involve a significant finding or vulnerability, we do not expect the Bureau of Information Services to allocate resources to the request until the issue can be investigated as part of system modernization efforts.

cc: Chief Information Officer
Director of Policy and Systems