Fiscal Year 2004 Evaluation of Information Security
at the Railroad Retirement Board
Report No. 04-11, September 30, 2004

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) evaluation of information security 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. Each major application system is comprised of one or more component systems.

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). FISMA, like its predecessor the Government Information Security Reform Act (GISRA), establishes program management and evaluation requirements including:

- annual agency program reviews,
- Inspector General security evaluations,
- an annual agency report to the Office of Management and Budget (OMB), and
- an annual OMB report to Congress.

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide integrity, confidentiality and availability. FISMA requires agencies to report significant deficiencies in policy, procedure or practice as material weaknesses in internal control in reports issued pursuant to the Federal Managers' Financial Integrity Act.

The OIG conducted security evaluations pursuant to GISRA during FY 2001 and FY 2002 and FISMA in FY 2003. These evaluations disclosed weaknesses throughout the RRB's information security program. The OIG cited the agency with material weaknesses due to significant deficiencies in access controls in the data processing and end-user computing environments and in the training provided to staff who have significant security responsibilities. Evaluations conducted during FY 2000 and FY 2001 by specialists under contract to the OIG had disclosed the need for improvements in security controls in both the data processing and end-user computing support systems.

Objective, Scope and Methodology

The objective of this evaluation was to fulfill the requirements of FISMA by assessing the effectiveness of the RRB's information system security program and practices during FY 2004.

In order to accomplish our objective, we monitored agency efforts to implement corrective actions in response to the findings and recommendations presented in prior OIG audit reports as well as third-party evaluations conducted at the request of the OIG including:

- "Information Systems Security Assessment Report," Defensive Information Operations Group, National Security Agency, June 28, 2000;
- "Review of RRB's Compliance with the Critical Infrastructure Assurance Program," August 9, 2000, OIG Report #00-13;
- "Review of Document Imaging Railroad Unemployment Insurance Act Programs," November 17, 2000, OIG Report #01-01;
- "Site Security Assessment," Blackbird Technologies, Inc., July 20, 2001;
- "Security Controls Analysis," Blackbird Technologies, Inc., August 17, 2001;
- "Review of Information Security at the Railroad Retirement Board," February 5, 2002, OIG Report #02-04;
- "Review of the Railroad Retirement Board's Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties," August 26, 2002, OIG Report # 02-11;
- "Fiscal Year 2002 Evaluation of Information Security at the Railroad Retirement Board," August 27, 2002, OIG Report #02-12;
- "Evaluation of the Self-Assessment Process for Information System Security," December 27, 2002, OIG Report #03-02;
- "Evaluation of RRB E-Government Initiative: RUIA Contribution Internet Reporting and Payment," December 27, 2002, OIG Report #03-03;
- "Review of the Railroad Retirement Board's PIN/Password System for On-Line Authentication," September 8, 2003, OIG Report #03-09;

- "Review of the Systems Development Life Cycle for End-User Computing," September 8, 2003, OIG Report #03-10; and

- "Fiscal Year 2003 Evaluation of Information Security at the Railroad Retirement Board," September 15, 2003, OIG Report #03-11.

We also considered the findings and recommendations reported as a result of the following evaluations conducted during FY 2004:

- "Review of Mainframe Access Controls at the Application Level: Federal Financial System," September 07, 2004, OIG Report #04-07;
- "Review of Mainframe Access Controls at the Application Level: RRB-Developed Applications Controlled by ACF2 and IDMS," September 07, 2004, OIG Report #04-08; and
- "Review of Mainframe Access Controls at the Application Level: Program Accounts Receivable System," September 09, 2004, OIG Report #04-09.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objective. Fieldwork was conducted at RRB headquarters during May through August 2004.

RESULTS OF EVALUATION

Agency management continues the process of strengthening information security. However, significant deficiencies in access controls and program management continue to exist. As a result, information security remains an area of material weakness in internal control.

The OIG's conclusions with respect to information system security are based on previously reported weaknesses in training and local area network access controls for which corrective action has not been completed, and FY 2004 evaluations that disclosed continued weaknesses in the agency's mainframe access controls. Our findings with respect to the implementation status of prior recommendations for corrective action and a summary of weaknesses identified during our FY 2004 evaluations follow.

Status of Prior Recommendations for Corrective Action

During FY 2004, agency management has continued to implement OIG recommendations for improved information security. The OIG monitored 132 recommendations for corrective action. As of March 31, 2004, 84 recommendations had been fully implemented, 11 had been rejected and 37 were pending further agency action.[1] However, the RRB has not completed the corrective action needed to eliminate the previously reported deficiencies in training and access controls that were the basis for the OIG's original finding of material weakness.

In addition, reviews conducted during FY 2004 indicate that completed corrective actions typically address only the specific situation cited by the OIG. Agency managers have not extended the underlying principles to the related elements of the information security program as a whole. In some instances, the OIG's recommendation was construed very narrowly and, as a result, the agency's corrective action had virtually no effect.

For example, BIS previously reported implementation of an OIG recommendation to "include all systems in the review and re-authorization process and mandate the frequency of the process for each mainframe system."[2] OIG evaluations conducted during FY 2004 revealed that although scheduled, some re-authorizations were not performed. Similarly, agency action to "implement security logs as an effective control by ensuring that all critical activities are subject to logging…" did not include all systems.[3]

A summary of the status of audit recommendations pertaining to information system security is presented in Appendix I.

[1] These totals do not include recommendations presented in OIG Reports #04-07**, #**04-08, #04-09 which were finalized after March 31, 2004 and for which the status of implementation was not monitored during FY 2004.
[2] OIG Report 02-04, Recommendation #22
[3] OIG Report 02-04, Recommendation #10

Evaluations Conducted During FY 2004

During FY 2004, the OIG continued to provide oversight to the RRB's information security program by conducting reviews of mainframe access controls at the application level. We assessed the effectiveness of agency procedures and controls in limiting and detecting access to the major application systems that support financial management, RRA and RUIA benefit payment operations.

In general, audit testing disclosed that the agency's review and re-authorization process is not adequate to ensure that users of these major application systems are limited to only the privileges required for the performance of their current job. We also observed that system features designed to ensure accountability for changes to certain security settings have not been implemented, and that the approval settings that control transaction processing and data entry are not consistently applied.[4]

In-House Developed Applications

The approximately 45 systems that support RRA and RUIA benefit payment operations were developed in-house by the RRB's Bureau of Information Services. Security for these systems is controlled by commercial software products: CA-ACF2, an access control software package, or IDMS, a database management system.

We performed tests, on a sample basis, of the access privileges of the 1,104 users of these systems. Our tests disclosed that the existing review and re-authorization process is not adequate to ensure that system users retain only those privileges required for their current jobs. We also identified weaknesses in the implementation of segregation of duties that permit some users to perform too many key activities. In addition, one system was initially developed without a "Read-Only" access option for those who do not require higher-level privileges. In this case, access cannot be appropriately restricted.

Federal Financial System

The Federal Financial System (FFS), which includes integrated subsystems for budget execution and procurement management, is a part of the RRB's major application system that supports financial management. FFS security is controlled by the security functions built into the system.

We performed tests, on a sample basis, of the access privileges of 527 users of this system which disclosed that existing controls are not adequate to ensure that FFS users have been limited to only those system privileges required for the performance of their current jobs. At the time of our fieldwork, the agency had not performed a re-authorization review of FFS access privileges for nearly five years. The last such review had been

[4] "Review of Information Security at the Railroad Retirement Board," February 5, 2002, OIG Report #02-04 included recommendations for improvement to the review and re-authorization process and more effective use of system logging features.

conducted in 1999; a review scheduled for FY 2003 was not performed. The agency initiated a review after the end of OIG fieldwork in 2004.

We also observed that FFS features designed to ensure accountability for changes to certain security settings had not been implemented, and we questioned the level of assurance provided by current document approval settings.

Program Accounts Receivable System

The Program Accounts Receivable (PAR) system, part of the Financial Management major application system, supports financial accounting for RRA and RUIA program debt. The PAR system is not integrated with FFS and has its own, separate, built-in security functions.

We performed tests, on a sample basis, of the access privileges of 669 users of this system which disclosed that existing controls are not adequate to ensure that PAR system users have been limited to only those system privileges required for the performance of their current jobs.

Our fieldwork disclosed that the agency had not performed a re-authorization review for the PAR system since FY 1998; the review scheduled for FY 2003 was not performed. Although a re-authorization review was performed during FY 2004, the information provided to supervisors did not include sufficient detail about the specific privileges granted to individual employees to provide a basis for an effective re-authorization decision.

We also observed that PAR system features designed to ensure accountability for changes to certain security settings had not been implemented and that the approval settings that control transaction processing and data entry were not consistent across programs.

CA-ACF2 Controls Could Be Strengthened

The RRB has not implemented adequate controls to ensure that CA-ACF2 security settings implement management's policies.

The RRB has established policies and procedures that govern the key features of system security including password management, implementation of upgrades, and the restriction of special privileges. We observed weaknesses in the management of passwords and inactive accounts as well as the implementation of global system options and special privileges that, when taken together, undermine the effectiveness of the RRB's information security program.

Initial access to the RRB's mainframe computer is controlled by CA-ACF2. CA-ACF2 security features include both global system options, which apply to all system users and special, high-level privileges for some users. System accounts may be granted to individual users or set-up as a "generic " to facilitate use by groups of individuals or system-to-system communication.

Password and Account Management

The RRB has not established a policy requiring individual or generic inactive accounts to be removed from the system. In addition, many generic accounts are established with a password that never expires. The lack of adequate policy and related controls and procedures to govern account management has resulted in a large number of system users, both individual and generic, that have inactive accounts and/or passwords that never expire. Our review disclosed that of 485 generic accounts, 188 do not carry a password expiration requirement and 143 have not been used in over one year.

Global System Options

BIS did not implement recent enhancements to the global system options that would bring system operation more closely in compliance with agency password management policy until those settings were identified by the OIG. In August 2003, the RRB upgraded its version of the CA-ACF2 software. The upgraded software provided for a closer fit between the agency's password policy and the security configurations within CA-ACF2. However, BIS had not implemented the new features.

Our review of global system settings also disclosed that the RRB has not implemented all settings required for compliance with the information security requirements of the Internal Revenue Service. The Internal Revenue Service mandates certain security configurations when Federal tax information is maintained in a system.

Special Privileges

BIS has not implemented policies and procedures to ensure that adequate documentation is maintained to support decisions to grant or modify the special privileges within CA-ACF2.

Individuals who hold various special privileges are able to perform high risk activities within the system. During our review, we questioned the adequacy of documentation to support special privileges granted, including five individuals whose special privileges were not required for their current jobs. In addition, the system creates logs that track changes made by system administrators, including special privileges; the logs are not subject to routine, periodic review.

Recommendations

We recommend that BIS:

1. establish a policy defining "inactive" status with respect to individual accounts and requiring the periodic review and deletion of such accounts;
2. establish a policy defining "inactive" status with respect to generic accounts and requiring the periodic review and deletion of such accounts;

3. establish a password expiration requirement for generic accounts other than those that are exclusively system-to-system access.
4. review global system settings and make changes as necessary to ensure compliance with Internal Revenue Service requirements;
5. implement an annual review of all special privileges;
6. maintain documentation to support changes to special privileges; and
7. require periodic review of the logs that record changes made by system administrators.

Management's Response

Management concurs with the OIG's findings and plans to implement either the recommended corrective action or an appropriate alternative.

The full text of the Chief Information Officer's response is included as Appendix II to this report.

Self-Assessment Not Performed

Security self-assessments were not performed during FY 2004 for the nine RRB systems which contain sensitive information.

FISMA requires annual evaluations of Federal information security programs. OMB has issued guidance regarding the extent of the annual reviews which are dependent upon an evaluation of risk and the comprehensiveness of last year's review. At a minimum, the NIST self-assessment tool (or an equivalent) should be used.

The OIG evaluated the RRB's FY 2002 self-assessment process and reported that the process was not effective in assessing the current status of the RRB's security program as a basis for future improvement.[5] At that time, the OIG recommended that BIS take action to ensure that the agency's self-assessment process is complete, credible and comprehensive with respect to NIST objectives, elements, and techniques; and provides a consistent basis for assessing changes in the agency's security status from year to year.

Although the RRB implemented the NIST self-assessment methodology during FY 2003, the previously recommended corrective actions have not yet been completed and gaps in the collection of data will impede the overall effectiveness of the improvement process. No further recommendations are being offered at this time.

[5]"Evaluation of the Self-Assessment Process for Information System Security," December 27, 2002, OIG Report #03-02.

Computer Security Plans

The computer security plan for payment of RUIA benefits, a major application system, does not comply with OMB and NIST requirements. OMB and NIST have established basic requirements for preparation and maintenance of system security plans including a description of the system environment and the controls in place.

When the Office of Programs evaluated the computer security plan for payment of RUIA benefits in March 2004, they determined that no changes were required from the previous version which had been prepared May 2002. That determination did not include consideration of a web based, public access component system that went into production later in March 2004.

Recommendation

We recommend that:

8. the Office of Programs update the computer security plan for the major application, payment of RUIA benefits, as necessary, to ensure completeness.

Management's Response

Management agrees with the recommendation and will be incorporating references to the new RUIAnet system as appropriate.

The full text of the Office of Program's response is included as Appendix III to this report.

Acceptance of Systems Development Projects

Formal acceptance of systems development projects does not require the signature of a senior agency official with budget authority.

OMB Circular A-130, Appendix III requires pre-implementation security authorization of new systems by a management official with responsibility for the organization supported by the system. NIST also requires authorization of information systems to be given by a senior management official. Management's authorization should be specific as to acceptance of security-related risk.

Within the RRB, user organizations accept and authorize new systems and system modifications using RRB FORM G-872 "Sign Off Sheet" which is typically executed by user analysts and managers below the level of "Senior Agency Official."

In FY 2003, the OIG recommended that the RRB implement a formal certification and accreditation process that would place the acceptance of system security risk with a higher level of management.[6] The agency rejected that recommendation because NIST guidance requiring such a process had not yet been finalized.

Recommendation

We recommend that:

9. BIS implement a NIST compliant certification and accreditation program.

Management's Response

Management concurs with the recommendation and will modify and/or develop system acceptance and authorization procedures for new systems and major system modifcations in accordance with OMB Circular A-130, Appendix III and NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems."

The full text of the Chief Information Officer's response is included as Appendix II to this report.

[6] "Review of the Systems Development Life Cycle for End-User Computing," September 8, 2003, OIG Report #03-10.

SUMMARY OF AUDIT RECOMMENDATIONS PERTAINING TO INFORMATION SECURITY
As of March 31, 2004

			RECOMMENDATIONS FOR CORRECTIVE ACTION		
		REPORT DATE	OFFERED	REJECTED	IMPLEMENTED
National Security Agency	Information Systems Security Assessment Report	06/28/00	19	5	11
OIG Report #00-13	Review of RRB's Compliance with the Critical Infrastructure Assurance Program	08/09/00	2	-	2
OIG Report # 01-01	Review of Document Imaging Railroad Unemployment Insurance Act Programs	11/17/00	3	-	2
Blackbird Technologies	Site Security Assessment	07/20/01	12	2	9
Blackbird Technologies	Security Controls Analysis	08/17/01	38	3	32
OIG Report #02-04	Review of Information Security at the Railroad Retirement Board	02/05/02	28	-	15
OIG Report # 02-11	Review of the RRB's Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties	08/26/02	1	-	1
OIG Report # 02-12	Fiscal Year 2002 Evaluation of Information Security at the Railroad Retirement Board	08/27/02	3	-	2
OIG Report #03-02	Evaluation of the Self-Assessment Process for Information System Security	12/27/02	4	-	-
OIG Report # 03-03	Evaluation of the RRB E-Government Initiative: RUIA Contribution Internet Reporting and Payment	12/27/02	9	-	8
OIG Report # 03-09	Review of the Railroad Retirement Board's PIN/Password System for On-Line Authentication	09/08/03	3	-	-

SUMMARY OF AUDIT RECOMMENDATIONS PERTAINING TO INFORMATION SECURITY
As of March 31, 2004

			RECOMMENDATIONS FOR CORRECTIVE ACTION		
		REPORT DATE	OFFERED	REJECTED	IMPLEMENTED
OIG Report # 03-10	Review of the Systems Development Life Cycle for End-User Computing	09/08/03	7	-	-
OIG Report # 03-11	Fiscal Year 2003 Evaluation of Information Security at the Railroad Retirement Board	09/15/03	3	1	2
			=====	=====	=====
			132	**11**	**84**

UNITED STATES GOVERNMENT

MEMORANDUM

RAILROAD RETIREMENT BOARD

SEP 3 0 2004

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Terri Morgan
Acting Chief Information Officer

SUBJECT: Draft Report – Fiscal Year 2004 Evaluation of Information Security at the Railroad Retirement Board

We have reviewed the subject report and provide you with the following responses to the recommendations included in the report.

Recommendations 1& 2

We recommend that BIS establish a policy defining "inactive" status with respect to individual and generic accounts and requiring the periodic review and deletion of such accounts.

BIS Response

We concur with the recommendations. BIS will establish a policy regarding "inactive" accounts. The policy will define what is considered an "inactive" account status, require periodic review to identify inactive system accounts, and specify action for deletion of these types of accounts. We will develop the policy by October 31, 2004. We will inform you when the policy has been accepted and published.

Recommendation 3

We recommend that BIS establish a password expiration requirement for generic accounts other than those that are exclusively system-to-system access.

BIS Response

We will review generic accounts that are not used exclusively for system-to-system access. Based upon this review we will determine appropriate password use for these generic accounts. We will advise you regarding the results of the review and expected password usage for any remaining generic accounts by December 31, 2004.

Recommendation 4

We recommend that BIS review global system settings and make changes as necessary to ensure compliance with Internal Revenue Service requirements.

BIS Response

We concur. We shall review ACF2 global system settings and make changes as necessary to ensure compliance with Internal Revenue Service requirements. We will conduct the review and shall inform you of the results by November 30, 2004.

Recommendation 5

We recommend that BIS implement an annual review of all special privileges.

BIS Response

We concur. We will include a review of special privileges as part of the annual review of non-cancel privileges normally conducted in May and June each year.

Recommendation 6

We recommend that BIS maintain documentation to support changes to special privileges.

BIS Response

We concur. We will maintain documentation that identifies any changes to special privileges for an individual and be held in the security access folder maintained by the system security specialist. The system security specialist is now doing this.

Recommendation 7

We recommend that BIS require periodic review of the logs that record changes made by system administrators.

BIS Response

We concur. System logs are generated daily using recently activated ACF2 facilities and reviewed daily by the system security specialist.

Recommendation 9

We recommend that BIS implement a NIST compliant certification and accreditation program.

BIS Response

We concur. We will modify and/or develop system acceptance and authorization procedures for new systems and major system modifications in accordance with OMB Circular A-130, Appendix III and NIST SP800-37 Guide for Security Certification and Accreditation of Federal Information Systems. In order to establish a target date for completion we must develop a plan of action for the activities involved in the development and implementation of procedures for system acceptance and authorization. We will complete this plan by January 31, 2005; at that time we will inform you of the target completion date for implementation of these procedures.

UNITED STATES GOVERNMENT

MEMORANDUM

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

SEP 24 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- Fiscal Year 2004 Evaluation of Information Security at the Railroad Retirement Board

Response to the Draft Report

General Comments	We have read the draft report and concur with the findings and recommendations. While the report makes nine recommendations only one recommendation is directed specifically to the Office of Programs (OP).
Recommendation 8	*We recommend that the Office of Programs update the computer security plan for the major application, payment of RUIA benefits, as necessary, to ensure completeness.*
OP response	We agree. We will be incorporating references to the new RUIAnet system as appropriate. The target date for these changes will be December 31, 2004.
Copies	Director of Policy and Systems Chief of Calculation Analysis and Systems Acting Chief Information Officer Chief Security Officer