Fiscal Year 2002 Evaluation of Information Security at the Railroad Retirement Board, Report No. 02-12, August 27, 2002

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 in excess of $8 billion in benefits during fiscal year (FY) 2001.

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 (LAN) and wide (WAN) 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 application system is comprised of one or more programs.

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (Security Act)."[1] The Security Act requires annual agency program reviews, annual Inspector General security evaluations, an annual agency report to the Office of Management and Budget (OMB), and an annual OMB report to Congress.

In February 2002, the OIG published "Review of Information Security at the Railroad Retirement Board" presenting the detailed results of the OIG's review of the agency's information security. That review, conducted pursuant to the Security Act, disclosed weaknesses in most areas of the RRB's information security program. At that time, the OIG concluded that significant deficiencies in program management and access controls made the agency's information security program a source of material weakness in internal control over financial reporting.

[1] This legislation is also referred to by the acronym "GISRA."

Objectives, Scope and Methodology

The objective of this review was to fulfill the requirements of the Security Act by performing an evaluation of the RRB's information system security program and practices. The scope of this review was information system security at the RRB during FY 2002.

In order to accomplish our objectives, we monitored agency efforts to implement corrective action 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 (NSA), 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. (BBT), July 20, 2001;
- "Security Controls Analysis," Blackbird Technologies, Inc. (BBT), August 17, 2001; and
- "Review of Information Security at the Railroad Retirement Board," February 5, 2002, OIG Report #02-04.

We also performed tests of selected controls related to disaster recovery and physical security.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objectives. Fieldwork was conducted at RRB headquarters during May through June 2002.

RESULTS OF EVALUATION

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

Corrective action has not been sufficient to eliminate the most significant weaknesses in program management and access controls. Program management continues to be significantly undermined by a lack of training among key personnel. Access controls cannot be considered fully effective because of the weaknesses in account management in both the mainframe and end-user computing environments.

In our previous report, we cited the absence of a strong framework with a central management focal point as the underlying cause of many situations in which the controls that have been designed and put into operation were less than fully effective. Since that initial assessment, the RRB's Chief Information Officer has appointed a Security Officer to lead the newly created Risk Management Group within the Bureau of Information Services. However, it would be premature to assess the impact of that appointment, made in February 2002, on management effectiveness.

The following sections of this report detail our findings with respect to management's plans to remedy the previously identified weaknesses in the RRB's information security program and the status of prior recommendations for corrective action. We have also included new findings and recommendations for improvements to the agency's disaster recovery program.

Agency's Plan of Action

The Security Act requires that agencies prepare an action plan, including target dates for implementation, to remedy any significant deficiencies in information security.

In October 2001, the agency prepared and submitted to OMB an action plan to strengthen its information security program. As of June 2002, the original 15 planned corrective actions had been increased to 16, and the agency had reported full implementation in six areas.

We concur with the agency's assessment of the status of five of the six weaknesses for which full implementation has been reported. However, we disagree with management's assessment of the status of a prior recommendation for a formal security training and awareness program. Management's actions to date are not sufficient to address the original recommendations.

In April 2002, the RRB's Management Control Review Committee (MCRC) completed its review of the OIG's detailed findings concerning information security. The MCRC agreed that the deficiencies identified by the OIG constitute a material weakness in internal control and a material non-conformance with the financial requirements of the Federal Managers' Financial Integrity Act (FMFIA).

We have been advised that, based on the MCRC's concurrence with the findings in the OIG's previous report, the agency will prepare an expanded action plan. Accordingly, the OIG will defer evaluation of the adequacy of the agency's planned corrective action until a comprehensive plan has been adopted.

Status of Recommendations for Corrective Action

Responsible management and staff in the Bureau of Information Services have implemented, or plan to implement, most of the recommendations for improved information security resulting from evaluations by the OIG and technical specialists under contract to the OIG.

The OIG monitored 102 recommendations for corrective action. To date, 50 have been fully implemented, 10 have been rejected, and 42 are targeted for completion in the next 18 months.

SUMMARY OF AUDIT RECOMMENDATIONS
PERTAINING TO INFORMATION SECURITY
Status as of June 15, 2002

Report	Date	No. of Items	Implemented	Pending	Rejected
NSA	06/28/00	19	8	6	5
OIG 00-13	08/09/00	2	1	1	
OIG 01-01	11/17/00	3	2	1	
BBT	07/20/01	12	6	4	2
BBT	08/17/01	38	27	8	3
OIG 02-04	02/05/02	28	6	22	
		=====	=====	=====	=====
Totals		102	50	42	10

Although agency management has taken many of the recommended corrective actions, the major changes that will be required to alleviate the significant deficiencies identified by the OIG could not be accomplished quickly. For example, although the agency provided basic security awareness training to most employees during FY 2002, this training falls far short of an ongoing program of security awareness and did little to enhance the knowledge, skills or abilities of those charged with the design and implementation of the security program.

Similarly, implementation of corrective action to strengthen access controls is largely dependent on the re-configuration of the hardware and software that support mainframe and end-user computing. Such changes can only be implemented as part of the larger long-term planning process.

Finally, the impact of the recent appointment of a Security Officer to lead the newly created Risk Management Group may not become evident for months, or even years.

Service Level Agreements

The Bureau of Information Services' Service Level Agreements with the end-user computing community do not address user expectations concerning data backup.

OMB Circular A-130 requires that Federal agencies establish, and periodically test, the capability to continue providing service within a system based upon the needs and priorities of the participants of the system. Agency plans should ensure the ability to recover and provide service sufficient to meet the minimal needs of users of the system.

Decisions on the level of service needed at any particular time and on priorities in service restoration should be made in consultation with the users of the system and incorporated in the system rules.

The understanding between system users and information technology support personnel is formalized in a written Service Level Agreement.

The absence of Service Level Agreements for data backup operations weakens the agency's disaster recovery program because the expectations of the user community may be different from actual practice.

Recommendation

The Bureau of Information Services should develop Service Level Agreements for its data backup operations (Recommendation #1).

Management's Response

The Bureau of Information Services did not totally concur with the finding. They cited an existing Service Level agreement for mainframe backup procedures and the local area network that supports the Bureau of Fiscal Operations. The agency-wide agreement is currently being revised to incorporate additional aspects of end-user computing needs.

The full text of management's response is included as an appendix to this report.

LAN Server Not Subject to Backup

During our review, we observed a LAN server (identified as the MIPS server) that is not subject to data backup.

OMB Circular A-130 requires that Federal agencies develop disaster recovery plans to ensure the ability to recover and provide service sufficient to meet the minimal needs of users of the system. The National Institute for Standards and Technology (NIST) recommends regular data backup and the implementation of policies specifying the frequency of backups based on data criticality and the frequency with which new information is introduced.

The agency's LAN data back-up operation does not include the MIPS server because this device has not been designated for backup in the automated backup device. Bureau personnel could not offer any documentation to support the decision to exclude the MIPS server. As previously discussed, the Bureau of Information Services does not have a Service Level Agreement which would document the basis for this exclusion.

The Bureau of Information Services has advised us that the MIPS server stores old system development information, some of which has not been modified recently, although it may still be in use. However, absent documentation to support a contrary position, the omission of the MIPS server from LAN back-up operations increases the agency's risk of loss in the event of disaster.

Recommendation

The Bureau of Information Services should confer with the owners/users of the data stored on the MIPS server to determine the appropriate back-up treatment (Recommendation #2).

Management's Response

The Bureau of Information Services concurs with the recommendation. The full text of management's response is included as an appendix to this report.

Contract for Disaster Recovery Services

Controls over the modification of RRB's contract for disaster recovery services are not adequate to ensure changes are made in accordance with management's plan.

OMB Circular A-130 requires that the disaster recovery plans of Federal agencies ensure the ability to recover and provide service sufficient to meet the minimal needs of users of the system.

The RRB contracts for the equipment and services that will be required to ensure the recovery of mission-critical operations in case of disaster. The present contract has not been revised to include recent upgrades, including an additional gigabyte of mainframe storage capacity and upgrades to the end-user computing support system.

We have been advised that the contract was not modified for the upgraded mainframe storage because the previous Chief Information Officer determined that it was not necessary to do so. However, no documentation to support that decision was provided for our review.

OIG auditors could not determine exactly why the contract has not been modified to reflect upgrades to the end-user computing support system. Although the discussion of contract modification is ongoing, we do not see evidence of an affirmative decision to actually modify the contract, or to delay modification pending further upgrades.

Recommendation

The Bureau of Information Services should develop controls to ensure that all decisions related to the disaster recovery contract are formally documented (Recommendation #3).

Management's Response

The Bureau of Information Services concurs with the recommendation. The full text of management's response is included as an appendix to this report.

Hardware and Software Inventory Records

During the period allotted for fieldwork, Bureau of Information Services personnel were unable to provide auditors with a current inventory of the agency's LAN hardware and software. The Bureau of Information Services provided several equipment lists but the information was not current.

An up-to-date inventory should be maintained to support financial management, permit effective asset management, and facilitate the disaster recovery process. The lack of a readily available inventory indicates that these activities are not adequately served by current systems.

In a previous report, the OIG recommended that the Bureau of Supply and Service develop and implement a new, comprehensive system of fixed asset accounting and internal control.[2] In that report, the OIG noted that the Bureau of Information Services maintained an equipment inventory separate from the agency's master accountable property record.

The RRB is in the process of implementing a new automated system to support fixed asset management. We have been advised that the new system was implemented in May 2002, but the process of ensuring the accuracy and integrity of the data transferred to the system is expected to continue at least through the end of the current fiscal year. Accordingly, we will make no recommendation for improved inventory accountability at the present time.

[2] OIG report #00-01, "Review of Internal Control Over Fixed Assets," October 5, 1999

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

August 26, 2002

TO : Henrietta Shaw
Assistant Inspector General, Audit

FROM : Kenneth J. Zoll
Chief Information Officer

SUBJECT: Draft Report – Fiscal Year 2002 Evaluation of Information
Security at the Railroad Retirement Board

We have completed our review of the subject report and have the following comments.

Recommendation 1 – The Bureau of Information Services should develop Service Level Agreements for its data backup operations.

BIS Response – We do not totally concur with your findings regarding Service Level Agreements. An agency-wide Service Level Agreements (SLA) currently exists and addresses user expectations for all backup procedures, primarily for mainframe applications. A separate (SLA) also exists for the Bureau of Fiscal Operations (BFO) to address specific backup procedures for their network environment. The agency-wide agreement is currently being revised to incorporate additional aspects of end-user computing needs and to reflect BIS organizational changes and recently introduced technologies. The target date for the revised SLA is December 1, 2002.

Recommendation 2 – The Bureau of Information Services should confer with the owners/users of the data stored on the MIPS server to determine the appropriate back-up treatment.

BIS Response – We concur with the recommendation. Initially this server was not included because data stored on this server was identified as test data that is subject to frequent changes. However, we reconsidered and have incorporated the specified server into the regularly scheduled LAN servers back-up operation effective August 23, 2002.

Recommendation 3 – The Bureau of Information Services should develop controls to ensure that all decisions related to the disaster recovery contract are formally documented.

BIS Response – We concur with the recommendation. Formal documentation will be provided in situations in which modifications to the contract are considered, however we determine no action is required.