Fiscal Year 2003 Evaluation of Information Security at the Railroad Retirement Board Report No. 03-11, September 15, 2003

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) 2002.

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 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.

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 issued reports dated February 5, 2002 and August 27, 2002. 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 both the mainframe and end-user computing environments and in the training provided to staff with 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 2003.

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; and
- "Fiscal Year 2002 Evaluation of Information Security at the Railroad Retirement Board," August 27, 2002, OIG Report #02-12.

We also considered the findings and recommendations reported as a result of the following evaluations conducted during FY 2003:

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

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 2003.

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 access controls for which corrective action has not been completed;
- FY 2003 evaluations that disclosed weaknesses in the agency's information security program; and
- the OIG's assessment of data security and access controls related to the RRB's E-Government initiative for RUIA contributions.

Our findings with respect to the implementation status of prior recommendations for corrective action and a summary of weaknesses identified during our FY 2003 evaluations follow.

Status of Prior Recommendations for Corrective Action

Responsible management and staff in the Bureau of Information Services (BIS) 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 119 recommendations for corrective action. To date, 61 have been fully implemented and ten have been rejected.[1]

Although agency management has completed many of the recommended corrective actions, the RRB has not completed corrective action to remediate the previously

[1] These totals include recommendations presented in OIG Report #03-02 and #03-03. These totals do not include recommendations presented in OIG Report #03-10 which were finalized after the end of fieldwork and for which the status of implementation was not monitored during FY 2003.

reported deficiencies in training and access controls that were the basis for the OIG's finding of material weakness.

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

Evaluations Conducted During FY 2003

During FY 2003, the OIG continued to provide oversight to the RRB's information security program by conducting an evaluation of the effectiveness of the agency's self-assessment process for information system security. We also assessed the effectiveness of the RRB's efforts in incorporating security requirements into the systems development life cycle for end-user computing. These evaluations revealed weaknesses in both processes that undermine the effectiveness of the agency's information security program.

We also documented and assessed security procedures over the Internet DC-1 filing process, including data security and access to RRB systems in connection with the RRB E-Government initiative for RUIA contributions. This project identified weaknesses in the implementation and administration of security features in this Internet-based system.

Security Self-Assessment Process

Information security self-assessment is a key part of the annual agency program review process. The self-assessment process is used to determine the current status of a security program, and where necessary, to establish a target for improvement. The National Institute of Standards and Technology (NIST) has published a self-assessment guide that presents a standardized approach for assessing system security.

The RRB's self-assessment process for information system security has not been effective in assessing the current status of the RRB's security program as a basis for future improvement. Our review disclosed that the agency's FY 2002 self-assessment process was weakened by inadequate coverage of NIST objectives, elements and techniques; anonymous, incomplete responses to the questionnaire that served as its basic evaluation tool; and a lack of supporting documentation.

The RRB's FY 2003 self-assessment is currently underway. The process is being facilitated with a NIST compliant tool, but has not been evaluated by the OIG for efficiency and effectiveness.

Consideration of Security in the Systems Development Life Cycle for End-User Computing

Existing procedures and controls are not adequate to ensure the integration of security in systems developed for the end-user computing environment in accordance with existing agency requirements.

In addition, the RRB has not implemented a risk-based approach to pre-implementation authorization of systems development projects. In a risk-based approach to the systems development life cycle, higher levels of management authorize implementation of those projects that pose the greatest risk.

We attribute these weaknesses to the lack of a comprehensive certification and accreditation process. As a result, newly developed systems exhibit a lack of applied audit trails, weak authentication methods and poor access controls. [2]

Security Procedures Over the Internet DC-1 Filing Process

As part of its responsibilities under the RUIA, the RRB collects employer contributions which are used to fund the RUIA program. Employers make contributions and report them to the RRB on a quarterly basis using Form DC-1. In March 2002, the RRB modified the existing payment system to add a new option for electronic payment over the Internet, and Internet filing of the DC-1 reports for those railroads that adopt the Internet payment option.

The OIG's assessment of security procedures over the Internet DC-1 filing process disclosed that:

- the contractor administering the system had not fully implemented restrictions on password use and limits on log-on attempts;
- authorized users were sharing their account, password and personal identification number with unauthorized users;
- certification of the Internet DC-1 cannot be adequately validated resulting in the risk of repudiation of the information contained therein; and
- the memorandum of understanding governing this process does not adequately address the privacy and security of the data being transmitted, nor were all concerned entities party to the memorandum of understanding.

Plan of Action and Milestones is Not an Effective Tool

The RRB's plan of action and milestones (POA&M) does not adequately articulate weaknesses in the agency's information security program and planned corrective actions.

OMB has mandated the development of a formal POA&M to identify vulnerabilities in information security and track the progress of corrective action. OMB requires the inspectors general, as part of the FISMA reporting process, to assess whether their

[2]BIS declined the OIG's recommendation (Report #03-10) for development of a formal certification and accreditation process. In their response, management stated that "rather than develop new or changed procedures, the issue of non-compliance with existing procedures should be addressed." They plan to defer a determination concerning the need for a formal certification and accreditation process until NIST finalizes pertinent standards. NIST is currently circulating draft standards for Federal certification and accreditation processes (NIST SP 800-37).

agencies have developed a POA&M that serves as the authoritative tool used to identify and monitor agency actions. In addition, OMB has cited the failure to maintain a comprehensive POA&M as a significant deficiency in an agency's security program.

The RRB's POA&M is incomplete and insufficiently detailed. The 10 outstanding vulnerabilities presented in the agency's POA&M do not include known areas of vulnerability, such as:

- LAN backup,
- service packs in the headquarters end-user computing environment,
- the mainframe database management system, and
- the existing certification and accreditation process.

In addition, we believe that the POA&M should be expanded to distinguish between certain vulnerabilities related to lack of training and insufficient policy and procedure. The agency has combined some vulnerabilities for which the corrective actions are largely un-related. The POA&M currently distinguishes between general security awareness training and the need for specialized vendor supplied training. As a basis for more effective prioritization, the POA&M should identify three levels of training:

- security awareness training for all employees;
- higher level training for staff outside BIS who participate in security-related processes, such as user analysts and systems administrators; and
- specialized technical training for employees in BIS who have significant responsibility for security administration or systems development.

Similarly, the RRB's current POA&M presents a single vulnerability relating to policies and procedures that include revisions to three major areas of responsibility that are addressed in separate agency documents. The POA&M should be expanded to address the three areas separately:

- overall security,
- disaster recovery, and
- systems development.

We also noted that the agency's POA&M process places the burden of developing action plans on the agency's security officer. Although agency procedure requires program officials to furnish plans detailing recommended corrective action for control weaknesses identified during their program reviews, such plans are not consistently prepared and submitted.

The POA&M is not the only tool being used within the RRB to monitor and track agency progress in achieving an effective, compliant system of information system security. The agency's security officer maintains detailed records concerning the status of known

vulnerabilities and the OIG monitors the status of its recommendations for corrective action, and circulates status reports to responsible agency management on a semi-annual basis.

The OIG does not consider the POA&M to be an effective tool for identifying vulnerabilities and monitoring agency corrective actions according to criteria established by OMB. However, the process of remediation, as a whole, is adequately coordinated and monitored using other tools. Accordingly the OIG does not consider the deficiencies in the RRB's POA&M to be a material weakness in the agency's security program.

Recommendations

We recommend that BIS:

1. review and revise the RRB's POA&M, and

2. remind program managers to identify vulnerabilities and develop action plans.

Management's Response

Management disagrees with the recommendation to review and revise the RRB's POA&M stating that "[t]he POA&M was designed by the Office of Management and Budget (OMB) to fulfill their reporting requirements" and that "[w]e have received no feedback from OMB to indicate the reports are insufficient or inadequate."

BIS has agreed to issue a reminder to program officials concerning their responsibility to report any identified information security vulnerability and to provide a corresponding plan of action for remediation.

The full text of management's response is included as Appendix II to this report.

OIG's Comments

OMB Memorandum 03-19, dated August 6, 2003, specifically directs the Inspectors General to report on the sufficiency of agency POA&M in their annual FISMA mandated report on information security. Since OMB has asked for the OIG's assessment, the absence of any prior criticism by OMB has no significance to our evaluation.

The OIG's criticism of the RRB's POA&M pertains to its value as the designated medium of internal and external reporting for which purpose we found it to be inadequately detailed in several respects. The availability of other information does not mitigate the impact of inadequacies on those readers, such as OMB, who may expect to rely on the POA&M as the sole source of information about identified vulnerabilities and the status of remediation efforts. Our acknowledgement of the agency's other monitoring tools was intended to recognize that deficiencies in the POA&M were not due to a lack of management oversight or information.

Access to the SURGE System is Not Granted Based on Least Privilege

Access to the Survivor G-90 Expeditor (SURGE) system is not granted based on the principle of least privilege. Least privilege is the practice of restricting a user's access (to data files, processing capability, or peripherals) or type of access (read, write, execute, or delete) to the minimum necessary to perform his or her job. As a result, some individuals have received and retained access to a system that they did not require for the performance of their assigned duties.

The SURGE system automates requests for an earnings and computation record used in the payment of survivor benefits. Access to the SURGE system is granted to those individuals who are also granted access to the DATA-Q system, an informational system that provides the current status of RRA benefits. The SURGE system accepts data input and produces documentary evidence of certain computations used in annuity calculations based on that input.

Decisions concerning security should be risk-based, documented and periodically subject to review. In establishing security requirements for the SURGE system, management did not recognize that granting access to all DATA-Q users would weaken security.

Recommendation

3. The Chief Information Officer should obtain an evaluation of the security needs of the SURGE system from the system owner.

Management's Response

Management concurs with the recommendation and has agreed to request that the system owners of DATAQ and Surge review the access granted to users employing the principle of least privilege. Should the results of this review indicate that users having access to the SURGE system violates the least privilege principle, the Chief Information Officer will request system changes as appropriate.

The full text of management's response is included as Appendix II to this report.

Appendix I

SUMMARY OF AUDIT RECOMMENDATIONS PERTAINING TO INFORMATION SECURITY
As of March 31, 2003

			RECOMMENDATIONS FOR CORRECTIVE ACITON		
		REPORT DATE	OFFERED	REJECTED	IMPLEMENTED
National Security Agency	Information Systems Security Assessment Report	06/28/00	19	5	8
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	7
Blackbird Technologies	Security Controls Analysis	08/17/01	38	3	28
OIG Report #02-04	Review of Information Security at the Railroad Retirement Board	02/05/02	28		12
OIG Report # 02-11	Review of 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		1
OIG Report #03-02	Evaluation of the Self-Assessment Process for Information 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		-
			=====	=====	=====
			119	**10**	**61**

UNITED STATES GOVERNMENT

MEMORANDUM

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

September 9, 2003

TO : Henrietta Shaw
Assistant Inspector General, Audit

FROM : Kenneth J. Zoll
Chief Information Officer

SUBJECT: Draft Report – Fiscal Year 2003 Evaluation of Information Security at the Railroad Retirement Board

We have completed our review of the subject report dated August 28, 2003, and submit to you our response regarding the recommendations.

Recommendation 1

The Bureau of Information Services should review and revise the RRB's Plan of Action and Milestones (POA&M).

BIS Response: We do not agree with the recommendation. The POA&M was designed by the Office of Management and Budget (OMB) to fulfill their reporting requirements. The tool has been adequate in identifying significant agency security weaknesses, as well as tracking the status and results of the remediation effort. The POA&M, and the quarterly updates, have been submitted in its current format for several years to assist OMB with their oversight responsibilities. We have received no feedback from OMB to indicate the reports are insufficient or inadequate. Although the reporting guidance issued this year by OMB includes format changes, these changes will not substantially change the information being reported.

The POA&M was never intended to replace internal agency tracking. As you pointed out in the report, the Chief Security Officer maintains other detailed records to maintain control on the status of all recommendations. For internal agency purposes, this record is sufficient to track remedial actions.

Recommendation 2

The Bureau of Information Services should remind program managers to identify vulnerabilities and develop action plans.

BIS Response: We agree with the recommendation. We will issue a reminder to program officials that all program managers are to notify the Chief Security Officer of any identified

information security vulnerability and provide a corresponding plan of action for remediation of the vulnerability resulting from any program review conducted throughout the year. Program reviews may be system self-assessments, audits, management control reviews, quality assurance reviews or any activity that affect information security controls within a major application or general support system. Target date is October 31, 2003.

Recommendation 3

The Chief Information Officer should obtain an evaluation of the security needs of the SURGE system from the system owner.

BIS Response: We concur with the recommendation. The CIO will request that the system owners of DATAQ and SURGE review the access granted to users employing the principle of least privilege. Should the results of this review indicate that users having access to the SURGE system violates the least privilege principle, the CIO will request that system changes be made to invoke the appropriate access based on an individual's specific job duties. Target date for release of the request for system review is September 30, 2003.

cc: Chief Security Officer