Fiscal Year 2006 Evaluation of Information Security at the Railroad Retirement Board
Report No. 06-11, September 27, 2006

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 over $9.2 billion in benefits during fiscal year (FY) 2005.

The RRB's information system environment consists of six major application systems and two general support systems, each of which has been designated as moderate impact systems in accordance with standards and guidance promulgated by the National Institute of Standards and Technology (NIST). The major application systems correspond to the RRB's critical operational activities, including RRA benefit payments, RUIA benefit payments, maintenance of railroad employee compensation and service records, administration of Medicare entitlement, financial management, and the RRB's financial interchange with the Social Security Administration. The two general support systems comprise the mainframe computer and the end-user computing 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) which requires annual agency program reviews, Inspector General security evaluations, and annual agency report to the Office of Management and Budget (OMB), and an annual OMB report to Congress. FISMA also establishes minimum requirements for the management of information security in the following nine areas:

1. Risk Assessment
2. Policies and Procedures
3. Testing and Evaluation
4. Training
5. Security Plans
6. Remedial Action Process
7. Incident Handling and Reporting
8. Continuity of Operations
9. Inventory of Systems

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 any significant deficiency in policy, procedure, or practice as a material weakness in reporting under the Federal Managers' Financial Integrity Act.[1]

The OIG previously evaluated information security at the RRB during FYs 2000 through 2005, and reported weaknesses throughout the RRB's information security program.[2] The OIG also cited the agency with significant deficiencies in access controls in the mainframe and end-user computing environments, training provided to staff with significant security responsibilities, and delays in meeting FISMA requirements for both risk assessments and periodic testing and evaluation.

Objective, Scope and Methodology

This evaluation was performed to meet FISMA requirements for an annual OIG evaluation of information security that includes:

1. testing of the effectiveness of information security, policies, procedures, and practices of a representative subset of the agency's information systems; and

2. an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.

To meet the first requirement, the OIG audited the incident handling and reporting program at the RRB and evaluated the RRB's disaster recovery plan. We also started an audit of the application controls of the Daily Activity Input System/Checkwriting Integrated Computer Operation component application of the RRA benefit payment major application, which is nearing completion. These reviews were conducted in FY 2006.

To meet the second requirement, we considered the results of prior audits and evaluations of information security during FYs 2000 through 2005, including the status of related recommendations for corrective action. We also obtained and reviewed documentation supporting the RRB's performance in meeting FISMA requirements and interviewed responsible agency management and staff.

The primary criteria for this evaluation were:

- FISMA requirements;

[1] A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

[2] OIG audit reports are maintained on the RRB website at http://www.rrb.gov/oig/library.asp.

- OMB Circular A-130, “Management of Federal Information Resources”; and
- NIST standards and guidance.

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objective. Fieldwork was conducted at RRB headquarters in Chicago, Illinois from May through September 2006.

RESULTS OF EVALUATION

The RRB continues to experience difficulty in achieving an effective, FISMA compliant security program. During FY 2006, the agency completed corrective action to eliminate the previously reported significant deficiency in training. Previously identified significant deficiencies in access controls, risk assessments, and periodic testing and evaluation continue to exist, as well as other observed weaknesses in the agency’s implementation of requirements for risk based policies and procedures, a remedial action process, continuity of operations, and inventory of systems.

The agency is addressing their significant deficiencies in the previously reported areas of access controls, risk assessments, and periodic testing and evaluation. However, much work remains to be completed.

The agency is also in the process of forming an agency-wide Security and Privacy Committee. The committee is expected to include employee representatives from each major application and general support system. They will be responsible for providing direction, issuing guidance, compiling certifications, and providing specific oversight for agency-wide implementation of FISMA requirements including risk assessments, annual evaluations, and testing of controls including certification and accreditation. The RRB’s three-member Board has not yet formally approved this committee.

The details of our assessment of agency progress in complying with FISMA requirements and a summary of the weaknesses identified during our FY 2006 tests of the effectiveness of information security, policies, procedures, and practices, follow. Agency management provided no formal comments for publication with this report.

Risk Assessment

The RRB has not yet implemented an effective risk assessment process that complies with Federal information processing standards and documents critical agency determinations concerning risk. Risk management drives a FISMA mandated security program and NIST compliant certification and accreditation process.

FISMA requires periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. Risk assessment is the first step in the risk management process. Organizations use risk assessment to determine the extent of the potential threat to information and information systems, and to ensure that the greatest risks have been identified and addressed.

The OIG has previously recommended that the agency ensure complete formal risk assessments are prepared in accordance with NIST guidance.[3] The RRB has begun the process of developing a risk assessment process. In FY 2006, the Bureau of Information Services (BIS) drafted a formal risk assessment methodology which is expected to be further developed and implemented by the Security and Privacy Committee. Our review of the initial draft of the risk assessment methodology shows that it incorporates NIST standards and guidance on risk management, minimum security requirements, and certification and accreditation. The draft also incorporates existing RRB policies concerning risk analysis.

Agency action to implement prior OIG recommendations for corrective action is pending; the OIG has no additional recommendations to offer at this time.

Policies and Procedures

The RRB's policies and procedures continue to need improvement to ensure that they are comprehensive and effective in all areas of the agency's information security program.

FISMA requires that agencies include risk-based policies and procedures that cost-effectively reduce information security risks to an acceptable level and ensure that information security is addressed throughout the life cycle of each information system in their information security programs. FISMA also requires each agency to have policies and procedures that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency.

The OIG has previously recommended that the RRB develop an agency-wide security configuration policy for server operating systems, and policy and procedures for the review of contractor operations in accordance with NIST guidance.[4]

Agency action to implement prior OIG recommendations for corrective action is pending; the OIG has no additional recommendations to offer at this time.

Testing and Evaluation

The RRB's efforts to implement a consistent, FISMA compliant testing and evaluation process are not complete. Although the agency has begun planning for such a process, much work remains to be done.

FISMA requires periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on

[3] OIG Report No. 05-08, Recommendation 4.

[4] OIG Report No. 05-11, Recommendations 1 and 2.

risk, but no less than annually. The periodic tests and evaluation must include testing of management, operational, and technical controls for every system identified in the agency's inventory of systems. NIST Special Publication (SP) 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems," provides procedures for assessing the effectiveness of security controls employed in Federal information systems and directly supports the security certification and accreditation process.

The OIG previously reported that prior RRB tests did not meet FISMA requirements because they did not include all major application systems and were not comprehensive with respect to all three categories of controls: management, operational and technical. In addition, the agency had not consistently performed tests of contractor operations.

The OIG previously recommended that management act to ensure that periodic independent evaluations of system security for major applications be performed, and to ensure the quality of security self-assessments.[5]

In FY 2006, BIS incorporated a subset of the NIST SP-800-53A procedures as a test plan for common controls which are not specific to any one major application or general support system. Testing of these controls is the responsibility of the BIS Risk Management Group. The common controls address the development of policies and procedures, continuity planning, incident response, physical environment security, and personnel security. Testing has begun. The remaining NIST SP-800-53A procedures will become the responsibility of the Security and Privacy Committee, and a test plan will be designed to specifically address each individual major application or general support system.

Training

The RRB has met the FISMA requirement for information security training. During FY 2006, the RRB implemented a role-based security training curriculum and has provided a substantial portion of the current year's training plan to employees with significant security responsibilities. In addition, the agency continued its existing program for providing general security awareness training to employees and contractors.

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities as well as their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition to security awareness training, agencies are required to provide appropriate training on information security to personnel with significant security responsibilities.

The OIG cited the RRB with a significant deficiency in training during FY 2001 because individuals with decision-making responsibilities for information system security did not

[5] OIG Report No. 02-04, Recommendation 3.
OIG Report No. 03-02, Recommendations 1, 2, 3, and 4.

have adequate formal training in the theory, principles, and practice of information security. During FY 2006, we observed that the RRB had ensured all employees with significant security responsibilities completed a substantial portion of the current year's training plan. As a result, the OIG no longer considers training to be a significant deficiency.

Prior OIG recommendations for corrective action will remain open, until the agency has provided the balance of training planned under the new role-based security training curriculum. The OIG has no additional recommendations to offer at this time.

Security Plans

FISMA requires that agencies maintain subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems. The RRB has developed and maintains such plans.

Remedial Action Process

The RRB continues to experience difficulty in implementing a remedial action process that is sufficient to meet FISMA and OMB requirements. In FY 2005, we reported that the existing POAM was not comprehensive with respect to identified weaknesses, was not driven by internal risk assessments and control evaluations, and did not demonstrate prioritization of agency plans and efforts to correct the weaknesses found. Current-year action has not been sufficient to correct these deficiencies.

FISMA requires Federal agencies to maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. OMB requires agencies to develop a formal Plan of Action and Milestones (POAM) to identify vulnerabilities in information security and track the progress of corrective action. Each year, OMB requires the Inspectors General to assess the agency's POAM as part of the FISMA reporting process.

The OIG previously recommended that the RRB review and revise its remedial action process.[6] In FY 2006, the BIS began to track weaknesses and related recommendations for corrective action using an automated project management tool. However, this initiative has not been fully effective. At the time of our review, the automated system was being used to track only those recommendations that the OIG had previously identified as most significant to achieving an effective, FISMA compliant security program. The automated system includes data for 33 recommendations for which corrective action is pending, which represents only 46% of all outstanding OIG recommendations for improved information security. Additionally, BIS has not begun to use the new system to track weaknesses identified through agency reviews performed internally or by their contractor consultants.

[6] OIG Report No. 05-11, Recommendation 3.

Agency action to implement prior OIG recommendations for corrective action is pending; the OIG has no additional recommendations to offer at this time.

Incident Handling and Reporting

The RRB's incident handling and reporting program is generally effective in ensuring the confidentiality, integrity and availability of the agency's information and information technology.

FISMA mandates that Federal agencies develop, document and implement procedures for detecting, reporting, and responding to security incidents as part of its agency-wide information security program.

The OIG performed a detailed review of the RRB's incident handling and reporting program during FY 2006.[7] Although we identified some areas of program management that could be improved, we found that the agency's overall efforts were sufficient to meet the requirements established by FISMA.

The RRB has agreed with the OIG recommendations for corrective action presented in that report, and has begun to address these deficiencies. The OIG has no additional recommendations to offer at this time.

Continuity of Operations

The agency's disaster recovery plan provides assurance that major information technology functions would be operational in the event of a disaster. However, the plan does not provide reasonable assurance that the agency will be able to recover from a major disaster and perform its critical business functions in a timely manner.

FISMA requires Federal agencies to implement plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

The OIG performed an evaluation of the RRB's disaster recovery plan during FY 2006.[8] We found that the RRB limits disaster recovery tests to the recovery phase of the plan and, as a result, does not have adequate assurance that procedures are maintained in a constant state of readiness. Additionally, the RRB has not completed corrective action to implement prior OIG recommendations that the agency update its overall disaster recovery plan and ensure that all decisions related to the disaster recovery contract be formally documented.[9]

[7] OIG Report No. 06-09.

[8] OIG Report No. 06-08.

[9] OIG Report No. 02-04, Recommendation 6.
OIG Report No. 02-12, Recommendation 3.

The RRB has agreed with the OIG recommendations for corrective action presented in OIG Report No. 06-08, and has begun to address these deficiencies. The OIG has no additional recommendations to offer at this time.

Inventory of Systems

The agency has not yet completed compilation of a reliable inventory of its systems. In FY 2006, BIS started the process of compiling a single, comprehensive inventory of application systems that is intended to address the needs of all organizational units.

FISMA established a requirement that each agency develop, maintain, and annually update an inventory of major information systems operated by the agency or that are under its control. This inventory is to include an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency.

In FY 2005, we reported that the RRB had not compiled a reliable inventory that identifies component applications operating in the end-user computing general support system, the related server locations or the security administrators. We also reported that the RRB's system inventories are maintained by several different organizational units whose efforts are not coordinated or consistent. Accordingly, the OIG has recommended that the agency take action to improve its systems inventory.[10]

In FY 2006, we reviewed agency efforts to date and noted that the BIS inventory continues to omit some systems identified by other organizational units. Additionally, the inventory does not show the same information system platform indicators (mainframe vs. end-user computing) for all systems. We shared these discrepancies with BIS in accordance with OMB's FY 2006 FISMA reporting requirements.

Agency action to implement prior OIG recommendations for corrective action is pending; the OIG has no additional recommendations to offer at this time.

[10] OIG Report No. 05-08, Recommendations 1, 2, and 3.