OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2008 Evaluation of Information Security at the Railroad Retirement Board

Report No. 08-05
September 30, 2008

RAILROAD RETIREMENT BOARD

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 $9.8 billion in benefits during fiscal year (FY) 2007. The RRB is headquartered in Chicago, Illinois and has 53 Field Offices across the nation.

The RRB's information system environment consists of six major application systems and two general support systems, each of which has been designated as a moderate impact system 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 employees' service and compensation 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 local area network/personal computer (LAN/PC) systems.

This evaluation was conducted pursuant to Title III of the E-Government Act of 2002, the Federal Information Security Management Act of 2002 (FISMA), which requires 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. FISMA also establishes minimum requirements for the management of information security in nine areas.

- Risk Assessment
- Policies and Procedures
- Testing and Evaluation
- Training
- Security Plans
- Remedial Action Process
- Incident Handling and Reporting
- Continuity of Operations
- Inventory of Systems

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity, and availability. An information system is a "discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology."[1]

The OIG previously evaluated information security at the RRB during FYs 2000 through 2007, 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 LAN/PC environments, as well as delays in meeting FISMA requirements for both risk assessments and periodic testing and evaluation.

The Bureau of Information Services (BIS), under the direction of the Chief Information Officer is responsible for the RRB's information security and privacy programs. FISMA requires agencies to report any significant deficiency as a material weakness under the Federal Managers' Financial Integrity Act.[3]

Objective, Scope and Methodology

This evaluation was performed to meet FISMA requirements for an annual OIG evaluation of information security during FY 2008. Our evaluation included:

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

2. assessing the RRB's compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.

To meet the first requirement, the OIG audited application controls in the Financial Interchange major application in accordance with NIST Special Publication (SP) 800-53 guidance.[4] We began an audit of the Financial Management major application in accordance with the Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM), GAO/AIMD-12.19.6. We also performed ongoing reviews of the agency's significant deficiency in access control by conducting penetration tests of agency servers.

[1] NIST Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems."

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

[3] A significant deficiency is a weakness in an agency's overall information systems security program, 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.

[4] FISMA establishes minimum security requirements for all agency operations and assets. These requirements are listed in NIST SP 800-53.

To meet the second requirement, we considered the results of prior audits and evaluations of information security during FYs 2000 through 2007, 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. Lastly, we examined documentation related to the RRB's Medicare contractor operations to determine whether controls were designed to meet FISMA requirements. Our tests of contractor operations did not include an assessment of whether the controls were operating or effective.

The primary criteria for this evaluation included:

- FISMA requirements;
- OMB Circular A-130, "Management of Federal Information Resources";
- OMB memoranda;
- NIST standards and guidance; and
- GAO FISCAM.

Our work was performed 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 May through September 2008.

RESULTS OF EVALUATION

The RRB has not yet achieved an effective FISMA compliant security program. The agency is addressing its significant deficiencies in the previously reported areas of access controls, risk assessments, and periodic testing and evaluation; however, much work remains to be completed.

Previously identified weaknesses in the areas of risk based policies and procedures, a NIST compliant certification and accreditation program, the identification of contractors, an effective remedial action process, the continuity of operations, and the inventory of systems continue to exist. During our FY 2008 evaluation, we also observed weaknesses in the agency's implementation of timely, NIST compliant, system security plans, and in the identification and training of temporary employees.

The details of our assessment of agency progress in complying with FISMA requirements and a summary of the weaknesses identified during our FY 2008 evaluations, including recommendations for corrective action, follow. Agency management has agreed to take the recommended corrective action for all recommendations except Recommendation 3 for which they are seeking legal counsel. The full text of managements' response is included in this report as Appendices I and II.

Certification and Accreditation

The RRB has not yet implemented a NIST compliant certification and accreditation program.[5] The OIG cited the RRB with this deficiency in FY 2003. We found that existing agency procedures for authorizing the processing of information systems were not adequate to meet NIST requirements because they did not place responsibility at a high enough level of agency management and were not supported by adequate risk assessment and testing processes.

OMB Circular A-130, Appendix III requires that agency management authorize systems for processing based on the formal technical evaluation of the management, operational, and technical controls. This authorization should occur at least every three years or when there has been a significant change to the system. NIST SP 800-37 provides that security accreditation should be given by a senior agency official who has authority to oversee the budget and business operations of the information system.

Agency management rejected the OIG's recommendation to develop a formal certification and accreditation process when it was first offered in FY 2003, but agreed to implement the recommendation when it was again offered in FY 2004.[6]

[5] The terms certification and accreditation are synonymous with the formal technical evaluation of the controls and the authorization of the information system for processing, respectively.

[6] OIG Report No. 03-10, Recommendation 6.

That recommendation is pending corrective action. Elsewhere in this report we discuss the significant deficiencies in the RRB's risk assessment and testing and evaluation processes which are critical elements of certification and accreditation.

During FYs 2007 and 2008, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's two general support systems and five of the six major applications. The contract includes the preparation of risk assessments, updated security plans, security testing and evaluations, and a Plan of Action and Milestones (POAM) for each system reviewed. As of August 2008, only the LAN/PC general support system had been fully certified and accredited. The certification and accreditation of the mainframe general support system and five major applications are currently in progress; certification and accreditation of the sixth major application has not been scheduled.

Our evaluation also disclosed that the Financial Management major application system was not included in the RRB's certification and accreditation initiative because of a pending government-wide financial management modernization project. That project, the Financial Management Line of Business, will require most Federal agencies to migrate their financial management activities to a shared service provider. While the RRB has budgeted for a feasibility study during FY 2010, it has not established a date for early implementation of a new system which OMB requires by September 2016. Excluded from the agency-wide effort, the financial management major application could operate for up to eight years without being certified and accredited.

Without a formal, NIST compliant, certification and accreditation of all of its major applications, the RRB cannot ensure that the information system is operating at an acceptable level of risk to agency operations, assets, or individuals.

Recommendation

1. We recommend that the Bureau of Fiscal Operations ensure that a formal, NIST compliant, certification and accreditation of the Financial Management major application is performed.

Management's Response

The Bureau of Fiscal Operations has agreed to request funding for a certification and accreditation of the Financial Management major application.

OIG Report No. 04-11, Recommendation 9.

Access Control

The design and implementation of access controls in the RRB's general support and application systems is not adequate to meet minimum standards of least privilege established by OMB Circular A-130, Appendix III. Least privilege is the practice of restricting a user's access or type of access to the minimum necessary to perform his or her job.

In our FY 2001 evaluation of information security (and confirmed by technical specialists under contract to the OIG), we cited the agency with a significant deficiency in access control and made several recommendations. Since that time, additional recommendations have been made. As of September 4, 2008, the agency has 14 open audit recommendations dealing with access control. [7]

Our FY 2008 assessment of information security in the Financial Interchange major application identified access and sharing permissions that do not restrict the financial interchange files and folders in a manner consistent with the principle of least privilege. We also reported that individuals with high-level privileges and non-unique identification and passwords compromise accountability and access control. Based on our review, we made three additional recommendations in the area of access control.

Our ongoing reviews of the agency's significant deficiency in access control through penetration tests of agency servers also disclosed poor security configurations that allowed access to unauthorized users. The results of these reviews were communicated to agency management through separate memoranda and agency officials have taken actions to address the weaknesses.

Excessive rights and privileges weaken the overall information security program.

<u>Recommendation</u>

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

[7] OIG Report No. 02-04, Recommendations 13, 20 and 21.
Blackbird Technologies, Inc. Report dated 07/20/01, Recommendation 5.
OIG Report No. 04-08, Recommendation 1.
OIG Report No. 05-08, Recommendations 10 and 11.
DSD LAN Report dated 06/07/05, Recommendations 6, 7, 8 and 9.
DSD SCAN Report dated 06/07/05, Recommendation 6.
DSD WEB Report dated 06/07/05, Recommendation 16.
OIG Report No. 07-08, Recommendation 1.

Risk Assessment

The RRB has not implemented an effective risk assessment process including documentation of agency determinations regarding risk. Organizations use risk assessments to determine the potential threats to information and information systems and to ensure that the greatest risks have been identified and addressed.

FISMA requires Federal agencies to periodically assess the risk and magnitude of harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or information systems. NIST SP 800-30, "Risk Management Guide for Information Technology Systems," presents a risk assessment methodology agencies can use when performing their periodic assessments.

In FY 2005, we cited the agency with a significant deficiency because the agency had made little progress in implementing a formal risk assessment process in accordance with NIST guidance. We also recommended that the agency complete formal, NIST compliant, risk assessments of the major application and general support systems.[8] That recommendation is pending corrective action.

During FYs 2007 and 2008, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's major applications and general support systems. This contract included the preparation of formally documented, NIST compliant, risk assessments. As of August 2008, only one risk assessment for the RRB's LAN/PC general support system had been finalized. Draft risk assessments have been prepared for most of the other information systems under the contract for certification and accreditation.

Our review of the LAN's risk assessment document showed that the contractor had completed the risk assessment in accordance with NIST guidance; however, we noted some weaknesses in the final product, particularly in the description of the system environment and in the control analysis for system backups. We attribute these weaknesses to an ineffective review process of contractor deliverables performed by BIS. As a result, the effectiveness of the certification and accreditation process and the information security program as a whole is undermined.

<u>Recommendation</u>

2. We recommend that the Bureau of Information Services review and update the LAN/PC general support system's risk assessment to accurately reflect the current RRB system environment and control analysis.

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

Management's Response

The Bureau of Information Services concurs with this recommendation and will adjust the risk assessment to compliment the current environment.

Testing and Evaluation

The RRB has not yet implemented a consistent, FISMA compliant, testing and evaluation process.

FISMA requires periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices performed with a frequency depending on 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, including contractor operations. NIST 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 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. We recommended that management act to ensure periodic independent evaluations of system security for major applications, as well as the quality of security self-assessments.[9]

The OIG's FY 2005 FISMA evaluation cited the RRB with a significant deficiency in its testing and evaluation program because the agency had made little progress in implementing a compliant periodic testing and evaluation process. In FY 2007, we reported agency efforts to perform NIST compliant tests of certain common controls were not fully effective because testing did not extend to RRB offices outside of headquarters. We recommended that agency test and evaluation plans be extended to include these other offices.[10]

During FY 2007, the RRB completed the certification and accreditation process for its LAN/PC general support system, but did not provide for subsequent testing and evaluation during FY 2008. BIS advised us that their FY 2008 testing had been limited to vulnerability scans to verify correction of weaknesses identified in the prior

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

[10] OIG Report No. 07-08, Recommendation 2.

year’s certification and accreditation process; however, no documentation was made available for our review.

Inadequate testing and evaluation weakens the security program as a whole. As a result, the RRB cannot ensure the confidentiality, integrity, or availability of agency information.

Recommendation

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 of Contractor Operations

The RRB’s tests and evaluations are not comprehensive with respect to contractor operations.

FISMA requires agencies to provide “information security protections … of (i) information collected or maintained by or on behalf of an agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency….” Additionally, each agency shall “develop, document, and implement an agencywide information security program … to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source….”

OMB M-08-21, “FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,” states that each agency must ensure their contractors abide by FISMA requirements. Additionally, agencies “are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not ‘equivalent,’ security procedures.”

In FY 2005 we reported that the agency did not have formal policies and procedures for the review of contractor operations and recommended that BIS develop the policies and procedures in accordance with NIST guidance. That recommendation was closed as implemented on July 5, 2007, when BIS published instructions on how to perform and document information security site assessments. These instructions are published in the RRB Information Systems Security Policy, Standards and Guidelines Handbook.

Although the RRB has implemented a policy to perform and document information security site assessments, they have not developed a comprehensive plan to accomplish testing and evaluation of all of the RRB’s contractor operations. We have observed that while some program managers are taking action to perform site assessments, others have not.

Inadequate testing and evaluation of contractor operations weakens the security program as a whole. As a result, the RRB cannot ensure the confidentiality, integrity, or availability of agency information processed by contractors.

Recommendation

3. We recommend that the Bureau of Information Services develop a comprehensive plan for the testing and evaluation of the agency's contractor operations.

Management's Response

The Bureau of Information Services advises that this recommendation is under consideration pending legal counsel to verify which agency contracts should be considered for certification and accreditation as information systems in compliance with FISMA requirements. They will advise the Office of Inspector General of their decision regarding concurrence or non-concurrence after guidance is provided.

Policies and Procedures

The RRB continues to need improvement in implementing risk-based policies and procedures that are comprehensive and effective in all areas of the agency's information security and privacy programs.

FISMA requires that agencies include risk-based policies and procedures that reduce risks to an acceptable level and ensure that information security (which includes the confidentiality, integrity, and availability of information) is addressed throughout the life cycle of each information system.

During FY 2007, we conducted several reviews which disclosed the need for additional policies, procedures and practices to address information security and privacy weaknesses for overall improvement in the agency's information security and privacy programs.[11] Those recommendations are pending corrective action.

During our FY 2008 review of the agency's security awareness and training program we identified a temporary employee in an RRB field office, for which no signed

[11] OIG Report No. 07-02, Recommendations 2, 3 and 4.
OIG Memorandum No. 07-02m, Recommendation 1.
OIG Report No. 07-04, Recommendations 1, 2, 3, 4, 5 and 6.
OIG Report No. 07-06, Recommendations 1, 2, 3, 5, 6, 7, 8, 10, 13, 14, 15 and 16.
OIG Report No. 07-07, Recommendations 2 and 4.
OIG Report No. 07-09, Recommendations 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, and 22.

Computer Access Authorization Request had been submitted to headquarters. The Computer Access Authorization Request includes the employee’s signed acknowledgement of the expected rules and behaviors associated with computer access. The form also provides the employee with notice of penalties should violation of the rules and behaviors occur. These forms are maintained by BIS to support access control. Temporary employees are hired by the RRB through local employment agencies on an as needed basis for short periods of time when workloads are high. Information for these employees is not maintained in the RRB’s personnel and payroll systems.

We found that BIS has not developed any controls to ensure timely submission of the authorization requests from field offices. As a result, there is a risk that the authorization request may not be obtained from the field office employee or be available to agency management, if the signed acknowledgement of the expected rules and behaviors is needed.

Recommendation

4. We recommend that the Bureau of Information Services develop controls to ensure Computer Access Authorization Requests are received from field offices in a timely manner.

Management’s Response

The Bureau of Information Services concurs with the recommendation and advises they are developing controls to ensure Computer Access Authorization Requests are received from field offices in a timely manner.

Training

The RRB has met the FISMA requirement for information security training for employees and contractors, but needs improvement to ensure that temporary employees are included in the training program.

FISMA requires agencies to provide security awareness training to employees, contractors, and other users of information systems. In addition to security awareness training, agencies are required to provide appropriate training on information security to personnel with significant security responsibilities. The RRB has developed a security awareness training pamphlet, RRB Form G-15, which provides an overview of the RRB’s policies and procedures for information security. Personnel are required to sign Form G-15a to acknowledge that they have read and understand this pamphlet. Annual refresher training may or may not consist of reviewing this pamphlet, as other areas of concentration may be desired by agency management.

Our review of the agency's security awareness and training program disclosed that the RRB did not provide security awareness training to all temporary employees because the field offices were not instructed to ensure such training. We also observed that the training records maintained by BIS inaccurately categorized some temporary employees as regular employees when the field office provided the security awareness training. In those instances, the field office provided the training to all field office employees, regardless of employment status.

Security awareness training informs users of their duties and responsibilities in complying with agency policies and procedures to reduce risks associated with information security. Untrained temporary employees pose additional risks because their corporate culture may not be aligned with agency policy, procedures, and rules of behavior.

Recommendation

5. We recommend that the Bureau of Information Services develop controls to identify temporary employees and ensure that each temporary employee is provided with security awareness training when the temporary employee is hired.

Management's Response

The Bureau of Information Services concurs with the recommendation and advises they are developing improved procedures to ensure that all employees and contractors are provided with security awareness training when hired.

Security Plans

The RRB has responded to the requirement for system security plans; however, more work is needed to ensure all plans are completed in accordance with NIST guidance.

FISMA requires that agencies maintain subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems. System security plans document this information. The RRB's Administrative Circular IRM-7, "Security Plans for Information Technology Systems," requires system security plans to be updated every two years using guidance established by NIST SP 800-18, "Guide for Developing Security Plans for Federal Information Systems."

During FYs 2007 and 2008, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's two general support systems and five of the six major applications, including the completion of updated system security plans in accordance with NIST guidance. As of August 2008, only the

LAN/PC general support system security plan was finalized. Draft system security plans have been prepared for most of the other information systems under contract for certification and accreditation. Since the Financial Management system was not included in the contract, no updated system security plan was prepared by the contractor for that system.

When we advised the RRB in July 2008 that the Financial Management major application's system security plan was out-of-date, the RRB took action to update that plan. However, they did not prepare the updated plan in accordance with NIST guidance. NIST guidance requires a description of the individual security controls in place or planned for the information system, as well as the identification of any common controls that are not system specific.

Our review of the LAN/PC system security plan showed that the contractor also did not complete the plan in accordance with NIST guidance. We noted that the system security plan contained inaccurate or missing information for system environment, wireless and mobile device accesses, system interconnections, and the identification of common controls. We also noted that the system security plan document did not contain completion or approval dates. We attribute these weaknesses to an ineffective review process of contractor deliverables performed by BIS.

Incomplete or inaccurate system security plans undermine the information security program as a whole.

Recommendations

6. We recommend that the Bureau of Fiscal Operations prepare an updated system security plan in accordance with NIST guidance.

7. We recommend that the Bureau of Information Services review and update the LAN/PC system security plan to address the inaccurate or missing information.

Management's Responses

The Bureau of Fiscal Operations has agreed to request funding for a certification and accreditation of the Financial Management major application, and hopes to utilize the existing contract the agency has in place for the other agency systems.

The Bureau of Information Services concurs with the recommendation and will review the system security plan that was provided during the certification and accreditation process.

Remedial Action Process

The RRB's remedial action process continues to be ineffective in identifying and prioritizing all weaknesses in the agency's information security and privacy programs.

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 POAM to identify vulnerabilities in information security and privacy, and to track the progress of corrective action. Each year, OMB requires the OIG to assess the agency's POAM as part of the FISMA reporting process.

The OIG first criticized the RRB's POAM in FY 2003 as ineffective in articulating weaknesses and planning corrective actions, and recommended the RRB review and revise the POAM to include the items that were missing. The RRB rejected that recommendation.[12] In FY 2005, we again reported that the existing POAM was not comprehensive with respect to identifying weaknesses, and provided inadequate prioritization of agency plans and efforts to correct the weaknesses found. In FY 2007, we also reported that the agency was not preparing action plans for their privacy-related weaknesses and those weaknesses were not being incorporated into the existing POAM. We made recommendations to address these issues.[13]

During FYs 2007 and 2008, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's two general support systems and five of the six major applications. The contract includes the preparation of individual POAMs for each system. As of August 2008, only the LAN/PC general support system has been fully certified and accredited. Certification and accreditation of the mainframe general support system and five major applications are currently in progress.

Our current assessment of the existing POAM shows that the agency has not prepared an "agency-wide" POAM, nor has the POAM developed during the LAN/PC certification and accreditation been kept up-to-date. On July 2, 2008, we were provided a copy of the POAM developed for the LAN/PC general support system which had not been updated since November 30, 2007. This POAM did not reflect any entries to support actions the agency claims to have taken to address the security weaknesses. Additionally, this POAM did not incorporate all of the weaknesses identified in the risk assessment process. For example, we observed

[12] OIG Report No. 03-11, Recommendation 1.

[13] OIG Report No. 05-11, Recommendation 3.
OIG Report No. 07-06, Recommendation 15.

that the risk assessment identified a weakness concerning modem usage, while the POAM omitted that weakness altogether.[14]

As a result, agency efforts to date have been insufficient in correcting POAM deficiencies, and it is not being used as the management tool OMB intended for identifying vulnerabilities and monitoring agency corrective actions.

Recommendation

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.

In FY 2006, the OIG performed a detailed review of the RRB's incident handling and reporting program and found that agency's overall efforts were sufficient to meet the requirements established by FISMA. We did, however, recommend some areas where program management could be improved.[15] Our reviews performed in FYs 2007 and 2008 did not disclose any additional weaknesses.

Recommendation

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

Continuity of Operations

The RRB has developed a continuity of operations plan that generally meets FISMA requirements, but some improvements can be made.

[14] We discuss this weakness in further detail in the report section entitled "Inventory of Systems."

[15] OIG Report No. 06-09, Recommendations 1, 2, 3, 4, 7, 8, 9 and 10.

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.

Historically, the RRB has provided for semi-annual off-site recovery testing of the two general support systems and the mainframe databases of its major application systems. The RRB generally also tests some of the major application batch processes, and LAN connectivity. As a result, the agency's disaster recovery plan provides assurance that most of the agency's major information technology functions would be operational in the event of a disaster. However, the agency has not yet ensured that the disaster recovery training plan is followed, data packs containing sensitive information are cleared before leaving the test site, or that each major application system is scheduled for off-site testing. [16]

In FY 2007, we reported that the agency had never performed off-site testing of the Financial Interchange major application and that the Financial Management major application had not been tested since FY 2002. In March 2008, the agency performed off-site testing of the Financial Management major application. The RRB also advised us that they expect to include the Financial Interchange major application in their off-site testing in September 2008.

Recommendation

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

Inventory of Systems

The RRB has generally complied with FISMA requirements to identify major and component applications, but continues to need improvement in establishing a reliable fixed asset inventory of information technology equipment.

FISMA requires that each agency develop, maintain, and annually update their inventory of major information systems. 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.

Our review showed that while the agency has made progress in updating their inventory of component applications and server locations, work remains to be completed to identify the component system's responsible official when security administration is decentralized.[17] Additionally, in FY 2007 we recommended that the

[16] OIG Report No. 06-08, Recommendation 5.
OIG Report No. 07-08, Recommendations 5 and 6.

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

RRB perform a physical inventory of information technology hardware and update the agency's official fixed asset inventory system.[18] That recommendation is currently pending corrective action.

During our review of the risk assessment prepared for the LAN/PC certification and accreditation, we noted a weakness had been reported concerning modem usage while the POAM omitted that weakness altogether. We obtained the results of a modem study performed by BIS between May and August 2008, and observed data discrepancies between the listing of modems identified in that study and the inventory of modems in the agency's fixed asset inventory system. Additionally, we observed that some employees listed in the study continue to have a modem in their workstation, even though they stated they no longer require the modem for their job functions. We noted that some, but not all, modems used by the agency are configured to access only other Federal agencies in a secure manner. We also noted that some modems are not secure, and pose additional threats to the agency's network.

Recommendation

8. We recommend that the Bureau of Information Services continue their efforts to identify each agency modem, address data discrepancies between their study and the fixed asset inventory system, and implement controls to ensure adequate protection of the RRB network.

Management's Response

The Bureau of Information Services concurs with the recommendation and states that the ongoing modem study project is intended to identify agency modems, address data discrepancies regarding modems in the fixed asset inventory system and assess RRB network modem controls.

[18] OIG Report No. 07-08, Recommendation 7.

Appendix I

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

SEP 24 2008

TO : Letty B. Jay
Assistant Inspector General for Audit

FROM : John M. Walter
Chief of Accounting, Treasury, and Financial Systems
THROUGH: Kenneth P. Boehne
Chief Financial Officer

SUBJECT: Fiscal Year 2008 Evaluation of Information Security at the Railroad Retirement Board

The draft report, "Fiscal Year 2008 Evaluation of Information Security at the Railroad Retirement Board," included the following recommendations for BFO:

1. ***We recommend that the Bureau of Fiscal Operations ensure that a formal, NIST compliant, certification and accreditation of the Financial Management major application is performed.***

6. ***We recommend that the Bureau of Fiscal Operations prepare an updated system security plan in accordance with NIST guidance.***

BFO requested fiscal year 2008 funding to initiate the effort to modernize its financial management system. Specifically, the funding was to have a contractor assist RRB management in planning a timeline for modernizing its financial management system, conducting an assessment of the RRB's core financial management system (FFS) to determine whether performance gap(s) exist or can be anticipated between its overall financial management strategy and its current financial solution. When evaluating a performance gap, the contractor is to consider Financial Systems Integration Office requirements, internal audit standards and statutory requirements, the agency's enterprise financial management system, and its business architecture. Due to budget constraints, funding was not available in fiscal year 2008 for this contract.

We have requested funding for a Certification and Accreditation (C&A) of the Financial Management major application. Hopefully, the funding will be available to utilize the existing contract the agency has in place for completing C&A's for the other agency systems.

cc: Terri Morgan, Chief Information Officer
Robert Piech, Chief Security Officer
Kris Garmager, Financial Systems Manager
Mike Zulevic, IT Specialist
William Flynn, Executive Assistant
Jill Roellig, Management Analyst

Appendix II

FORM G-115f (1-92)

UNITED STATES GOVERNMENT

MEMORANDUM

RAILROAD RETIREMENT BOARD

September 30, 2008

TO : Letty Benjamin Jay
Assistant Inspector General, Audit

FROM : Terri Morgan
Chief Information Officer Terri S. Morg

SUBJECT: Draft Report – Fiscal Year 2008 Evaluation of Information Security at the Railroad Retirement Board

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

Recommendation 2

We recommend that the Bureau of Information Services review and update the LAN/PC general support system's risk assessment to accurately reflect the current RRB system environment and control analysis.

BIS Response

We concur with the recommendation. There is already a system risk assessment process existing that should be updated. Once we have a document that accurately reflects the current RRB system environment, we can adjust our risk assessment plans to compliment the current environment. An accurate map of our environment has to be provided by the engineers in order to accomplish this recommendation. This should be completed by September 30, 2009.

Recommendation 3

We recommend that the Bureau of Information Services develop a comprehensive plan for the testing and evaluation of the agency's contractor operations.

BIS Response

This recommendation is under consideration. We are seeking legal counsel on this issue to verify which agency contracts should be considered for certification and accreditation as information systems in compliance with FISMA requirements. We will advise the OIG of our decision regarding concurrence or non-concurrence after guidance is provided.

Recommendation 4

We recommend that the Bureau of Information Services develop controls to ensure Computer Access Authorization Requests are received from field offices in a timely manner.

BIS Response
We concur with the recommendation. We are developing procedures to ensure that Computer Access Authorization Requests are received from field offices in a timely manner. The process improvement will be implemented by October 31, 2008.

Recommendation 5
We recommend that the Bureau of Information Services develop controls to identify temporary employees and ensure that each temporary employee is provided with security awareness training when the temporary employee is hired.

BIS Response
We concur with the recommendation. We are developing improved procedures to ensure that all employees and contractors are provided with security awareness training when hired. The new procedures will be implemented by November 21, 2008.

Recommendation 7
We recommend that the Bureau of Information Services review and update the LAN/PC system security plan to address the inaccurate or missing information.

BIS Response
We concur with the recommendation. The System Security Plan (SSP) provided to the Agency by DSD during the C&A process (Aug-2007) will be reviewed and completed by December 31, 2008.

Recommendation 8
We recommend that the Bureau of Information Services continue their efforts to identify each agency modem, address data discrepancies between their study and the fixed asset inventory system, and implement controls to ensure adequate protection of the RRB network.

BIS Response
We concur with the recommendation. The ongoing modem study project is intended to identify agency modems, address data discrepancies regarding modems in the fixed asset inventory system and assess RRB network modem controls by March 30, 2009.