OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2007 Evaluation of Information Security at the Railroad Retirement Board

Report No. 07-08
September 27, 2007

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 $9.5 billion in benefits during fiscal year (FY) 2006. Also in FY 2006, the RRB reported over 522,000 Medicare enrollees for which 11.7 million Medicare Part B claims totaling more than $900.5 million were paid. The RRB is headquartered in Chicago, Illinois, and has 53 Field Offices and 3 Regional 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 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 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. The Bureau of Information Services, 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 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 2006, 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. During FY 2006, the agency completed corrective action to eliminate the previously reported significant deficiency in training.

During FY 2007, the agency formed two new committees to help manage information security and privacy related issues. The Information Security and Privacy Committee is responsible for facilitating the implementation of FISMA and the E-Government Act and for ensuring agency-wide compliance with the Acts. The committee is also involved in privacy management compliance. The Agency Core Response Group is responsible for conducting a risk analysis to determine whether a loss of personal information resulting from a data breach poses identity theft problems. The agency's response to the data breach will be contingent upon the nature and scope of the risk identified by the committee.

Objective, Scope and Methodology

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

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 the application controls of the Daily Activity Input System/Checkwriting Integrated Computer Operation component application of the RRA benefit payment major application, the state wage match data transmission controls, the federal income taxes withheld from railroad retirement annuities, and the controls to safeguard sensitive personally identifiable information.

[1] 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.

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

The OIG also evaluated the RRB's privacy program, and began an evaluation of the information security for the financial interchange major application. These reviews were conducted in FY 2007.

To meet the second requirement, we considered the results of prior audits and evaluations of information security during FYs 2000 through 2006, 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 for one of the RRB's contractor operations to determine whether controls were designed to meet FISMA requirements.[3] 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"; 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 2007.

Scope Limitation Caused by Appropriation Restrictions

FISMA requires an annual OIG evaluation of the agency's information security program and practices which includes all agency general support and major application systems, including the Medicare program. However, we cannot fulfill our FISMA oversight mandates because we are prevented by law from reviewing the agency's Medicare program which includes over 522,000 enrollees with claims totaling more than $900.5 million. This paradox results from long-standing restrictions on OIG appropriations dating back to 1997.

In FY 1999, P.L. 105-277 made the restriction on OIG appropriations permanent when the section entitled "Limitation on the Office of Inspector General" stated:

> "… none of the funds made available under this heading in this Act, or subsequent Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Acts, may be used for any audit, investigation, or review of the Medicare Program." [Emphasis added.]

[3] FISMA establishes minimum security requirements for all agency operations and assets. These requirements are listed in NIST Special Publication (SP) 800-53.

As of the end of FY 2007, the OIG has included all of the RRB's general support systems and major applications in their FISMA evaluations, except the administration of Medicare entitlements as proscribed by appropriation law. Since the OIG is prevented from applying appropriation funds for any audit, investigation, or review of the RRB's Medicare program, a scope limitation results from the OIG's inability to perform its FISMA oversight mandates.

Additionally, the OIG has previously cited the RRB with a significant deficiency in periodic testing and evaluations because the RRB has failed to implement a consistent, FISMA compliant process which includes evaluating the effectiveness of information security policies, procedures, and practices. We believe this deficiency extends to the RRB's Medicare program.

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. Additionally, other observed weaknesses in the agency's implementation of requirements for 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.

The details of our assessment of agency progress in complying with FISMA requirements and a summary of the weaknesses identified during our FY 2007 evaluation of information security, including recommendations for corrective action, follow. Agency management has agreed to take the recommended corrective actions for all recommendations except Recommendation 6 for which we have made an alternative recommendation. The full text of management's responses is included in this report as Appendices I and II.

Access Controls

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 its FY 2001 evaluation of information security (and confirmed by technical specialists under contract to the OIG), the OIG cited the agency with a significant deficiency in this area and made several recommendations. Weaknesses included:

- inadequate management of user accounts and passwords,
- the inability to support detailed security evaluations of LAN user accounts and privileges using existing facilities, and
- a process of reviewing and re-authorizing access to some mainframe component applications that was not fully effective.

During FYs 2004 and 2005 the OIG, and technical specialists under contract to the OIG, performed detailed tests of user privileges in the mainframe and end-user computing general support systems. That testing also found that employees had been granted privileges in excess of those required for their job functions. Additional recommendations in the area of access control were made, bringing the total

number of recommendations in this area to 31. As of August 1, 2007, the agency has fully implemented 9 of the recommendations, resulting in 22 that require further corrective action.[4]

Our FY 2007 review of security configuration policies governing all domain servers and desktops showed that some settings still include default privileges to global groups that allow excessive access. We also noted that an individual whose account is currently inactive is also defined within the group policy object. These settings violate the principle of least privilege and good security management practices. Excessive rights and privileges weaken the overall information security program. Previously, we reported that the RRB does not have an agency-wide security configuration policy, and recommended that one be developed.[5] The agency has not yet addressed this recommendation.

Recommendation

1. We recommend that the Bureau of Information Services review the privileges defined in the group policy objects, and remove global groups that allow excessive access and individually defined inactive accounts.

Management's Response

The Bureau of Information Services concurs with the recommendation and will prepare a plan to address the group policy, remove global groups, and establish organizational unit groups.

Certification and Accreditation

The OIG cited the RRB with a deficiency in implementing a NIST compliant certification and accreditation program in FY 2003. We found that existing agency procedures for authorizing the processing of information systems were not adequate to meet 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.

---

[4] OIG Report No. 02-04, Recommendation 13, 20, and 21.
Blackbird Technologies, Inc., report dated 07/20/01, Recommendation 5.
Blackbird Technologies, Inc., report dated 08/17/01, Recommendations 5a, 5b, and 5c.
OIG Report No. 04-07, Recommendations 1, and 3.
OIG Report No. 04-08, Recommendation 1.
OIG Report No. 04-09, Recommendations 1, and 3.
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, Recommendations 1 and 6.
DSD WEB Report dated 06/07/05, Recommendations 13 and 16.

[5] OIG Report No. 05-11, Recommendation 1.

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.[6] In May 2004, NIST released Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" which provides guidelines for security certification and accreditation of information systems supporting the executive agencies of the Federal government. 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.[7]

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.[8] 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 FY 2007, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's end-user computing general support system. Certification and accreditation of the RRB's mainframe computing general support system and each of the six major applications are expected to begin following the completion of the end-user computing accreditation. 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.

Recommendation

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

Risk Assessment

The RRB has not implemented an effective risk assessment process including documentation of agency determinations regarding risk. A risk assessment process is a critical component of a NIST compliant certification and accreditation process.

[6] 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.

[7] NIST SP 800-37 functionally replaced Federal Information Processing Standard 102, "Guideline for Computer Security Certification and Accreditation," dated September 1983. That standard stated that "accrediting officials must possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies." Therefore, NIST SP 800-37 continues to prescribe information system accreditation at a level of management consistent with long-standing requirements.

[8] OIG Report No. 03-10, Recommendation 6.
OIG Report No. 04-11, Recommendation 9.

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.

The OIG first reported in FY 2002 that the RRB's risk assessment process was made in connection with management control reviews performed for the Federal Managers' Financial Integrity Act of 1982. At that time, we reported that the reviews may or may not include security-related control objectives and techniques.

In our FY 2005 FISMA report, the OIG cited the agency with a significant deficiency in this area 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 risk assessments of the major application and general support systems in accordance with NIST guidance.[9] While the agency drafted a risk assessment methodology in FY 2006, that document has not yet been approved, adopted, or implemented.

During FY 2007, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's end-user computing general support system, including the completion of a formally documented, NIST compliant, risk assessment. Similar actions for the RRB's mainframe computing general support system and each of the six major applications are expected to begin following the completion of the contract for end-user computing.

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

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. 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

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

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. Additionally, the agency had not consistently performed tests of contractor operations. 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.[10]

In our FY 2005 FISMA report, the OIG cited the agency with a significant deficiency in this area because the agency had made little progress in implementing a compliant periodic testing and evaluation process.

In FY 2006, the Bureau of Information Services 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, and began testing. The common controls address the development of policies and procedures, continuity planning, incident response, physical environment security, and personnel security. In FY 2007, they completed their test. However, they did not incorporate the RRB's regional and field offices in the test. Since each field office location has its own server containing agency information, the results of the common control tests pertaining to physical security are impacted by field office omission.

During FY 2007, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's end-user computing general support system, including the completion of security tests and evaluations. Similar actions for the RRB's mainframe computing general support system and each of the six major applications are expected to begin following the completion of the contract for end-user computing. However, that contract only requires contractor employees "to perform their necessary services at the RRB headquarters facility, located in `Chicago, Illinois." Therefore, it does not appear that those test procedures will include any physical environment tests of the RRB's regional and field offices.

The lack of testing outside of RRB headquarters may result in weaknesses that will go undetected, increasing the RRB's risk that information and information systems are not protected from unauthorized access, use, disclosure, disruption, modification or destruction. As a result, the RRB cannot ensure the confidentiality, integrity, or availability of agency information.

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

Recommendation

2. We recommend that the Bureau of Information Services extend their test and evaluation plans to include agency information and information systems located outside of RRB headquarters, including regional and field offices.

Management's Response

The Bureau of Information Services concurs with the recommendation and will develop guidance for the regional, field, and headquarters office managers on how to perform security assessments to validate whether adequate physical, environmental and information security controls are in place.

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 and privacy programs.

FISMA requires that agencies include risk-based policies and procedures that cost-effectively 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, the OIG conducted several reviews which disclosed the need for additional policies, procedures, and practices to address information security and privacy weaknesses.[11]

Recommendation

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

Training

The RRB has met the FISMA requirement for information security training for employees, but needs improvement in identifying contractors. Our review of security

[11] OIG Report No. 07-02, Recommendations 1, 2, 3, 4, and 5.
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, 4, 5, 6, 7, 8, 9,10, 11, 12, 13, 14, 15, 16, and 17.
OIG Report No. 07-07, Recommendations 2, 3, and 4.

Additionally, our audit of controls to safeguard sensitive personally identifiable information with 22 recommendations is pending management's response to the draft report.

awareness training provided to employees and contractors showed that the methodology used by the Bureau of Information Services to identify contractors for security awareness training is ineffective. As a result of our discussions with agency personnel concerning the methods used by them to identify contractors for training, the number of contractors notated on the agency's training control log doubled during the month of August 2007. Most of these contractors had obtained their system access prior to January 2007. Previously, in our review of the agency's privacy program, we reported a similar weakness regarding unidentified contractors with access to personally identifiable information, and made recommendations to improve that program.[12]

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, Form RRB 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.

The procedure used by the Bureau of Information Services to identify contractors for training only considers those contractors for whom email addresses are known. Additionally, agency personnel did not keep records of any attempts to identify contractors for whom email addresses were unknown. Good sources of contractor information can be found in access control lists, contract files and discussions with the Contracting Officer's Technical Representatives, and through the compiled results of prior reviews.

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 contractors pose additional risks because their corporate culture may not be aligned with agency policy, procedures, and rules of behavior.

Recommendations

3. We recommend that the Office of Administration revise the Contracting Officer's Technical Representative instructional letter to include a requirement for all new contractor employees to receive the security awareness training pamphlet, Form RRB G-15, and to obtain the written acknowledgement from them via Form G-15a.

4. We recommend that the Bureau of Information Services compile and maintain comprehensive listings of all contractors for future annual refresher training by

[12] OIG Report No. 07-06, Recommendations 11, 12, and 14.

implementing a procedure to use all available sources of identification, including access control lists and contract files.

Management's Responses

The Office of Administration concurs with the recommendation and will revise the Contracting Officer's Technical Representative instructional letter.

The Bureau of Information Services concurs with the recommendation and will develop procedures to maintain a comprehensive listing of all contractors in time for the next annual cycle of awareness training.

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.

In FY 2007, the agency contracted with technical specialists to assist in the certification and accreditation of the RRB's end-user computing general support system, including the completion of an updated security plan. Similar actions for the RRB's mainframe computing general support system and each of the six major applications are expected to begin following the completion of the end-user computing contract.

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. We recommended that the RRB review and revise the POAM to include items that were missing. The RRB rejected the recommendation stating the POAM was for internal agency purposes and did not require revision to track remedial actions.[13]

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

In FY 2005, we again reported that the existing POAM was not comprehensive with respect to identifying weaknesses. We also reported that it 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. We recommended that the RRB review and revise its remedial action process to ensure that **all** security weaknesses are included and to ensure that the POAM demonstrated the prioritization of agency remediation efforts.[14] The RRB responded that they found the POAM "to be a cumbersome document to maintain and update" but agreed to modify it "to reflect outstanding security recommendations … with sufficient summarized detail to permit oversight and tracking of agency remediation progress."

In FY 2007, we reported that the agency was not preparing action plans for their privacy-related weaknesses, and as a result those weaknesses were not being incorporated into the existing POAM. We recommended that the agency develop appropriate action plans and update the POAM for all privacy-related weaknesses.[15] The RRB has only agreed to include **significant** privacy-related weaknesses.

Our current assessment of the existing POAM shows that the agency continues to omit many known weaknesses identified either through OIG reviews or through agency reviews. As a result, agency efforts to date have been insufficient in correcting POAM deficiencies.

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.[16]

[14] OIG Report No. 05-11, Recommendation 3.
[15] OIG Report No. 07-06, Recommendation 15.
[16] OIG Report No. 06-09, Recommendations 1, 2, 3, 4, 7, 8, 9, and 10.

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 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, but the plan does not provide reasonable assurance that the agency will be able to recover from a disaster and perform its critical business functions in a timely manner. Additionally, procedures do not ensure the protection of sensitive information.

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. However, the RRB has never tested the Continuity of Operations Plan which ensures business continuity. In FY 2006, the OIG recommended such testing, as well as other continuity of operations procedures and practices.[17] Additionally, we had previously recommended that the agency update its overall disaster recovery plan, which is still pending.[18]

In FY 2007, the RRB performed a desk examination of the Continuity of Operations Plan. This consisted mainly of having team members read a training document, update the team rosters, and verify that the plan procedures are correct.

At the time of our FISMA evaluation, the RRB had also performed one of the two scheduled off-site recovery tests. Our review of the test's results show that the RRB did not adequately dispose of all data packs containing sensitive information. We were told that the time allotted for off-site testing had lapsed, so the Bureau of Information Services personnel left the test site without clearing the data packs. Instead, they left the removal of sensitive information to the off-site disaster recovery vendor. As a result, the RRB lost control of their sensitive information and cannot determine whether the data was inappropriately accessed or compromised by an off-site vendor employee.

We also reviewed the results of all off-site test results since FY 2001, and noted that one of the RRB's major applications (Financial Interchange) has never been tested

[17] OIG Report No. 06-08, Recommendations 2, 4, 5, and 6.
[18] OIG Report No. 02-04, Recommendation 6.

off-site, and another RRB major application (Financial Management) has not been tested off-site since FY 2002. As a result, the RRB cannot ensure that the procedures for recovering these two major applications are operable or effective.

Recommendations

We recommend that the Bureau of Information Services:

5. Schedule enough time following off-site testing to ensure all data packs containing sensitive information are cleared before leaving the test site. In the unfortunate chance that test time may lapse, a responsible Bureau employee should stay to observe the clearing of the disk packs to ensure no compromise of sensitive information occurs.

6. Schedule the major application systems for off-site testing to ensure that all major applications are tested on a rotational basis in a reasonable amount of time.

Management's Responses

The Bureau of Information Services concurs with Recommendation 5 and will set aside a specific amount of time to scrub the data from the disk packs at the next disaster recovery test. They have also obtained permission to stay past the contracted time, if necessary, to accomplish this task. Additionally, the Bureau of Information Services will pursue a more permanent solution and update their procedures accordingly.

For Recommendation 6, the Bureau of Information Services agrees, in theory, that it is appropriate for all major application systems to be involved in recovery off-site testing, but that they cannot force system owner participation in such exercises. The Bureau of Information Services has agreed, however, to develop a procedure to document solicitations to participate in off-site testing, and document system owner responses.

OIG's Comments on Management's Response

The Bureau of Information Services has indicated that they cannot agree to Recommendation 6 because they "cannot force participation in such exercises by systems owners." Disaster recovery testing is a critical part of any information security program. Accordingly, we believe that the Chief Information Officer should seek the required authority from the agency's three-member Board. If such authority is not forthcoming, we offer the alternative recommendation that the Chief Information Officer develop a procedure to advise the agency's Executive Committee and/or three-member Board of the history and status of disaster recovery testing for the various major application systems.

A continued inability to obtain a change of behavior among system owners will be considered a significant deficiency in future FISMA evaluations. The

recommendation will remain in the OIG's audit follow-up system until the Chief Information Officer has pursued this matter as described above.

Inventory of Systems

The agency has not yet completed compilation of a reliable inventory of systems. In FY 2005, we reported that the RRB did not have a reliable inventory that identified component applications operating in the end-user computing general support system, the related server locations, or the identification of security administrators. Accordingly, we made recommendations to address these issues; implementation of which is currently pending.[19]

FISMA requires that each agency develop, maintain, and annually update their inventory of major information systems operated by, or under the control of, the agency. 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 connection with our review of the agency's security configurations, we noted the RRB maintains a separate, special purpose, inventory of servers located in RRB headquarters. This inventory includes data that is not present in the agency's official fixed asset inventory system, including operating system, physical location within the data center, server function, and server status such as "to be de-commissioned" or "not used". A comparison of the two inventories and a physical review of individual servers revealed several discrepancies in server serial identification numbers, and eight servers that were missing from the agency's official fixed asset inventory system. Additionally, our review of physical servers revealed additional errors in the special purpose inventory, including incorrect operating system and server status.

Complete, accurate, and reliable inventories of information systems, including applications and hardware, strengthen the information security program by facilitating best practices over physical security controls.

Recommendations

We recommend that the Bureau of Information Services:

7. Perform a physical inventory of information technology hardware, and update the agency's official fixed asset inventory system.

8. Research the possibility of using the agency's official fixed asset inventory system to track the additional data the Bureau requires, and considers migrating to that inventory system if those requirements can be met.

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

Management's Responses

The Bureau of Information Services concurs with Recommendations 7 and 8 and will perform a physical inventory for headquarters equipment by September 30, 2007, and for field office equipment after the deployment of newly purchased equipment. They will also create procedures for improving control over data collection and entry into the agency's fixed asset system. Additionally, the Bureau of Information Services will use the agency's official fixed asset inventory system to track the additional data they require.

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

UNITED STATES GOVERNMENT

MEMORANDUM

September 24, 2007

TO : Letty Jay
Supervisory Auditor

FROM : Terri S. Morgan
Chief Information Officer Terri S. Morgan

SUBJECT : Draft Report – Fiscal Year 2007 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 – We recommend that the Bureau of Information Services review the privileges defined in the group policy objects, and remove global groups that allow excessive access and individually defined inactive accounts.

BIS Response – We are in the process of setting up a plan to address group policy and to remove global groups and set up organizational groups (OU)'s which will grant individuals only the access that they need to perform their job functions. We will have the plan to accomplish this prepared by December 31, 2007.

Recommendation 2 – We recommend that the Bureau of Information Services extend their test and evaluation plans to include agency information and information systems located outside of RRB headquarters, including Regional and Field offices.

BIS Response – RMG's network surveillance capabilities already include the ability to logically examine and test all remote and local agency systems. RMG will develop a new policy chapter in the Information Security Handbook that will provide guidance for the Regional, Field and HQ office managers on how to perform security assessments to validate that their office site has adequate physical, environmental and information security controls in place to protect the confidentiality, integrity and availability of RRB data by June 2008.

Recommendation 4 – We recommend that the Bureau of Information Services compile and maintain comprehensive listings of all contractors for future annual refresher training by implementing a procedure to use all available sources of identification, including access control lists and contract files

BIS Response – RMG has made continuous improvement in the annual awareness training program by refreshing the subject content and streamlining the management process. While the agency has achieved excellent compliance performance from employees, contractor participation can be improved. This year RMG has made progress in identifying all agency contractors and will develop procedures to maintain a

comprehensive listing of all contractors in time for the next annual cycle of awareness training in March 2008.

Recommendation 5 – We recommend that the Bureau of Information Services schedule enough time following off-site testing to ensure all data packs containing sensitive information are cleared before leaving the test site. In the unfortunate chance that test time may lapse, a responsible Bureau employee should stay to observe the clearing of the disk packs to ensure no compromise of sensitive information occurs.

BIS Response – Bureau of Information Services is responsible for the agency's data used in the Disaster Recovery Exercise at the IT Recovery site. We agree that a procedure must be in place to ensure that agency PII data is scrubbed from off-site disks used in disaster recovery exercises. We are currently in the process of evaluating ways to accomplish scrubbing of data from the packs when out at the disaster recovery site. At this time we are allowing a 7 hour window for this DR test to scrub the packs before we leave. We have the permission from SunGard to stay past our contracted time, if necessary, to accomplish this task. However a more permanent solution is needed for future tests and we are working to resolve this issue, put a plan in place and update our DR procedures. We will have a plan completed by February 1, 2008.

Recommendation 6 – We recommend that the Bureau of Information Services schedule the major application systems for off-site testing to ensure that all major applications are tested on a rotational basis in a reasonable amount of time.

BIS Response – It is appropriate that all major application systems have an opportunity to be involved in a recovery off-site test. RMG is acquiring an additional staff member who will work with the bureau and office areas to improve and test the RRB's business continuity plans and processes and ensure that the contingency plans for major applications are proper. That individual has been hired and is expected to join the agency in January 2008. Although the Bureau of Information Services cannot force participation in such exercises by system owners, a procedure will be developed to document solicitations to participate in the 2008 semi-annual off-site disaster tests and provide a record of responses.

Recommendation 7 – We recommend that the Bureau of Information Services perform a physical inventory of information technology hardware, and update the agency's official fixed asset inventory system.

BIS Response – The Bureau of Information Services conducts an annual physical inventory of information technology hardware that is recorded in the agency's WiseTrack asset management system. This year's physical inventory is scheduled to be completed by the end of the current fiscal year, Sept. 30, 2007. The inventory will be completed for HQ equipment only because the field inventory is being deferred until after the new equipment is deployed. A WiseTrack Task Force was formed to create procedures for improving control over data collection and entry into WiseTrack. These procedures and the final report should be available in October 2007.

Recommendation 8 – We recommend that the Bureau of Information Services research the possibility of using the agency's official fixed asset inventory system to track the

additional data the Bureau requires, and considers migrating to that inventory system if those requirements can be met.

BIS Response – The System & Network Services Group will work with the Administrative Services Group to use the agency's official fixed asset inventory system to track the additional data that the Bureau of Information Services requires. A list of additional requirements will be provided for inclusion in the inventory system by December 2008.

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

UNITED STATES GOVERNMENT

MEMORANDUM

September 17, 2007

TO: Letty Benjamin Jay
Supervisory Auditor

FROM: Henry M. Valiulis
Director of Administration

SUBJECT: Draft Report – Fiscal Year 2007 Evaluation of Information Security at the Railroad Retirement Board

We have reviewed the draft audit dated September 13, 2007 and our comment on recommendation # 3 directed to the Office of Administration is as follows:

Recommendation

We recommend that the Office of Administration revise the Contracting Officer's Technical Representative instructional letter to include a requirement for all new contractor employees to receive the security awareness training pamphlet, Form RRB G-15, and to obtain the written acknowledgement from them via Form G-15a.

Response

The Office of Administration will revise the instructional letter to comply the recommendation. This will be done with the next instructional letter to be released.

Thank you for the opportunity to review the draft report and provide comment.

cc: Chief Information Officer
Supervisory Contract Specialist