OFFICE OF INSPECTOR GENERAL

Audit Report

Fiscal Year 2009 Evaluation of Information Security at the Railroad Retirement Board

Report No. 10-01
November 12, 2009

RAILROAD RETIREMENT BOARD

TABLE OF CONTENTS

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 $10.1 billion in benefits during fiscal year (FY) 2008. The RRB is headquartered in Chicago, Illinois and has 53 Field Offices across the nation.

Throughout much of FY 2009, the RRB's information system environment consisted 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. In September 2009, the RRB combined four of their six major applications into one major application, benefit and payment operations.[1]

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 agency report to the Office of Management and Budget (OMB), and an OMB report to Congress. FISMA also establishes minimum requirements for the management of information security in nine areas:

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

[1] The four major applications combined into benefit and payment operations are RRA benefit payments, RUIA benefit payments, maintenance of railroad employees' service and compensation records, and administration of Medicare entitlement.

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."[2]

The OIG previously evaluated information security at the RRB from FYs 2000 through 2008, and reported weaknesses throughout the RRB's information security program.[3] The OIG also cited the agency with significant deficiencies in access controls in the mainframe and LAN 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.[4]

Objectives

The objectives of this evaluation were to fulfill the requirements of FISMA which include:

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

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

Scope

The scope of this evaluation was information security at the RRB during FY 2009. This included the status of audit recommendations for corrective action which resulted from prior audits and evaluations performed from FY 2000 through FY 2009.

Methodology

To meet the first objective, the OIG audited the general and application controls over the financial management major application system using the methodology contained in the Government Accountability Office's (GAO) *Federal Information System Controls*

---

[2] *Minimum Security Requirements for Federal Information and Information Systems,* NIST Federal Information Processing Standards Publication 200 (March 2006).
[3] OIG audit reports are maintained on the RRB website at http://www.rrb.gov/oig/library.asp.
[4] A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

Audit Manual (FISCAM).[5, 6] We also performed a system-level assessment of security controls over the Medicare major application.[7] Additionally, we considered tests of security controls over access and the segregation of duties in conjunction with OIG audits of the agency's FY 2008 financial statement preparation and the accounts payable subsystem of the financial management major application.[8]

To meet the second objective, we considered the results of prior audits and evaluations of information security from FY 2000 through FY 2009, including the status of related recommendations for corrective action. We also obtained and reviewed documentation supporting the RRB's performance in meeting FISMA requirements and interviewed responsible agency management and staff.

The primary criteria for this evaluation included:

- FISMA,
- NIST standards and guidance,
- OMB Circular A-130,[9]
- OMB memoranda,
- GAO FISCAM, and
- GAO *Standards for Internal Control in the Federal Government*.[10]

We conducted this performance audit 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 2009 through October 2009.

[5] *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6 (January 1999), and revision GAO-09-232G (February 2009).
[6] *Audit of the General and Application Controls in the Financial Management Major Application System*, OIG Report No. 09-05, September 30, 2009.
[7] *Audit of the Railroad Retirement Board's Medicare Major Application System*, OIG Report No. 09-06, September 30, 2009.
[8] *Fiscal Year 2008 Financial Statement Audit Letter to Management*, OIG Report No. 09-02, March 24, 2009, and *Audit of Internal Control Over Accounts Payable*, OIG Report No. 09-03, March 31, 2009.
[9] *Management of Federal Information Resources,* OMB Circular A-130 (November 2000).
[10] *Standards for Internal Control in the Federal Government,* GAO/AIMD-00-21.3.1 (November 1999).

RESULTS OF EVALUATION

The RRB has not yet achieved a fully effective information security program. The RRB has implemented all nine program elements required by FISMA; but the security program, as a whole, is undermined by significant deficiencies in access control and the internal control over the certification and accreditation review process. Additionally, some previously identified lesser deficiencies in the implemented FISMA elements continue to exist.

During FY 2009, the agency has taken action to correct previously reported significant deficiencies in risk assessments and periodic testing and evaluation, and completed their first NIST compliant certification and accreditation program. However, an ineffective review process for contractor deliverables has resulted in a significant deficiency in internal control over the certification and accreditation process.

During FY 2009, we also observed that although the agency has corrected the significant deficiencies in risk assessments and periodic testing and evaluation, some weaknesses in those areas continue to exist. Additionally, we observed other areas where security program improvements should be made, such as the implementation of the RRB's agency-wide configuration policy.

The details of our findings and recommendations for corrective action follow. Agency management has agreed to take corrective actions for all recommendations. The full text of management's response is included in this report as Appendix II.

Certification and Accreditation

The RRB's certification and accreditation process is ineffective and represents a significant deficiency in the RRB's internal control structure.

OMB Circular A-130, Appendix III requires that agency management authorize systems for processing based on the formal technical evaluation of the management, operation, and technical controls. This process is also known as certification and accreditation, and it should occur at least every three years or when there has been a significant change to the system. Additionally, continuous monitoring should be performed on a regular basis. This includes the assessment of a subset of security controls, and the reporting and documentation of the results of the assessment.

GAO has defined internal control as "the plans, methods, and procedures used to meet missions, goals, and objectives and, in doing so, supports performance-based management. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. In short, internal control, which is synonymous with management control, helps government program managers achieve desired results through effective stewardship of public resources."[11]

[11] *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (November 1999).

The OIG previously reported that the RRB did not have a NIST compliant certification and accreditation program.[12] The agency later contracted with technical specialists to assist in the certification and accreditation of the two general support systems and six major applications.

In our FY 2008 FISMA report, we identified a weakness in BIS's process for reviewing contractor deliverables received for the completed LAN/PC general support system and recommended that BIS review and update the certification and accreditation documentation.[13] The RRB has not been effective in correcting this weakness.

In FY 2009, the RRB's contractor completed certification and accreditation of the remaining two major applications, consolidated the documentation for four major applications into one, and conducted continuous monitoring of the agency's LAN/PC, mainframe, and the newly consolidated benefit and payment operations major application. We reviewed the certification and accreditation documentation completed during FYs 2008 and 2009, as well as the continuous monitoring documentation, and observed that these documents contained many of the same deficiencies as previously reported.

Our evaluation of the certification and accreditation and continuous monitoring documentation disclosed that the RRB's review process for contractor deliverables is ineffective in:

- identifying incomplete and inaccurate information in the description of system environment and interconnections;
- ensuring that all of the baseline controls have been considered during testing;
- ensuring that all identified weaknesses have been incorporated in the Plan of Action and Milestones (POAM) for remedial action; and
- identifying when a designated system owner employee is no longer employed at the RRB.

We found that the RRB's policy for the certification and accreditation of agency systems does not include consideration of contractor support and the necessary controls that must be in place to ensure adequate contractor deliverables. The RRB's certification and accreditation process does not provide senior agency officials with complete, accurate, and trustworthy information on the security status of the general support systems. Therefore, the senior agency officials have not been provided an adequate factual basis for rendering their security accreditation decisions.

[12] OIG Report No. 04-11, September 30, 2004, Recommendation 9.
[13] OIG Report No. 08-05, September 30, 2008, Recommendations 2 and 7. At the time of our review, only the LAN/PC general support system had been certified and accredited.

Recommendation

We recommend that the Bureau of Information Services:

1. implement controls to ensure an effective certification and accreditation review process that includes complete, accurate, and trustworthy documentation, whether prepared by agency employees or contractor personnel.

Management's Response

The Bureau of Information Services has agreed with this recommendation and has advised that they initiated a rigorous review of the FY 2009 mainframe and LAN/PC documentation to resolve any inaccurate or missing information.

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.

OMB Circular A-130, Appendix III, defines least privilege as 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, we cited the agency with a significant deficiency in access control and made several recommendations. Since that time, additional recommendations have been made.[14] Although the agency has implemented corrective action for many of the recommendations made since FY 2001, our ongoing evaluations show that the agency continues to have difficulty in this area.

Our FY 2009 assessments of information security in the financial management and Medicare major applications disclosed weaknesses in access control including:

- user privileges that were not commensurate with job functions;
- inadequate segregation of duties over transaction level entries and approvals;
- user account expirations; and
- password configuration settings.

Excessive rights and privileges weaken the overall information security program.

[14] OIG Report No. 02-04, February 5, 2002, Recommendations 13, 20, and 21.
OIG Report No. 04-08, September 7, 2004, Recommendation 1.
DSD LAN Report, June 7, 2005, Recommendation 7.
DSD WEB Report, June 7, 2005, Recommendation 16.
OIG Report No. 05-08, July 18, 2005, Recommendation 10.
OIG Report No. 07-08, September 27, 2007, Recommendation 1.
OIG Report No. 09-02, March 24, 2009, Recommendations 6, 7, and 8.
OIG Report No. 09-03, March 31, 2009, Recommendations 1 and 2.
OIG Report No. 09-05, September 30, 2009, Recommendations 1, 2, 3, 4, 6, 7, 8, 11, 12, 13, 14, 15, 19, and 20.
OIG Report No. 09-06, September 30, 2009, Recommendations 3, 4, 5, and 6.

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's contractor has prepared risk assessments as required by FISMA; however, more work is needed to ensure all risk assessments are completed in accordance with NIST guidance.

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. 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.

In FY 2005, we cited the RRB with a significant deficiency because the agency had made little progress in implementing a formal risk assessment process in accordance with NIST guidance. We previously recommended that the agency complete formal, NIST compliant, risk assessments of the major application and general support systems.[15] In FY 2008, we reviewed the risk assessment prepared for the LAN/PC general support system and found that although the contractor had completed the risk assessment in accordance with NIST guidance, some weaknesses in the final product existed. We recommended that the LAN/PC general support system's risk assessment be reviewed and updated to accurately reflect the current RRB system environment and control analysis.[16]

Our review of the risk assessments prepared by the RRB's contractor in FY 2008 and 2009 disclosed weaknesses similar to those previously identified in the contractor prepared risk assessment for the LAN/PC general support system. Weaknesses include incomplete and inaccurate information in the description of the system environment, as well as missing or not fully documented baseline controls. We attribute these weaknesses to an ineffective review process for contractor deliverables performed by agency personnel. As a result, the effectiveness of the certification and accreditation process as a whole is undermined.

Recommendation

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

[15] OIG Report No. 05-08, July 18, 2005, Recommendation 4.
[16] OIG Report No. 08-05, September 30, 2008, Recommendation 2.

Policies and Procedures

The RRB has developed information security policies and procedures as required by FISMA, but 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. The policies and procedures should also ensure compliance with minimally acceptable system configuration requirements.

In prior reviews, we identified many areas in which the development of policies and procedures would strengthen the RRB's information security and privacy programs, and made recommendations for overall improvement. Many of these recommendations are pending corrective action. [17]

During FY 2009, the RRB completed the development of an agency-wide configuration policy for Windows 2003 servers. Our review of the implementation of the agency-wide configuration policy showed that the agency has not yet fully implemented the policy for all Windows 2003 servers, and their attempts at implementation have not been efficiently managed or successful.

We were advised that the agency-wide policy settings have been made locally on newly deployed Windows 2003 servers in calendar year 2008, and that BIS did not keep records of which servers had been configured with the policy. As of May 2009, the agency had an inventory of 39 Windows 2003 servers deployed prior to 2008, and 7 Windows 2003 servers deployed in 2008. We reviewed the configuration settings for a Windows 2003 server deployed in 2008, and found that 42% of the settings do not match the agency-wide policy. We also observed that no Organizational Unit Group Policy Object had been created to implement the policy agency-wide.

We were advised that the RRB does not intend to develop an agency-wide configuration policy for Windows 2000 servers because they intend to gradually remove these servers from the production environment.[18] However, the RRB has not developed a formal plan to remove the Windows 2000 servers from the production environment. Such a plan should include timeframes and resources required to complete this phase-out action.

---

[17] OIG Report No. 07-02, March 9, 2007, Recommendations 2, 3, and 4.
OIG Memorandum No. 07-02m, March 9, 2007, Recommendation 1.
OIG Report No. 07-04, March 28, 2007, Recommendations 1 and 2.
OIG Report No. 07-06, July 30, 2007, Recommendations 5, 6, 7, 13, 14, and 16.
OIG Report No. 07-07, July 30, 2007, Recommendations 2 and 4.
OIG Report No. 07-09, September 27, 2007, Recommendations 1, 2, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 15, 17, and 18.
OIG Report No. 09-03, March 31, 2009, Recommendations 7, 12, and 13.
OIG Report No. 09-05, September 30, 2009, Recommendations 9, 10, 16, 17, and 18.
OIG Report No. 09-06, September 30, 2009, Recommendations 7, 8, and 9.

[18] As of May 2009, the agency had an inventory of 73 Windows 2000 servers.

During FY 2009, the RRB implemented the Federal Desktop Core Configuration (FDCC) settings for workstations with Windows XP operating systems. In this process, they documented the deviations necessary to allow the FDCC settings to work properly in the RRB LAN/PC general support system. However, our review of the documented deviations showed that some of the reasons for deviation were outdated, inaccurate, or incomplete. We also observed other, unidentified, deviations between the FDCC policy established by NIST and the FDCC settings implemented by BIS. As a result, the RRB cannot ensure that their implemented FDCC settings are in full compliance with NIST requirements.

Recommendations

We recommend that the Bureau of Information Services:

2. develop and implement a plan to efficiently apply the Windows 2003 agency-wide configuration policy to all Windows 2003 servers.

3. develop a formal plan to remove the Windows 2000 servers from the production environment.

4. review the implemented FDCC settings against the NIST requirements, and document the reason for any deviations.

Management's Response

The Bureau of Information Services has agreed to take equivalent corrective action for recommendation two, and has agreed with recommendations three and four. They will:

- evaluate each Windows 2003 server with respect to the server configuration policy, and make the necessary changes or document those items that are deemed to risky to perform;

- develop a project plan for decommissioning the Windows 2000 servers; and

- provide adequate documentation to explain the reasons for any deviations with FDCC requirements.

Security Plans

The RRB's contractor has prepared system security plans as required by FISMA; 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 type of information.

In FY 2008, we reviewed the LAN/PC system security plan completed by the RRB's contractor in August 2008, and found that the plan was not completed in accordance with NIST guidance. We noted that the system security plan contained inaccurate or missing information, and recommended that the plan be reviewed and updated to address the inaccurate or missing information.[19]

In FY 2009, we reviewed the RRB's remaining system security plans and the updated LAN/PC system security plan. Our review of the system security plans disclosed weaknesses similar to those previously identified in FY 2008. As previously discussed in the certification and accreditation section of this report, no changes had been made to the LAN/PC or mainframe system security plans to address the inaccurate or missing information prepared by the RRB's contractor.

We attribute these weaknesses to an ineffective review process for contractor deliverables performed by agency personnel. As a result, the effectiveness of the certification and accreditation process as a whole is undermined.

Recommendation

We recommend that the Bureau of Information Services:

5. review and update the mainframe system security plan to address the inaccurate or missing information.

Management's Response

The Bureau of Information Services has agreed with this recommendation and has advised that they initiated a rigorous review of the FY 2009 mainframe and LAN/PC documentation to resolve any inaccurate or missing information.

Training

The RRB has met the FISMA requirement for information security awareness training for employees and contractors, although some previously identified weaknesses in the RRB's training programs for information security or privacy are pending corrective action.[20]

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 specialized training to personnel with significant security responsibilities.

[19] OIG Report No. 08-05, September 30, 2008, Recommendation 7.
[20] OIG Report No. 06-09, August 24, 2006, Recommendation 1.
OIG Report No. 07-06, July 30, 2007, Recommendations 3 and 8.
OIG Report No. 07-09, September 27, 2007, Recommendation 12.
OIG Report No. 08-05, September 30, 2008, Recommendation 5.

Our review of the RRB's security awareness training results for FY 2009 showed that the agency was generally compliant with the FISMA provision to provide training to all agency employees and contractors. We found that all employees and contractors took the required general information security awareness training, and that employees with significant security responsibilities took some form of the specialized training assigned by the senior agency information security officer. However, we found that two employees with significant security responsibilities did not take the full extent of specialized training because their immediate supervisor overrode the instructions given by the senior agency information security officer. [21]

Although some form of specialized training took place, which meets the requirements of FISMA, agency management should be aware of the risk associated with management overrides of the internal control environment. Such practices may result in the agency's inability to meet FISMA requirements in the future. As FISMA requirements were met this year, we offer no additional recommendations for corrective action.

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 Agency Information Systems

The RRB has implemented a program for periodic testing and evaluation of agency information systems as required by FISMA; however, more work is needed for a fully 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 testing 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 certification and accreditation process. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, requires the information system owner to select an appropriate subset of controls for periodic assessment, also referred to as the continuous monitoring phase of certification and accreditation. The controls selected should be approved by the authorizing official and the senior agency information security officer.

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.[22]

[21] See Appendix I for details of our testing methodology.
[22] OIG Report No. 02-04, February 5, 2002, Recommendation 3.
OIG Report No. 03-02, December 27, 2002, Recommendations 1, 2, 3, and 4.

In FY 2005, we 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 that 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.[23]

Our review of the certification and accreditation documentation prepared by the agency's contractor in FY 2008 and 2009 disclosed that the risk assessments and POAM had not always been updated to reflect the security test and evaluation results, as required by NIST. We were advised that the specific controls selected for testing during the FY 2009 continuous monitoring were agreed to by the system owners and the contractor prior to testing, but observed the Security Test and Evaluation Plan did not specifically identify which individual controls would be tested, and conflicting information exists in the documentation supporting the test scope and results. Additionally, the contractor reported obtaining current test information through an interview with an employee who had left the RRB's employment prior to the contract award.

We attribute these weaknesses to an ineffective agency review process for contractor prepared test and evaluation documentation. Inadequate testing and evaluation of agency information systems weakens the security program as a whole.

Recommendation

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

Management's Response

RRB management has agreed with our finding, but has offered comments on this area of review. See Appendix II for the full text of management's comments.

Testing and Evaluation of Contractor Information Systems

The RRB has implemented a policy to perform and document information security site assessments, but they have not developed a comprehensive plan to accomplish testing and evaluation of the contractor information systems that contain RRB data.

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 …."

[23] OIG Report No. 07-08, September 27, 2007, Recommendation 2.

In FY 2008, we reported that the RRB did not have a comprehensive plan for testing and evaluation of contractor operations and recommended that BIS develop such a plan.[24] BIS responded that they would seek legal counsel to verify which agency contracts should be considered for certification and accreditation as information systems in compliance with FISMA requirements.

We reviewed the legal opinion prepared by the RRB's General Counsel, and observed that BIS was advised to have the senior agency information security officer review the contracts, obtain input from staff and other key participants, and make the necessary classifications regarding contractor information systems.[25]

When a contractor system is considered an independent information system, a certification and accreditation schedule should be established. If the system is considered a subsystem functioning as part of an overall general support system or major application, no independent certification and accreditation is necessary. However, per NIST requirements, all subsystems classified under an overall general support system or major application must fall under the same management authority. Management control includes budgetary or operational authority for day-to-day operations and maintenance of the information systems.[26]

The RRB has contracted with non-Federal service providers, and other Federal agencies. We have observed that many of the RRB's contractor systems do not fall under RRB management authority for day-to-day operations. For example, the RRB has contracted for web services with a telecommunications contractor and administrative actions such as disabling user accounts must be requested through the contractor's work management system. The RRB does not maintain full administrative control over these web services and the contract specifically states that the RRB request maintenance activities through the contractor's work management system.

In September 2009, we were advised by the senior agency information security officer that no work had been completed in response to the legal opinion, and that he did not intend to report any contractor systems in his FY 2009 FISMA report. Inadequate testing and evaluation of contractor information systems weakens the security program as a whole.

Recommendation

We recommend that the senior agency information security officer:

6. perform the reviews as instructed by the RRB's General Counsel to determine which RRB contractors are independent information systems.

[24] OIG Report No. 08-05, September 30, 2008, Recommendation 3.
[25] *Classification of Contractor Systems Interacting with RRB's Information Systems*, Legal Opinion L-2009-11, June 15, 2009, page 5.
[26] *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST SP 800-37, Chapter 2.3, May 2004.

Management's Response

The Bureau of Information Services has agreed with this recommendation and the senior agency information security officer will review all contractors to determine if they are independent information systems.

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. In FY 2005, we again reported that the existing POAM was not comprehensive with respect to identifying weaknesses, and that it provided inadequate prioritization of agency plans and efforts to correct the weaknesses found. In FY 2007, we 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.[27]

During FY 2009, we reviewed the agency POAMs created and/or updated by the contractor during certification and accreditation or continuous monitoring activities and observed that all of the POAMs did not reflect the full results of the security tests and evaluations. As separate POAMs for each general support system and major application have been prepared by the contractor, the agency took steps to consolidate the contractor POAMs into one agency-wide POAM for those systems.[28] However, our review of the agency-wide POAM showed that the weaknesses have not been prioritized to ensure they would be addressed in a timely manner, milestone tasks and dates have not been developed, and the resources needed for remediation have not been identified. We also observed that system owners were not provided the user privileges to access and update the consolidated agency-wide POAM.

[27] OIG Report No. 05-11, September 28, 2005, Recommendation 3.
OIG Report No. 07-06, July 30, 2007, Recommendation 15.

[28] The agency maintains open audit recommendations from OIG reviews separately from the contractor prepared POAMs. During FY 2009, the agency worked to address many of the most significant open audit recommendations as identified by the OIG, but much work remains to be completed overall. For example, at the time our fieldwork for this FISMA review began in May 2009, the agency had over 100 open audit recommendations dealing with information security and privacy.

As a result, agency efforts to date have been insufficient in managing 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.

Management's Response

RRB management has agreed with our finding, but has offered comments on this area of review. See Appendix II for the full text of management's comments.

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, although some previously identified weaknesses are pending corrective action.

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. *Federal Incident Reporting Guidelines* specify categories of incidents and timeframes in which Federal agencies are to report incidents to US-CERT. US-CERT uses these reports to analyze the information provided by all agencies to identify trends and precursors of attacks. BIS also reports security incidents to agency managers each month in the BIS Monthly Administrative Report to keep them apprised of agency actions.

In FY 2006, the OIG performed a detailed review of the RRB's incident handling and reporting program and found that the 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, including controls to ensure the accuracy and completeness of internal and external security incident reports.[29]

Our review of the RRB's incident handling and reporting performed during FY 2009 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.

[29] OIG Report No. 06-09, August 24, 2006, Recommendations 1, 2, 3, 4, 7, 8, 9, and 10.

Management's Response

RRB management has offered comments on this area of review. However, they quoted a statement that did not appear in the draft report released for comment. The matter cited was resolved during the briefing process. See Appendix II for the full text of management's comments.

Continuity of Operations

The RRB has developed a continuity of operations plan that meets the requirements of FISMA, although some previously identified weaknesses are pending corrective action.[30]

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

The RRB provides for semi-annual off-site recovery testing of the two general support systems, and the mainframe databases of its major application systems. Generally, the RRB 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.

Our review performed in FY 2009 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.

Inventory of Systems

The RRB has generally complied with FISMA requirements to identify major application systems, but some improvement is still needed with respect to component application systems.

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

[30] OIG Report No. 07-08, September 27, 2007, Recommendations 5 and 6.

decentralized.[31] Additionally, we previously recommended that the RRB perform a physical inventory of information technology hardware and to update the agency's official fixed asset inventory system and implement controls to ensure adequate protection of the RRB network.[32] Those recommendations are currently pending corrective action.

Our review performed in FY 2009 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.

[31] OIG Report No. 05-08, July 18, 2005, Recommendation 3.
[32] OIG Report No. 07-08, September 27, 2007, Recommendation 7.
OIG Report No. 08-05, September 30, 2008, Recommendation 8.

Sampling Methodology and Results
Information Security Awareness Training

This appendix presents the methodology and results of our judgmental sampling test of information security awareness training records.

Sample Objective

Our objective was to determine whether employees whom the agency reported to have taken information security awareness training received general awareness training, and employees with significant security responsibilities received specialized training. Additionally, we determined whether RRB managers maintained adequate records of the training taken by their employees.

Sample Universe

We selected our sample from the population of 945 RRB employees reported by the agency as having taken security awareness training in FY 2009.

Sample Review Methodology

We used judgmental sampling to select a sample size of 40 employees, 18 of which required the general awareness training and some form of specialized training, and 22 of which required only the general awareness training. Employees were selected from a wide variety of agency departments, including those located at headquarters and in the field offices. In our judgment, this sample size was sufficient to determine whether the training provided was appropriate to job function, and fully documented.

For each RRB employee in our sample, we obtained and reviewed the employee-completed training certification indicating the extent of training taken. Interviews were held as necessary.

An error was defined as:

- an employee who did not read the basic section of the information security awareness pamphlet;
- an employee with significant security responsibilities who did not read the additional sections of the information security awareness pamphlet; or
- a manager who could not produce the required documentation to support the training taken by their respective employees.

Results of Review

We found that all 40 employees took the required basic security awareness training, as reported by the agency. We also found that the 18 employees with significant security responsibilities took some form of specialized training, although 2 did not take the full scope of specialized training at the direction of their immediate supervisor. We also

found that agency managers maintained adequate documentation to support the training taken by their employees.

Conclusion

The RRB's training records are accurate to support the overall conclusion that the RRB has provided information security awareness training. As some form of specialized training took place for employees with significant security responsibilities, which meets the requirements of FISMA, we offer no recommendations for corrective action for the two employees who did not take the full scope of specialized training.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

November 10, 2009

TO : Letty B. Jay,
Assistant Inspector General for Audit

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

SUBJECT: Draft Report – Fiscal Year 2009 Evaluation of Information Security At the Railroad Retirement Board

The RRB appreciates the opportunity to comment on the Office of Inspector General's (OIG) draft report entitled, "Fiscal Year 2009 Evaluation of Information Security At the Railroad Retirement Board." In this draft report, while the OIG acknowledges that the "RRB has implemented all nine elements required by FISMA" for the management of information security, they still assert at the "RRB has not yet achieved a fully effective information security program" because of "significant deficiencies in access control and the internal control over the certification and accreditation process." The OIG states, "The RRB's contractor has prepared system security plans as required by FISMA; however, more work is needed to ensure all plans are completed in accordance with NIST guidance."

Recommendation #1
We recommend that the Bureau of Information Services implement controls to ensure an effective certification and accreditation process that includes complete, accurate and trustworthy documentation, whether prepared by agency employees or contractor personnel.

Recommendation #5
We recommend that the Bureau of Information Services review and update the mainframe system security plan to address the inaccurate or missing information.

Response
BIS concurs with the recommendation regarding documentation but disagrees with the statements regarding the effectiveness of the process.

The RRB believes that we have fully documented that agency systems are robust and exhibit security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, using cost-effective management, personnel, operational, and technical controls. The NIST prescribed certification and accreditation process was conducted at the RRB and in 2009, the Post-Accreditation phase was initiated. As part of the NIST Risk Management Framework process, we will review and update all System Security Plan documents every year. The LAN and Mainframe general support systems will undergo another certification and accreditation and security control monitoring will be performed on all major applications in FY2010. The certification documentation for all systems will become more complete with each iteration of this process.

The RRB does not dispute that we should have performed more careful documentation reviews. Nevertheless, we maintain that the certification and accreditation process produced

documentation that fairly and adequately described the risk to agency operations and assets and allowed all Designated Accrediting Authorities to make an informed assessment with respect as to whether security controls met security requirements. Nonetheless, the Bureau of Information Services has initiated a rigorous review of the 2009 Mainframe and LAN documentation to resolve any inaccurate or missing information. We will completed this review and provide updated documents before November 25, 2009.

Background for Recommendation #2
In the evaluation paper the OIG notes, "We reviewed the configuration settings for a Windows 2003 server deployed in 2008, and found that 42% of the settings do not match the agency-wide policy." Thus, the OIG recommends that "the Bureau of Information Services develop and implement a plan to efficiently apply the Windows 2003 agency-wide configuration policy to all Windows 2003 servers" and also "develop a formal plan to remove the Windows 2000 servers from the production environment."

Recommendation #2
We recommend that the Bureau of Information Services develop and implement a plan to efficiently apply the Windows 2003 agency-wide configuration policy to all Windows 2003 servers.

Response
BIS disagrees with the recommendation but agrees that certain actions must be taken to evaluate the risks of applying the configuration policy to servers already in production.

When the RRB produced a final Server Configuration Policy in 2009, it was stated that the policy would be implemented on all new servers provisioned from that date forward. Changing configuration settings on servers that are already used in production may have negative ramifications on the server. Making configuration setting changes to such servers may adversely affect performance or even disable the applications on the device.

Each 2003 server will need to be handled discretely to ascertain the impact of making configuration changes. The RRB's plan is to list all 2003 servers, evaluating each server with respect to the 2003 server configuration policy. We will meet with application business owners and discuss the risks to server configuration changes. If it is acceptable, BIS will make changes that are agreed upon and document those items that are deemed too risky to perform. This methodology will be repeated with each Win 2003 server. This project will commence in January 2010 and is anticipated to be completed in December 2010.

Recommendation #3
We recommend that the Bureau of Information Services develop a formal plan to remove the Windows 2000 servers form the production environment.

Response
BIS agrees with this recommendation.

Windows 2000 servers are not significant security risks as long as they are properly maintained and supported. Nevertheless, we do intend to replace Windows 2000 machines as funding and other resources become available.

The plan will commence with a Project Plan Charter for decommissioning Win 2000 servers that will be developed by March 2010. BIS will initiate a kickoff meeting with ADG, Programs, etc. to define the scope of project and create a work-breakdown structure. As funds are allocated, the software and hardware needed will be procured and a schedule will be created that identifies impacted applications and their order of migration. Engineering will create a Windows 2003 or 2008 infrastructure with development, test, and production platforms and install the hardware and software. Applications will be tested and migrated into the new production environment.

Background for Recommendation #4
The OIG agrees that "during FY2009, the RRB implemented the Federal Desktop Core Configuration (FDCC) settings for workstations with Windows XP operating systems. In this process, they documented the deviations necessary to allow the FDCC settings to work properly in the RRB LAN/PC general support system. However, our review of the documented deviations showed that some of the reasons for deviation were outdated, inaccurate, or incomplete. We also observed other, unidentified, deviations between FDCC policy established by NIST and the FDCC settings implemented by BIS. As a result, the RRB cannot ensure that their implemented FDCC settings are in full compliance with NIST requirements."

Recommendation #4
We recommend that the Bureau of Information Services review the implemented FDCC settings against the NIST requirements, and document the reason for any deviations.

Response
BIS agrees with this recommendation; however the RRB maintains that the agency is in full compliance with FDCC requirements. We will improve and provide adequate documentation to explain reasons for any deviations by December 31, 2009.

Background for Recommendation #6
The OIG attests that "The RRB has implemented a policy to perform and document information security site assessments, but they have not developed a comprehensive plan to accomplish testing and evaluation of all the RRB's contractor information systems....For example, the RRB has contracted for web services with a telecommunications contractor, and administrative actions such as disabling user accounts must be requested through the contractor's work management system. The RRB does not maintain full administrative control over these web services, and the contract specifically states that the RRB request maintenance activities through the contractor's work management system."

Recommendation #6
We recommend that the senior agency information security officer perform the reviews as instructed by the RRB's General Counsel to determine which RRB contractors are independent information systems.

Response
BIS agrees with this recommendation. The senior agency information security officer will review all contractors to determine if they are independent information systems. The contractor reviews will be completed by October 2010.

BIS response to comments in the audit report that did not result in recommendations:
Testing and Evaluation Process
The OIG states, "The RRB has implemented a program for periodic testing and evaluation of agency information systems as required by FISMA; however, more work is needed for a fully compliant testing and evaluation process...We attribute these weaknesses to an ineffective agency review process for contractor prepared test and evaluation documentation." The RRB concurs that it has an effective program for periodic testing and evaluation of agency information systems as required by FISMA and that any problems are documentation issues and are not security related.

Plan of Action and Milestones (POAM)
The OIG states, "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." They state, "Our review of the agency-wide POAM showed that the weaknesses have not been prioritized to ensure they would be addressed in a timely manner, milestone tasks and dates have not been developed, and the resources needed for remediation have not been identified." The RRB concurs with this preliminary analysis of the POAM that was under development in the

SharePoint environment. The OIG staff saw a previous developmental version of the POAM that has already been revised and reformatted. The agency-wide POAM continues to be a work in progress on SharePoint.

Incident Handling and Response
The OIG states, "The RRB's incident handling and reporting program is generally effective in ensuring the confidentiality, integrity, and availability of the agency's information and in information technology, but some improvement in reporting is needed....Our review of the RRB's incident handling and reporting performed during FY 2009 showed that the RRB did not consistently report all security incidents each month in the BIS Monthly Administrative Report, including three months in which no security incidents had been reported."

FISMA, OMB Circular A-130 (Appendix III), NIST SP 800-53, NIST SP 800-61, and the Federal Incident Reporting Guidelines define the requirements and guidance for federal agency incident handling and response programs. FISMA and NIST guidance require that federal agencies report security incidents to US-CERT within specified time frames. FISMA and NIST guidance also require federal agencies to determine which incidents must be reported internally, when they must be reported and to whom.

The RRB-CERT submitted all monthly US-CERT Administrative Reports to US-CERT in FY 2009. In accordance with RRB incident handling and response procedures, the RRB-CERT also submitted all monthly RRB-CERT Administrative Reports to the Chief Security Officer and to the Chief Information Officer. BIS is not required to include the RRB-CERT Administrative Report within the BIS Monthly Administrative Report. As the RRB-CERT properly submitted all monthly reports to the appropriate external organizations and internal agency officials, the RRB finds this criticism to be erroneous.

Cc:
Patricia Henaghan
Robert Laberry
Robert Piech