Fiscal Year 2005 Evaluation of Information Security at the Railroad Retirement Board Report No. 05-11, September 28, 2005

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 billion in benefits during fiscal year (FY) 2004.

The RRB's information system environment consists of two general support systems and six major application systems. The two general support systems are the data processing system, which supports all mainframe computing activity; and the end-user computing system, which supports the agency's local and wide area networks. The major application systems correspond to the RRB's critical operational activities: payment of RRA and RUIA benefits, maintenance of compensation and service records, administration of Medicare entitlement, financial management, and the RRB's financial interchange with the Social Security Administration. Each major application system is comprised of one or more component systems.

This evaluation was conducted pursuant to the E-Government Act of 2002 (P.L. 107-347), Title III, the Federal Information Security Management Act of 2002 (FISMA) which requires annual agency program reviews, Inspector General security evaluations, 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 the following nine areas:

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

A significant deficiency is a weakness in an agency's overall information system 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. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers' Financial Integrity Act (FMFIA).

A reportable condition exists when a security or management control weakness does not rise to the level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. A reportable condition under FISMA is not reported as a material weakness under FMFIA.

The OIG previously evaluated information security at the RRB during FYs 2001 through 2004 and reported weaknesses throughout the RRB's information security program. The OIG cited the agency with significant deficiencies in access controls in the data processing and end-user computing environments and in the training provided to staff who have significant security responsibilities.

Objective, Scope and Methodology

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

1. testing of the effectiveness of information security, policies, procedures , and practices of a representative subset of the agency's information systems; and
2. an assessment of compliance with FISMA requirements and related information security policies, procedures, standards and guidelines.

To meet the first requirement, the OIG audited access controls in the RRB's end-user computing general support system. We also retained technical specialists to perform additional security tests and evaluations of the agency's local area network, and internet operations used in two major application systems. To meet the second requirement, we considered the results of prior audits and evaluations of information security during FYs 2000 through 2005, including the status of related recommendations for corrective action. We also obtained and reviewed documentation supporting the RRB's performance in meeting FISMA requirements and interviewed responsible agency management and staff.

The list of current and prior year audits considered by the OIG in performing this evaluation is presented in Appendix I.

The primary criteria for this evaluation were:

- the requirements established by FISMA;
- OMB Circular A-130, "Management of Federal Information Resources," Appendix III, dated November 28, 2000 which established a minimum set of controls to be

included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123; and

- Standards and guidance promulgated by the National Institute for Standards and Technology (NIST).

Our work was performed in accordance with generally accepted government auditing standards as applicable to the objective. Fieldwork was conducted at RRB headquarters during May through August 2005.

RESULTS OF EVALUATION

The RRB is experiencing difficulty in achieving an effective, FISMA compliant security program. The OIG's FY 2005 evaluation identified two new significant deficiencies in the agency's security program due to delays in meeting FISMA requirements for risk assessments and periodic testing and evaluation. In addition, previously cited significant deficiencies in training and access controls persist. These deficiencies are subject to reporting as material weaknesses under the FMFIA.

We have also identified reportable conditions that require agency action to ensure a fully effective, FISMA compliant security program. We observed such weaknesses in the agency's implementation of requirements for risk based policies and procedures, a remedial action process, continuity of operations, and inventory of systems.

The details of our assessment of agency compliance with FISMA requirements and the weaknesses disclosed by our tests of the effectiveness of information security follow. We have also reported on agency performance in implementing OMB and NIST requirements for certification and accreditation of information systems which has been adversely impacted by the above cited weaknesses in the FISMA mandated security program.

Periodic Assessment of Risk

The RRB has made little progress in implementing an effective risk assessment process, a significant deficiency in its information security program. The RRB has not documented critical agency determinations concerning risk which drive a FISMA mandated security program and NIST compliant certification and accreditation process.

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

Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems" and related NIST guidance provide a common framework for categorizing systems according to risk. The framework establishes three levels of potential impact on organizational operations, assets, or individuals should a breach of security occur—high (severe or catastrophic), moderate (serious), and low (limited)—and are used to determine the impact for each of the FISMA-specified security objectives of confidentiality, integrity, and availability. Once determined, security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization.

The RRB has categorized its two general support systems and six major application systems as "high potential impact," which means, according to FIPS 199, that a breach of

security in one of these systems has the potential for a severe or catastrophic adverse effect on organizational operations, organization assets, or individuals. The RRB has not documented the initial determination of "high impact" for its general support and major application systems or the ongoing consideration of risk.

The RRB relies primarily on its Management Control Review process to document the assessment of risk in its information systems. That process, implemented to meet FMFIA requirements, does not address the basic elements of an effective risk management program as described in NIST Special Publication (SP) 800-30, "Risk Management Guide for Information Technology Systems."

In addition, the RRB's "Security Handbook" requires an annual risk assessment for the agency's general support systems and any major application systems categorized as "high risk." Management control reviews cannot meet this internal requirement because they are conducted less than annually.

The OIG has recommended that the agency ensure complete formal risk assessments be prepared in accordance with NIST guidance.[1] Agency management has agreed to "develop and publish a standardized risk assessment format in accordance with NIST guidance to be used in developing formal risk assessments of the components of the major application and general support systems." The agency has established a target date of November 2005 for completion of the guidance; no target date has been established for completion of the risk assessments.

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 Based Policies and Procedures

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

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

[1] OIG Report #05-08, Recommendation #4

During our review we observed that the RRB has not developed an agencywide security configuration policy for their server operating systems or formal policies and procedures for the review of contractor operations. We also noted that the lack of periodic risk assessments undermines agency efforts to maintain current, comprehensive policies and procedures. In addition, weaknesses in the implementation of access controls in the end-user computing general support system suggest that the framework of policies and procedures is not fully effective for that system.

Recommendations

We recommend that the Bureau of Information Services develop:

1. an agencywide security configuration policy for server operating systems; and
2. policy and procedures for the review of contractor operations in accordance with NIST guidance.

Management's Response

Management concurs with the recommendations. In response to recommendation #1, the Bureau of Information Services plans to develop a policy to use standard and secure industry conventions to install and upgrade Microsoft Windows operating systems on RRB servers. In response to recommendation #2, the Bureau of Information Services plans to publish an agency security policy on this subject in the RRB Information Systems Security Policy, Standards and Guidelines Handbook.

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

Testing and Evaluation

The RRB's efforts to implement a consistent, FISMA compliant testing and evaluation process have not been successful. Weaknesses in this process have increased to the extent that it now represents a significant deficiency in the agency's information security program.

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 required inventory of major information systems. NIST special publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems" provides guidance in classifying controls.

Tests performed during FY 2005 were not sufficient to meet FISMA requirements because they did not include all major application systems and were not comprehensive with respect to all three categories of controls: management, operational and technical. In addition, the agency had not performed any tests of contractor operations during the first 10 months of FY 2005.

In drawing our conclusion concerning compliance in this area, we considered tests performed during FY 2005 by agency personnel, the OIG and technical specialists under contract to the OIG. We also considered tests performed as part of the agency's Management Control Review process during FY 2005; however, such tests are performed less than annually, and do not include sufficient coverage of management, operational, and technical controls, as defined by NIST, to meet FISMA requirements.

We also noted that the RRB has not performed a security self-assessment since FY 2003. Security self-assessments can be used to meet the minimum requirement for periodic testing and evaluation.

The OIG has previously recommended management act to ensure that periodic independent evaluations of system security for major applications are performed and to ensure the quality of security self-assessments.[2]

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

Although the RRB provides general security awareness training, it has not completed plans to ensure that personnel with significant security responsibilities have had appropriate training. Accordingly, training remains an area of significant deficiency.

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

The OIG first cited lack of training as a material weakness as a result of its first evaluation of information security conducted in FY 2001 when we observed that:

> Employees with decision-making responsibility for information system security have not had adequate formal training in its theory, principles and practice. As a result, some employees do not have an adequate knowledge base to support the security-related decisions required by their positions.

[2] OIG Report #02-04, Recommendation #3
OIG Report #03-02, Recommendations #1, #2, #3, and #4

At that time, the OIG recommended that management develop and implement a plan to provide security specific training to agency employees who have decision-making responsibilities for information systems and, specifically, to personnel with responsibility for administration of the agency's local and wide area networks.[3] The Bureau of Information Services has advised us that it has identified employees who require security-specific training, developed a role-based security training curriculum and begun the training process.

Recommendation

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

Security Plans

FISMA requires that agencies maintain subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems. The OIG did not identify any significant deficiencies or reportable conditions in this area of program management during FY 2005.

Remedial Action Process

The RRB needs to improve its Plan of Action and Milestones to ensure that its remedial action process is sufficient to meet FISMA and OMB requirements.

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.

The OIG previously recommended that the RRB review and revise its remedial action process because we had concluded that the Plan of Action and Milestones was not an effective tool for identifying vulnerabilities and monitoring agency corrective actions according to criteria established by OMB.[4] Management disagreed with the finding stating that:

> The POA&M was designed by the Office of Management and Budget (OMB) to fulfill their reporting requirements … We have received no feedback from OMB to indicate the reports are insufficient or inadequate.

In our opinion, the RRB's Plan of Action and Milestones is less effective now than when we first cited it as a deficiency in FY 2003. During FY 2005, the RRB's plan was not comprehensive with respect to identified weaknesses and was not driven by internal risk

[3] OIG Report #02-04, Recommendations #1 and #14
[4] OIG Report #03-11, Recommendation #1

assessments and control evaluations. We also observed that the existing plan does not demonstrate prioritization of agency plans and efforts to correct information security weaknesses.

Recommendation

3. We recommend that the RRB review and revise its remedial action process to ensure that all security weaknesses are included in the agencywide Plan of Action and Milestones and ensure that the plan demonstrates the prioritization of agency remediation efforts.

Management's Response

Management concurs in principle with the recommendation. Although management prefers a different approach to governance, the Bureau of Information Services has agreed to modify the agency's Plan of Action and Milestones to reflect outstanding security recommendations and to update it with sufficient summarized detail to permit oversight and tracking of agency remediation progress.

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

Incident Response Reporting

FISMA requires that Federal agencies implement procedures for detecting, reporting, and responding to security incidents. The OIG did not identify any significant deficiencies or reportable conditions in this area of program management during FY 2005.

Continuity of Operations

Agency action has not yet fully addressed prior OIG findings that some aspects of its disaster recovery plan are outdated and incomplete and that disaster recovery tests have not consistently included LAN/WAN applications other than establishing connectivity and general administration.

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.

In FY 2001, the OIG recommended that the RRB complete installation of the mainframe software that will back up LAN server contents; and in FY 2002, that the agency update its overall disaster recovery plan and ensure that all decisions related to the disaster recovery contract be formally documented.[5]

[5] OIG Report #01-01, Recommendation #14
OIG Report #02-04, Recommendation #6
OIG Report #02-12 Recommendation #3

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 needs to improve its process for inventorying information systems.

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

The RRB has not compiled a reliable inventory that identifies component applications operating in the end-user computing general support system, the related server locations or the security administrators. The RRB has defined its major application systems by the functional area of agency operations that they support, for example "Payment of Railroad Retirement Act Benefits." Each major application is comprised of many subordinate component systems of which a complete and accurate inventory does not exist. Each subordinate component system needs to be considered if the agency's overall security program is to be effective.

System inventories are maintained by several different organizational units but their efforts are not coordinated or consistent. In FY 2005, the OIG recommended that the agency take action to improve its systems inventory by compiling an official inventory of individual component systems that comprise the major application systems, identify the servers on which the LAN systems operate, as well as the official responsible for each system.[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.

Implementation of Security

The design and implementation of access controls in the RRB's general support and application systems is not adequate to meet minimum standards established by OMB A-130, Appendix III, which represents a significant deficiency in the agency's information security program.

[6] OIG Report #05-08, Recommendations #1, #2, and #3

The OIG first cited access controls as an area of material weakness in its FY 2001 evaluation of information security. The OIG initially identified weaknesses in the management of user accounts and passwords in the data processing and end-user computing general support systems. We have reported on the inability of existing facilities to support detailed third-party security evaluations of LAN user accounts and privileges. Prior reviews of information security in mainframe-based component systems disclosed that the process of reviewing and re-authorizing access to these systems was not fully effective.

During FY 2005, the OIG performed detailed tests of user privileges in the end-user computing general support system; each of the 45 randomly selected employees in the sample had been granted privileges in excess of those required for their jobs. These privileges ranged from actions that should only be performed by an administrator to the ability to read, write, execute or delete files when a lesser privilege (or no privilege) would have been sufficient.
We have recommended that the agency establish policies for the management of certain high-risk LAN accounts, take action to eliminate systemic weaknesses caused by the use of global groups to grant LAN system access, and perform reviews of system administrator activities.[7]

Recommendation

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

Certification and Accreditation

Existing agency procedures are inadequate to meet OMB requirements for authorizing information systems to process, and accepting the associated risk. The agency has not yet implemented a NIST compliant certification and accreditation program; the OIG has previously found that current procedures are not an adequate substitute. Although the RRB believes it has a satisfactory process in place, existing agency procedures are not adequate because they do not place responsibility at a high enough level of agency management and are not supported by adequate risk assessment and testing processes.

Although system authorization is not a FISMA requirement, OMB asks agencies to report on their certification and accreditation process as part of the FISMA reporting process. For FY 2005, OMB requires agencies to report the number of systems authorized for processing after completing certification and accreditation. OMB also requests that the Inspectors General assess the quality of their agency's certification and accreditation process.

---

[7] OIG Report #02-04, Recommendation #13 and #24
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 #04-07, Recommendation #1, #3, and #4
OIG Report #04-08, Recommendation #1
OIG Report #04-09, Recommendation #1
OIG Report # 04-11, Recommendations #1, #2, and #3
OIG Report # 05-08, Recommendations #6, #10, #11, #13, #14, and #15

OMB's policy for federal information security requires that agency management officials formally authorize their information systems to process information and, thereby, accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan. 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 the security certification and accreditation of information systems supporting the executive agencies of the federal government.

In FY 2004, OMB mandated that agencies use a process consistent with NIST SP 800-37 when authorizing (or re-authorizing) systems after May 2004. NIST SP 800-37 states that the "assessment of risk and the development of system security plans are two important activities in an agency's information security program that directly support security accreditation …" That same year, OMB eliminated separate reporting on risk assessments and security plans; instead, the performance measure for certification and accreditation was revised to include the use of the FIPS 199 to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of a security certification are used to reassess the risks and update the system security plan, thus providing the factual basis for an authorizing official to render a security accreditation decision.

Security accreditation is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

The OIG previously recommended that the RRB implement a formal certification and accreditation process that would place the acceptance of system security risk with a higher level of management.

Although the OIG's recommendation pre-dated OMB's mandate of compliance with NIST SP 800-37, which was still in draft, certification and accreditation was already required by OMB Bulletin A-130, Appendix III. In addition, the NIST SP 800-37 requirement that accreditation be "given by a senior agency official" who "should have the authority to oversee the budget and business operations of the information system" was not new. Federal Information Processing Standard (FIPS) 102, "Guideline for Computer Security Certification and Accreditation," issued in September 1983, stated that "accrediting officials must also possess authority to allocate resources to achieve acceptable security and to remedy security deficiencies."

Agency management rejected the OIG's recommendation when it was first offered in FY 2003 but agreed to implement the recommendation when it was offered again in FY 2004.[8] Earlier in this report, we discussed weaknesses in the RRB's risk assessment and testing processes which we consider significant deficiencies in the agency's security program. Risk assessment and control testing are critical elements of certification and accreditation. Weaknesses in these two areas need to be corrected so that the RRB can implement a NIST compliant certification and accreditation process.

Recommendation

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

[8] OIG Report #03-10, dated September 8, 2003, Recommendation #6
OIG Report #04-11, dated September 30, 2004, Recommendation #9

Related Audit and Evaluations

Our evaluation included consideration of the findings and recommendations of audits, evaluations and assessments of information security conducted in the current and prior years.

FY 2005 Reports

- "U.S. Railroad Retirement Board (RRB), Local Area Network Security Scan, Security Test and Evaluation Report," June 7, 2005, DSD Laboratories
- "U.S. Railroad Retirement Board (RRB) Local Area Network, Security Test and Evaluation Report," June 7, 2005, DSD Laboratories
- "U.S. Railroad Retirement Board (RRB), Railroad Unemployment Insurance Act Network (RUIANET), Security Test and Evaluation Report," June 7, 2005, DSD Laboratories
- "U.S. Railroad Retirement Board (RRB), Employer Reporting System (ERS), Security Test and Evaluation Report," June 7, 2005, DSD Laboratories
- "Review of Access Controls in the End-User Computing General Support System," OIG Report #05-08, July 18, 2005

Prior Year Reports

- "Information Systems Security Assessment Report," Defensive Information Operations Group, National Security Agency, June 28, 2000
- "Review of RRB's Compliance with the Critical Infrastructure Assurance Program," August 9, 2000, OIG Report #00-13
- "Review of Document Imaging Railroad Unemployment Insurance Act Programs," November 17, 2000, OIG Report #01-01
- "Site Security Assessment," Blackbird Technologies, Inc., July 20, 2001
- "Security Controls Analysis," Blackbird Technologies, Inc., August 17, 2001
- "Review of Information Security at the Railroad Retirement Board," February 5, 2002, OIG Report #02-04
- "Review of the Railroad Retirement Board's Controls Over the Access, Disclosure, and Use of Social Security Numbers by Third Parties," August 26, 2002, OIG Report #02-11
- "Fiscal Year 2002 Evaluation of Information Security at the Railroad Retirement Board," August 27, 2002, OIG Report #02-12
- "Evaluation of the Self-Assessment Process for Information System Security," December 27, 2002, OIG Report #03-02
- "Evaluation of RRB E-Government Initiative: RUIA Contribution Internet Reporting and Payment," December 27, 2002, OIG Report #03-03

Appendix I

Related Audit and Evaluations

- "Review of the Railroad Retirement Board's PIN/Password System for On-Line Authentication," September 8, 2003, OIG Report #03-09
- "Review of the Systems Development Life Cycle for End-User Computing," September 8, 2003, OIG Report #03-10
- "Fiscal Year 2003 Evaluation of Information Security at the Railroad Retirement Board," September 15, 2003, OIG Report #03-11
- "Review of Mainframe Access Controls at the Application Level: Federal Financial System," September 07, 2004, OIG Report #04-07
- "Review of Mainframe Access Controls at the Application Level: RRB-Developed Applications Controlled by ACF2 and IDMS," September 07, 2004, OIG Report #04-08
- "Review of Mainframe Access Controls at the Application Level: Program Accounts Receivable System," September 09, 2004, OIG Report #04-09
- "Fiscal Year 2004 Evaluation of Information Security at the Railroad Retirement Board," September 30, 2004, OIG Report #04-11

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)

RAILROAD RETIREMENT BOARD

SEP 27 2005

TO : Henrietta B. Shaw
Assistant Inspector General, Audit

FROM : Terri Morgan
Chief Information Officer

SUBJECT: Draft Report – Fiscal Year 2005 Evaluation of Information Security at the Railroad Retirement Board

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

Recommendation 1

We recommend that BIS develop an agencywide security configuration policy for server operating systems.

BIS Response

We concur with the recommendation. Infrastructure Services (IS) agrees with the recommendation to develop an agency wide security configuration policy for server operating systems. IS will address this, and other related OIG concerns related to the RRB network infrastructure. A policy will be developed to use standard and secure industry conventions to install and upgrade Microsoft Windows operating systems on RRB servers. IS will develop a project plan listing the tasks and deliverables addressing this issue and submit it by October 28, 2005.

Recommendation 2

We recommend that BIS develop policy and procedures for the review of contractor operations in accordance with NIST guidance.

BIS Response

We concur with this recommendation. BIS will publish an agency security policy on this subject congruent with the legislative and regulatory requirements by including an additional chapter on this subject to the RRB Information Systems Security Policy,

Standards and Guidelines Handbook by December 2005. The new security handbook chapter will specify agency policy on the review and reporting requirements for assessments of contractor operations.

Recommendation 3

We recommend that the RRB review and revise its remedial action process to ensure that all security weaknesses are included in the agencywide Plan of Action and Milestones (POA&M) and ensure that the plan demonstrates the prioritization of agency remediation efforts.

BIS Response

We concur in principle with this recommendation. The POA&M template is an OMB defined reporting tool for the documentation of IT security weaknesses and the reporting of remediation efforts, but we have found the POA&M spreadsheet, by its very nature, to be a cumbersome document to maintain and update. As a practical matter, the agency has already initiated the standardized use of the Microsoft Project utility program as a better mechanism for this governance purpose. We prefer the flexibility and ease of using the automated MS Project control process format to efficiently organize, prioritize, document and manage all I.T. projects including development of the detailed tracking tasks and allocation of resources required to successfully complete remediation of outstanding audit recommendations. Nevertheless, the agency POA&M will be modified to reflect outstanding security recommendations by March 2006 and will subsequently be updated with sufficient summarized detail to permit oversight and tracking of agency remediation progress by OMB and OIG on a quarterly basis.

K:\IRMShare\Q_CS\31-A FISMA Reports\FY2005\BIS Response to OIG FISMA evaluation 9-12-05.doc