OFFICE OF INSPECTOR GENERAL

Audit Report

The Railroad Retirement Board's Progress in Implementing Federal Information Security Management Act Requirements

Report No. 10-08
May 19, 2010

RAILROAD RETIREMENT BOARD

TABLE OF CONTENTS

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) evaluation of the Railroad Retirement Board's (RRB) progress in implementing Federal Information Security Management Act (FISMA) requirements.[1]

Background

The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and the Railroad Unemployment Insurance Act. These programs provide income protection during old age and in the event of disability, death, temporary unemployment or sickness. The RRB paid over $10.8 billion in benefits during fiscal year (FY) 2009. The RRB is headquartered in Chicago, Illinois and has 53 Field Offices across the nation.

FISMA requires each agency to develop, document, and implement an agencywide information security program for the information and information systems that support the operations and assets of the agency. Such a program includes:

- periodic assessments of risk;
- risk-based policies and procedures that ensure information security is addressed;
- developing and implementing system security plans;
- security awareness training for personnel, contractors, and other users of the information system;
- periodic testing and evaluation of the effectiveness of the information security policies, procedures, and practices;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents;
- plans and procedures to ensure the continuity of operations; and
- developing and maintaining an information systems inventory.

FISMA also 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. Additionally, OMB requires an annual report of agency activities performed in accordance with the Privacy Act, and an Inspector General assessment of the agency's privacy program and privacy impact assessment process.[2]

Past audits and evaluations by the OIG and contractors hired by the OIG have disclosed weaknesses throughout the RRB's information security program, including significant deficiencies in access controls over both the mainframe and LAN environments; training provided to staff with significant security responsibilities; delays in meeting FISMA requirements for both risk assessments, and periodic testing and

[1] FISMA was enacted as Title III, E-Government Act of 2002, P.L. 107-347.
[2] The Privacy Act of 1974, 5 U.S.C. § 552a.

evaluation; and the internal control over the certification and accreditation process due to an ineffective review process for contractor deliverables.

The RRB has addressed the significant deficiencies for training, risk assessments and periodic testing and evaluation, but the significant deficiencies for access controls and the internal control over the certification and accreditation process continue to exist.

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

Objective

The objective of this evaluation was to determine the progress made by the RRB in implementing the information security program required by FISMA.

Scope

The scope of this evaluation was the RRB's information security program from FY 2000 to FY 2009, and the status of agency actions to correct or mitigate previously reported information security weaknesses as of March 23, 2010. Such status is determined after an OIG review of agency corrective actions, and an OIG decision to close the audit recommendation as implemented.

Methodology

To accomplish our objective we reviewed our prior reports to identify previously reported weaknesses and the corresponding OIG audit follow-up records, including documentation previously submitted through the audit follow-up process. Additionally, we conducted interviews of agency staff, and obtained and reviewed documentation to support significant accomplishments made by the RRB, as necessary. Our work did not include any assessments against new or previously established criteria.

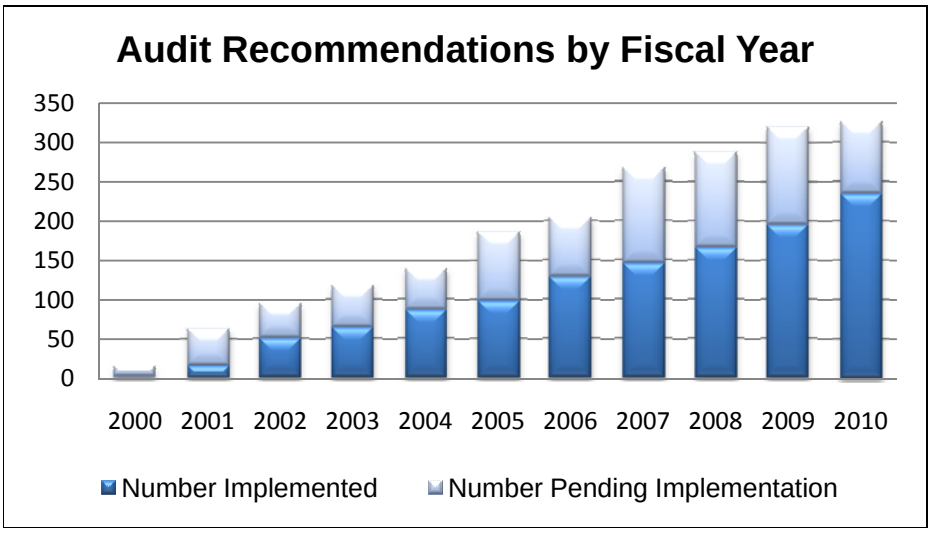
We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. 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 January 2010 through April 2010.

[3] The Federal Managers' Financial Integrity Act of 1982, 31 U.S.C. § 3512.

RESULTS OF EVALUATION

Over the past ten years, the RRB has made significant progress in implementing an information security program that meets the requirements of FISMA. Since FY 2000, they have made steady progress in correcting previously reported deficiencies in their information security and privacy programs. Additionally, the RRB is currently addressing important outstanding audit recommendations that will continue to strengthen the overall security and privacy programs.

Many of the FISMA required elements did not exist or were inconsistently enforced when the OIG first began evaluating the RRB's information security program. Since FY 2000, the OIG has made over 325 audit recommendations for improvement. As of March 23, 2010, the RRB has implemented 234 of these audit recommendations, resulting in every FISMA required element to be addressed. Appendix I lists important outstanding recommendations that require additional action by agency personnel to ensure all FISMA requirements are in place and effectively operating on a consistent basis.



The RRB has made steady progress in implementing audit recommendations.

The details of our findings and conclusions follow. A draft of this report was sent to the RRB and no comments were provided.

Certification and Accreditation

In FY 2009, the RRB completed actions to ensure that every major application and general support system is certified and accredited in accordance with requirements set forth by the National Institute of Standards and Technology (NIST).[4] The RRB is continuing its work to ensure an effective certification and accreditation process.

[4] NIST requirements for certification and accreditation are presented in Special Publication 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems - A Security Life Cycle Approach*, February 2010.

OMB Circular A-130, Appendix III, requires that agency management authorize systems for processing based on a formal technical evaluation of management, operational, and technical controls.[5] This authorization should be performed at least every three years, following an independent review of the security controls. This review of security controls culminates in a NIST compliant certification and accreditation of the information system.

In February 2002, the OIG first reported the need for the RRB to periodically perform independent evaluations of information system security, which leads to an authorization for processing or the certification and accreditation of the information system. In FY 2007, the RRB contracted for independent evaluations and NIST compliant documentation to support a certification and accreditation process. Contractor evaluations occurred between FY 2007 and FY 2009.

In FY 2008, we reported a weakness in the RRB's process for reviewing contractor deliverables, and noted in FY 2009 that the RRB was not effective in correcting that weakness. Due to the ineffective review process for contractor deliverables, we cited the agency with a significant deficiency in the internal control over the certification and accreditation process.

The RRB has started addressing this significant deficiency by conducting a BIS review of the FY 2009 contractor deliverables for the mainframe and LAN/PC information security review to resolve inaccurate or missing information. Specific controls will need to be placed into operation to ensure a consistent and effective certification and accreditation review process of documentation prepared by agency employees or contractor personnel.

Access Controls

The RRB has taken numerous actions to strengthen controls over information system access. They continue to address this significant deficiency.

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. Other interrelated controls such as separation of duties and user authentication, including passwords, are used to assure adequate security for all information processed, transmitted, or stored in Federal information systems.

In FYs 2000 and 2001, contractors hired by the OIG reported that the RRB did not have a formal password policy and noted weaknesses in password management including the lack of password complexity, password history files, and poor password encryption on some information systems.

[5] OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources.*

In February 2002, the OIG reported that passwords were not set to expire for some users and noted that an application displayed an unencrypted administrator password. We also reported numerous other access control deficiencies including poor account management, excessive user rights, and an inadequate user reauthorization process. Due to the nature and extent of these deficiencies, the OIG reported that the RRB's access controls were not effective, and cited the agency with a significant deficiency.

Since that time, the RRB has taken numerous steps to strengthen controls over information system access. For instance, they are developing a formal password policy and are working to enforce that policy across all agency platforms. They have addressed many account management weaknesses by implementing procedures to identify and remove inactive accounts, unnecessary shared or administrative accounts, and accounts of separated employees.

The RRB has also taken significant steps to ensure least privilege in the LAN environment. In February 2002, we reported that the RRB was unable to identify or produce a listing of system users. We later found that many of the LAN applications were designed to give excessive rights (to the extent of "full control") to every user. Actions taken by the agency to remedy this weakness involved full application rewrites and a migration to a newer operating system that allowed the principle of least privilege to be applied. Additionally, the agency implemented a three-server environment that segregated LAN systems for development, test, and production, which alleviated segregation of duties weaknesses for systems development staff. These improvements were a major undertaking for the agency and required several years to implement. In FY 2009, the RRB was able to conduct its first reauthorization review of LAN user access.

Privacy

The RRB has implemented several OMB directives on privacy. They continue to address OMB's privacy-related directives and audit recommendations made by the OIG.

The Privacy Act requires Federal agencies to protect the privacy interests of individuals by placing restrictions on the government's collection, use, and dissemination of personal information. The E-Government Act of 2002 set forth additional privacy protections when agencies collect, maintain, or disseminate personal information using information technology. OMB has issued a number of directives to agencies regarding their responsibilities for safeguarding and protecting this information, and for reporting certain privacy-related actions and reviews performed by the agency.[6]

[6] OMB Circular A-130, Appendix I, *Federal Agency Responsibilities for Maintaining Records About Individuals*;
OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*;
OMB M-06-15, *Safeguarding Personally Identifiable Information*;
OMB M-06-16, *Protection of Sensitive Agency Information*; and
OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*.

In response to OMB directives and OIG audit recommendations, the RRB:

- formed two committees, the information security and privacy committee which aids in privacy policy making, and the agency core response group which is responsible for safeguarding against and responding to breaches of personally identifiable information;
- implemented policies and procedures for general privacy information management;
- implemented policies and procedures for performing privacy impact assessments when personally identifiable information is collected, maintained, or disseminated using information technology;
- conducts privacy impact assessments in accordance with the above procedures;
- issued agency owned laptops with NIST approved encryption to RRB employees who work with personally identifiable information outside of RRB facilities;
- conducts training on privacy-related responsibilities to the above employees;
- issued procedures for the identification of contractors who are exposed to personally identifiable information;
- conducts training on privacy-related responsibilities to the above contractors;
- revised numerous forms, letters, and other correspondence to eliminate the use of social security numbers;
- revised several online information systems to eliminate the display of social security numbers; and
- conducts the necessary reviews of privacy information and records as required by OMB.

The RRB has implemented a privacy program that addresses the Privacy Act requirements, security breaches involving personally identifiable information, and ongoing assessments for the impact of using privacy-related information. They continue to address other outstanding directives and OIG audit recommendations.

Risk Assessment

The RRB has taken action to ensure NIST compliant risk assessments are developed for every major application and general support system, thus removing a significant deficiency. They continue to address audit recommendations for ensuring the risk assessments are complete and accurate.

FISMA requires agencies to develop, document, and implement periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

Early risk assessments prepared by the RRB were designed to provide reasonable assurance that the agency accomplished its mission and protected its assets. These

risk assessments were not designed to consider information security control objectives and techniques. During FY 2003 and FY 2005, the OIG had recommended that the agency implement a formal certification and accreditation process which would include security-based risk assessments, and the completion of formal risk assessments in accordance with NIST guidance, respectively. In September 2005, we reported that the RRB had made little progress in implementing an effective risk assessment process and cited the agency with a significant deficiency due to this delay.

Formal NIST compliant risk assessments were prepared in response to the RRB's FY 2007 contract for the certification and accreditation of their major applications and general support systems. As a result, we removed this significant deficiency. However, our review of the risk assessments prepared by the RRB's contractor showed that the assessments were not complete or accurate with regard to the RRB's operating environment. Therefore, existing OIG audit recommendations pertaining to complete and accurate risk assessments remain open. The RRB continues to address these open audit recommendations.

Policies and Procedures

The RRB continues to take action to implement information security and privacy policies and procedures.

FISMA requires agencies to develop, document, and implement risk-based policies and procedures that ensure that information security is addressed throughout the life cycle of each information system and that ensure compliance with other FISMA requirements, including minimally acceptable system configuration requirements and the security control areas promulgated by NIST.

The RRB has implemented various policies and procedures to strengthen their information security and privacy programs. These policies and procedures encompass multiple areas, including systems development, systems configurations, incident handling and response, access control, continuity of operations, and privacy management. The RRB continues to address other information security and privacy areas that require new or updated policies and procedures.

System Security Plans

The RRB has taken action to ensure NIST compliant system security plans are developed for every major application and general support system. They continue to address audit recommendations for ensuring that the system security plans are complete and accurate.

FISMA requires agencies to develop, document, and implement subordinate plans for providing adequate information security for networks, facilities, and systems or groups

of information systems. These subordinate plans are otherwise referred to as system security plans.

The RRB has historically maintained system security plans for its major applications and general support systems. Occasionally, the OIG has found that the plans require revisions to more accurately reflect the RRB's operating environment.

System security plans were prepared when the RRB contracted for the certification and accreditation of its major applications and general support systems in FY 2007. However, our review of the system security plans prepared by the RRB's contractor showed that the plans were not complete and were inaccurate with regard to the RRB's operating environment. Therefore, existing OIG audit recommendations for complete and accurate system security plans remain open. The RRB continues to address these open audit recommendations.

Training

The RRB has implemented a security awareness training program that meets the requirements of FISMA for employees and contractors. They continue to address open audit recommendations for the specific training needs of some individuals.

FISMA requires agencies to develop, document, and implement a security awareness training program to inform employees, contractors, and other users of the information systems about the risks associated with their activities and their responsibilities in complying with agency policies and procedures designed to reduce those risks.

In February 2002, the OIG cited the agency with a significant deficiency in security training for key personnel with decision-making responsibilities. In FY 2006, we reported that the RRB had implemented a role-based security training curriculum and had provided a substantial portion of the current year's training plan to employees with significant security responsibilities. The agency also continued its existing program for providing general security awareness training to full-time employees and contractors. As a result, we removed the significant deficiency in this area.

Since that time, the RRB has consistently ensured annual training to its employees and contractors; however, improvements can be made for specific training needs of certain individuals. The RRB continues to address these training needs.

Testing and Evaluation

The RRB has taken action to ensure tests and evaluations of management, operational, and technical controls are performed for every major application and general support system, thus removing a significant deficiency. They continue to address audit recommendations for performing tests and evaluations for agency information and

information systems located outside of RRB headquarters, including RRB field offices and contractor operations.

FISMA requires agencies to develop, document, and implement annual testing and evaluation of the effectiveness of the information security policies, procedures, and practices of the agency's management, operational, and technical controls over information systems.

In February 2002, the OIG reported that the RRB was not performing periodic evaluations of system security as required by OMB Circular A-130, Appendix III. During FY 2003 and FY 2004, we recommended that the agency implement a formal certification and accreditation process, which would include tests and evaluations of system security controls. In September 2005, the OIG reported that the RRB had made little progress in implementing a consistent FISMA compliant testing and evaluation process, and cited the agency with a significant deficiency due to this delay.

Formal tests and evaluations of the management, operational, and technical controls of agency major applications and general support systems were prepared in response to the RRB's FY 2007 contract for the certification and accreditation. As a result, we removed this significant deficiency. However, our review of the test and evaluation plans and results showed that the testing did not extend to RRB information systems located outside of RRB headquarters, including RRB field offices and contractor operations. Therefore, additional audit recommendations have been made. The RRB continues to address these open audit recommendations.

Remedial Action Process

The RRB has begun the process of preparing an agency-wide Plan of Actions and Milestones (POAM) to address information security and privacy weaknesses. The RRB continues work to ensure it is effective in identifying all weaknesses and in prioritizing their remediation efforts.

FISMA requires 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. Additionally, OMB requires each agency to develop a formal POAM to identify vulnerabilities in information security and privacy, and to track the progress of corrective action.

Between FY 2003 and FY 2007, the OIG reported that the RRB's POAM was incomplete and insufficiently detailed to be an effective tool for identifying information security and privacy vulnerabilities, and for prioritizing agency plans and efforts to correct the weaknesses found.

Formal POAMs were prepared for RRB major application and general support systems in response to the RRB's FY 2007 contract for certification and accreditation. These

POAMs, coupled with OIG audit follow-up records, represent the RRB's agency-wide POAM as required by FISMA. However, our review of the POAMs prepared for the major application and general support systems showed that they did not reflect the full results of the contractor's testing, nor were they prioritized by the RRB to ensure timely and effective remediation.

The RRB has begun the process of consolidating the POAMs and allowing the means to prioritize the information security and privacy weaknesses. Actions taken to date have not been evaluated by the OIG to determine their overall effectiveness for managing the agency's remediation efforts. The RRB continues its work to ensure an effective remedial action process.

Incident Handling and Reporting

The RRB has taken numerous actions to strengthen controls over incident handling and reporting. They continue to address open audit recommendations in this area.

FISMA requires agencies to develop, document, and implement procedures for detecting, reporting, and responding to security incidents. This includes mitigating risks associated with such incidents before substantial damage is done, notifying and consulting with the Federal Information Security Incident Center (US-CERT), and with law enforcement agencies (OIG-Office of Investigations (OI)), as appropriate.

Audit reports dating back to FY 2000 have disclosed the need for improvement in the RRB's incident handling and reporting processes. Since that time, the RRB has made significant progress in establishing a computer emergency response team (RRB-CERT) that is capable of identifying and handling security incidents in a timely manner. Additionally, the RRB has implemented procedures to ensure timely and accurate reporting of incidents, both internally to agency management and externally to US-CERT and OIG-OI.

The RRB now has a comprehensive program that utilizes an array of prevention and detection tools to protect RRB information and information systems. RRB-CERT works closely with the agency core response group when data breaches occur. The RRB continues to address open audit recommendations and to ensure the effectiveness of this incident response program.

Continuity of Operations

The RRB has implemented a continuity of operations plan that meets the requirements of FISMA. They continue to work on some outstanding audit recommendations.

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

Past audits dating back to FY 2001 have disclosed the need to improve the RRB's continuity of operations by updating the disaster recovery plans to reflect the current operating environment and critical business systems. We also recommended additional testing to ensure that critical business systems are scheduled for off-site testing on a rotational basis, which would provide assurance that all critical systems can be recovered and become operational in a timely manner. Additionally, we recommended that the RRB schedule their off-site tests to ensure sensitive data is cleared from the facility's data packs when testing is complete.

The RRB performs off-site disaster recovery testing twice a year, and has tested all major applications and general support systems over the past few years. They continue to address open audit recommendations for a rotational schedule and for ensuring the data packs are cleared.

Inventory of Systems

The RRB has implemented an inventory of major applications in accordance with FISMA. They continue to address outstanding audit recommendations for the overall improvement of their information systems inventory.

FISMA requires each agency to 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.

In FY 2002, the OIG reported that the RRB was unable to provide the auditors with a current inventory of the agency's LAN hardware and software. At that time, no audit recommendation was made because the RRB was in the process of implementing a new automated system to support fixed asset management. In FY 2005, we reported that the RRB was maintaining several separate inventories of systems and recommended that they develop an official inventory of the component applications that comprise the major application systems. We also recommended that they identify the servers where individual LAN component systems operated, and the security administrators of decentralized component systems.

The RRB has addressed all three of the above audit recommendations and developed a method for maintaining the system inventory in accordance with FISMA requirements. They continue to work to improve the procedures and practices for maintaining their information systems inventory.

Important Outstanding Audit Recommendations

Certification and Accreditation

- Implement controls to ensure an effective certification and accreditation review process. (OIG Report No. 10-01, #1)

Access Controls

- Develop controls to ensure that least privilege is applied to the LAN general support system on an ongoing basis. (OIG Report No. 02-04, #20)
- Develop controls to ensure that workstation connectivity is controlled by a management policy that minimizes risk. Restrict file and folder access and develop controls to maintain the principle of least privilege. (OIG Report No. 02-04 #21; OIG Report No. 08-03 #1)
- Reduce administrator access privileges, if appropriate. (OIG Report No. 08-03, #2)
- Prohibit the FFS system administrator from entering, approving, or modifying transactions. (OIG Report No. 09-02, #7)
- Enforce separation of duties in FFS to prevent employees from approving transactions they have entered. (OIG Report No. 09-02, #8)
- Implement regular reviews of Medicare options cases for accuracy. (OIG Report No. 09-05, #2)
- Restrict the Field Service access profile to only those positions that require all system privileges contained in the profile. (OIG Report No. 09-05, #12)
- Review inactive contractor access accounts, establish contractor system access with an expiration date, and reauthorize annually. (OIG Report No. 09-05, #15 and OIG Report No. 09-06, #4)

Privacy

- Develop test database without personally identifiable information (PII) for use in system development. (DSD Web, #18)
- Update current agreements and plan for encryption of data transmitted for state wage match. (OIG Report No. 07-04, #1and #2)
- Issue agency laptops with encryption software to employees when working at home. (OIG Report No. 07-06, #5)
- Install mainframe tape encryption for tapes transported off-site. (OIG Report No. 07-06, #7)
- Develop comprehensive program to ensure physical security of PII. (OIG Report No. 07-09, #1)
- Ensure all tapes removed from the computer center are properly inventoried. (OIG Report No. 07-09, #9)
- Establish policy and procedures for: compliance with disposal requirements, equipment sanitation procedures prior to disposal, proper sanitization of damaged hard drives, hard drive physical destruction, and reuse of hard drives. (OIG Report No. 07-09, #3, #14, #15, #17, and #18)

Policies and Procedures

- Develop procedures to identify and refer for correction date of birth discrepancies. (OIG Report No. 07-02, #3)
- Develop an electronic history of Medicare premium refunds, of tax withholding transactions, and of FAME transactions. (OIG Report No. 07-02, #4; OIG Report No. 07-07, #4; and OIG Report No. 09-03, #7)
- Develop procedures and controls for emergency programming changes. (OIG Report No. 09-05, #16 and #17)
- Ensure documented password policy conform to Federal Desktop Core Configuration (FDCC) security configuration. (OIG Report No. 09-05, #18)
- Develop plans to implement Windows 2003 configuration policy and remove Windows 2000 servers; implement FDCC settings and document FDCC deviations. (OIG Report No. 10-01, #2, #3, and #4)

Testing and Evaluation

- Conduct penetration testing annually. (DSD LAN, #2)
- Extend test plans to include locations outside of RRB headquarters. (OIG Report No. 07-08, #2)
- Develop a comprehensive plan for testing agency contractor systems. Perform reviews to determine which RRB contractors are independent information systems. (OIG Report No. 08-05, #3 and OIG Report No. 10-01, #6)

Remedial Action Process

- Ensure that all security weaknesses are included in the agency wide POAM and that the plan demonstrates the prioritization of agency remediation efforts. (OIG Report No. 05-11, #3)
- Update all privacy weaknesses to the agency wide POAM. (OIG Report No. 07-06, #15)

Incident Handling and Reporting

- Centrally manage all servers and workstations with virus scanning software signatures. (DSD LAN, #3)

Continuity of Operations

- Ensure data packs used in off-site testing are cleared of PII after testing. (OIG Report No. 07-08, #5)
- Schedule all general support systems and major applications to participate on a rotational basis in the off-site disaster recovery tests. (OIG Report No. 07-08, #6)