U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF AUDITS

Final Audit Report

Subject:

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S Service Credit Redeposit and Deposit System FY 2012

Report No. 4A-CF-00-12-015

Date: August 9, 2012

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

--

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S SERVICE CREDIT REDEPOSIT AND DEPOSIT SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-CF-00-12-015

Date: August 9, 2012

Michael R. Esser
Assistant Inspector General
for Audits

--CAUTION--

This audit report has been distributed to Federal officials who are responsible for the administration of the audited program. This audit report may contain proprietary data which is protected by Federal law (18 U.S.C. 1905). Therefore, while this audit report is available under the Freedom of Information Act and made available to the public on the OIG webpage, caution needs to be exercised before releasing the report to the general public as it may contain proprietary information that was redacted from the publicly distributed copy.

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S SERVICE CREDIT REDEPOSIT AND DEPOSIT SYSTEM
FY 2012

WASHINGTON, D.C.

Report No. 4A-CF-00-12-015

Date: August 9,2012

This final audit report discusses the results of our audit of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Service Credit Redeposit and Deposit System (SCRD). Our conclusions are detailed in the "Results" section of this report.

During this audit, we discovered that OPM had made little progress in implementing many of the recommendations from a prior audit of SCRD. These prior audit recommendations relate to the weak systems development lifecycle controls used by OPM during its effort to correct ongoing issues with prior versions of SCRD. Considering the fact that this system will likely need to be replaced in the near future, we are very concerned that the fundamental issues that plagued the prior service credit systems have not been addressed by OPM.

OPM should immediately dedicate the appropriate resources needed to address our prior audit recommendations so that the agency does not face another system failure, and the repercussions that result from such failure.

In addition to this concern, we noted the following controls in place and opportunities for improvement for SCRD:

Certification and Accreditation Statement (C&A)

A C&A of the SCRD was completed in July 2010. We reviewed the certification package for all required elements of a C&A, and determined that the package contained all necessary documentation.

Federal Information Processing Standards (FIPS) 199 Analysis

The security categorization of the SCRD appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of “moderate.”

Information System Security Plan (ISSP)

The SCRD ISSP contains the critical elements suggested by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18.

Risk Assessment

A risk assessment was conducted for the SCRD in fiscal year (FY) 2010 that addresses all the required elements outlined in relevant NIST guidance.

Independent Security Control Testing

An independent test of security controls was completed for the SCRD as a part of the system’s C&A process in June 2010. However, the results of the test contained many inconsistencies and the test was not completed in accordance with NIST SP 800-37 requirements.

Security Control Self-Assessment

A security controls self-assessment was conducted for SCRD in FY 2011.

Contingency Planning and Contingency Plan Testing

A contingency plan was developed for the SCRD that is in compliance with NIST SP 800-34. However, a contingency plan test was not conducted for SCRD in FY 2011.

Privacy Impact Assessment (PIA)

A PIA was completed for the SCRD in March 2010.

Plan of Action and Milestones (POA&M) Process

The SCRD POA&M follows the format of the OPM POA&M guide, and has been routinely submitted to the Office of the Chief Information Officer for evaluation. However, vulnerabilities found during the security controls self-assessment were not documented and tracked on the SCRD POA&M.

NIST SP 800-53 Evaluation

We evaluated the degree to which subsets of the IT security controls outlined in NIST SP 800-53 were implemented for SCRD. Although the majority of the tested security controls have been successfully implemented, some controls were not fully satisfied. Audit logging policies and procedures have not been created and implemented for SCRD. In addition, numerous vulnerabilities were identified in the results of the OIG vulnerability scan of SCRD.

Contents

Page

Introduction

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we evaluated the information technology (IT) security controls related to the Office of Personnel Management's (OPM) Service Credit Redeposit and Deposit System (SCRD).

Background

SCRD is one of OPM's critical IT systems. As such, FISMA requires that the Office of the Inspector General (OIG) perform an audit of IT security controls of this system, as well as all of the agency's systems on a rotating basis. OPM's Retirement Services (RS) division has ownership and managerial responsibility of the SCRD system. The Benefits Systems Group (BSG) within OPM's Office of the Chief Information Officer (OCIO) is responsible for IT development, support, and maintenance of the system.

Service Credit is a retirement program mandated by law *(CFR Title 5, Part 831, Subpart 831.105)* that provides government employees an opportunity to make payments into the Civil Service Retirement System or Federal Employee Retirement System for periods of service during which they either did not contribute to the Civil Service Retirement and Disability Fund (CSRDF), or for which they received a refund of their retirement contributions. An employee may participate in the Service Credit program to ensure receipt of the maximum retirement benefits to which he or she is entitled. Eligible employees may pay a deposit into the CSRDF to cover any creditable Federal civilian service that was not subject to retirement deductions, or they may make a redeposit to cover any period of Federal service for which a refund of retirement contributions was received.

Until 2006, this process was facilitated by a mainframe-based information system that had been in place for many years. This system handled basic transactions, but was not designed to accommodate the many complexities of the business process, particularly the special retirement rules for various classes of federal employees. In April 2006, a newer, more modern version of the service credit system was released which was designed to allow most types of transactions to be automatically processed on users' desktop computers.

In December 2007, RS (then known as the Center for Retirement and Insurance Services) discovered anomalies in the payment and interest amounts computed by SCRD. It was later discovered that the system was not properly calculating interest in some cases. Attempts to correct the problems were not successful, and the system was eventually taken offline in July 2008. Corrections were made to the system and it was brought back on-line in October of 2008. In August 2009, a new version of the system was distributed to users and programmers attempted to correct data that had been corrupted because of the problems with the previous version. However, users continued to identify problems with both the system and the data. It wasn't until

December 2010 that SCRD Version 4.5, including a proper data correction process, was tested and implemented.

The OIG conducted a review of the system during the development and testing phase of SCRD Version 4.5 (Report No. 4A-CF-00-10-021, issued January 8, 2010). The 2010 report contained eight recommendations, six of which were still open as of May 31, 2012.

Objectives

Our objective was to perform an evaluation of the security controls for SCRD to ensure that RS officials have implemented IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and OPM's OCIO.

OPM's IT security policies require managers of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for SCRD, including:

- Certification and Accreditation Statement;
- FIPS 199 Analysis;
- Information System Security Plan;
- Risk Assessment;
- Independent Security Control Testing;
- Security Control Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment;
- Plan of Action and Milestones Process; and
- NIST Special Publication (SP) 800-53 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of RS officials responsible for SCRD, including IT security controls in place as of April 2012.

We considered the SCRD internal control structure in planning our audit procedures. These procedures were mainly substantive in nature, although we did gain an understanding of management procedures and controls to the extent necessary to achieve our audit objectives.

To accomplish our objective, we interviewed representatives of OPM's RS division and other individuals with SCRD security responsibilities. We reviewed relevant OPM IT policies and procedures, federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of SCRD are located in the "Results" section of this report. Since our audit would not necessarily disclose all significant matters in the internal control structure, we do not express an opinion on the SCRD system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Technology Security Policy Volumes 1 and 2;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- E-Government Act of 2002 (P.L. 107-347), Title III, Federal Information Security Management Act of 2002;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30, Risk Management Guide for Information Technology Systems;
- NIST SP 800-34, Contingency Planning Guide for Information Technology Systems;
- NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems;
- NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems;
- NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories;
- Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to time constraints, we did not verify the reliability of the data generated by the various information systems involved. However, nothing came to our attention during our audit testing utilizing the computer-generated data to cause us to doubt its reliability. We believe that the data was sufficient to achieve the audit objectives. Except as noted above, the audit was conducted in accordance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The audit was performed by the OPM Office of the Inspector General, as established by the Inspector General Act of 1978, as amended. The audit was conducted from November 2011 through April 2012 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether RS management of SCRD is consistent with applicable standards. Nothing came to the OIG's attention during this review to indicate that RS is in violation of relevant laws and regulations.

Results

I. Certification and Accreditation Statement

A security certification and accreditation (C&A) of SCRD was completed in July 2010.

NIST SP 800-37 "Guide for the Security Certification and Accreditation of Federal Information Systems," provides guidance to federal agencies in meeting security accreditation requirements. The SCRD C&A appears to have been conducted in compliance with NIST requirements.

OPM's Senior Agency Information Security Officer (representing the OCIO) reviewed the SCRD C&A package and signed the system's certification package on July 20, 2010. The system owner signed the accreditation statement and authorized the continued operation of the system on July 23, 2010.

II. FIPS 199 Analysis

Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, requires federal agencies to categorize all federal information and information systems in order to provide appropriate levels of information security according to a range of risk levels.

NIST SP 800-60 Volume II, Guide for Mapping Types of Information and Information Systems to Security Categories, provides an overview of the security objectives and impact levels identified in FIPS Publication 199.

The SCRD information system security plan (ISSP) categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. SCRD is categorized with a moderate impact level for confidentiality, moderate for integrity, moderate for availability, and an overall categorization of moderate.

The security categorization of SCRD appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of moderate.

III. Information System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, suggest that these controls be documented in an ISSP for each system, and provides guidance for doing so.

The ISSP for SCRD was created using the template outlined in NIST SP 800-18. The template requires that the following elements be documented within the ISSP:

- System Name and Identifier;
- System Categorization;
- System Owner;

- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;
- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

The SCRD ISSP adequately addresses each of the elements required by NIST.

IV. Risk Assessment

A risk assessment is used as a tool to identify security threats, vulnerabilities, potential impacts, and probability of occurrence. In addition, a risk assessment is used to evaluate the effectiveness of security policies and recommend countermeasures to ensure adequate protection of information technology resources.

NIST SP 800-30, Risk Management Guide for Information Technology Systems, offers a nine step systematic approach to conducting a risk assessment that includes: (1) system characterization; (2) threat identification; (3) vulnerability identification; (4) control analysis; (5) likelihood determination; (6) impact analysis; (7) risk determination; (8) control recommendation; and (9) results documentation.

A risk assessment was conducted for SCRD in 2010 that adequately addresses all of the elements outlined in the NIST guidance.

V. Independent Security Control Testing

An independent security controls test was completed for SCRD in June 2010 as a part of the system's C&A process. The test was conducted by OPM's Human Resources Tools and Technology group, which was operating independently from RS. The test was designed to be a full-scope assessment of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems.

However, we do not believe that SCRD has been subject to an adequate independent security controls assessment. During our review of the test results we identified the following anomalies:

- The description of several controls indicated that the controls were not satisfied or not implemented; however, these items are labeled as "passed."
- Several controls that are only partially implemented are labeled as "passed."

- None of the security weaknesses identified during this test, including those labeled as “failed” are listed on the SCRD Plan of Action and Milestones (POA&M).

NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, requires that a proper security assessment report be part of the final accreditation package. Without an accurate assessment report the certification agent cannot determine if the system controls have been implemented correctly, are operating as intended, and are producing the desired outcome with respect to meeting the system’s security requirements.

Recommendation 1

We recommend that RS complete a full-scope independent security controls assessment of SCRD.

RS Response:

“Retirement Services agrees with the recommendation. We were already contracting an independent tester for the upcoming year's continuous monitoring. RS will ensure a full-scope independent security controls assessment of Service Credit is conducted.”

OIG Reply:

As part of the audit resolution process, we recommend that RS provide Internal Oversight and Compliance (IOC) with evidence supporting the remediation of the recommendation.

VI. Security Control Self-Assessment

FISMA requires that the IT security controls of each major application owned by a federal agency be tested on an annual basis. In the years that an independent security controls test is not conducted on the system, the system’s owner must conduct an internal self-assessment of security controls.

A partial-scope vulnerability assessment was conducted on the SCRD system in April 2011. The assessment included a review of a subset of management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Although this test meets the FISMA requirement of an annual partial-scope security controls assessment, it does not address the required full-scope independent test that is required with each C&A (see Recommendation 1, above).

VII. Contingency Planning and Contingency Plan Testing

NIST SP 800-34, Contingency Planning Guide for IT Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM’s security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The SCRD contingency plan documents the functions, operations, and resources necessary to restore and resume SCRD operations when unexpected events or disasters occur. The SCRD contingency plan closely follows the format suggested by NIST SP 800-34 and contains a majority of the required elements.

Contingency Plan Test

NIST SP 800-34, Contingency Planning Guide for Information Technology, provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A simulated "table top" test of the SCRD contingency plan was conducted in June 2010. The documented results of this test indicate that it was conducted in compliance with NIST 800-34 guidelines. However, no annual contingency plan test was completed for SCRD in FY 2011.

Failure to complete a contingency plan test increases the likelihood that system owners will be unable to recover their systems when unexpected events or disasters occur.

Recommendation 2

We recommend RS conduct a contingency plan test of SCRD in FY 2012.

RS Response:

"Retirement Services concurs with this recommendation. Since the SCRD was just revived in December 2010, there was a management decision to not participate in the May 2011 annual OPM disaster recovery testing. Retirement Services is scheduling and preparing to test SCRD in the Annual Disaster Recovery exercise to be executed later this month."

VIII. Privacy Impact Assessment

FISMA requires agencies to perform a screening of federal information systems to determine if a Privacy Impact Assessment (PIA) is required for that system. OMB Memorandum M-03-22 outlines the necessary components of a PIA. The purpose of the assessment is to evaluate any vulnerabilities of privacy in information systems and to document any privacy issues that have been identified and addressed.

In March of 2010 the system owners of SCRD completed a PIA based on the guidelines contained in OPM's PIA Guide. The PIA was reviewed by OPM's Chief Privacy Officer and Chief Information Officer.

IX. Plan of Action and Milestones Process

A POA&M is a tool used to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for IT security weaknesses. OPM has implemented an agency-wide POA&M process to help track known IT security weaknesses associated with the agency's information systems.

The SCRD POA&M follows OPM's standard template and has been routinely submitted to OCIO for evaluation. However, we determined that the SCRD POA&M did not contain action items for all security weaknesses of the system identified through various security control tests and audits. In 2009, the OIG conducted an audit of the new SCRD system and identified many areas for improvement and provided recommendations accordingly; these recommendations are not listed on the SCRD POA&M.

FISMA requires all agencies to report on their efforts to remediate security weaknesses in information technology systems and programs. Agencies must report their progress through quarterly and annual reports.

Failure to track all identified system security weaknesses on the POA&M increases the risk that these vulnerabilities remain unresolved for a prolonged period, increasing the likelihood that an attacker may exploit the weaknesses.

Recommendation 3

We recommend RS incorporate all vulnerabilities discovered during security controls testing and independent audits into the SCRD POA&M.

RS Response:

"Retirement Services concurs with this recommendation."

X. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems, provides guidance for implementing a variety of security controls for information systems supporting the federal government. As part of this audit, we evaluated 47 of these security controls from the following families:

- Access Control
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identification and Authentication
- Incident Response
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Information Integrity

These controls were evaluated by interviewing individuals with SCRD security responsibility, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, and conducting tests directly on the system.

Although it appears that the majority of NIST SP 800-53 security controls have been successfully implemented for SCRD, several tested controls were not fully satisfied.

a) AU-1 Audit and Accountability Policy and Procedures, AU-2 Auditable Events, AU-6 Audit Review, Analysis and Reporting

SCRD does not currently have audit and accountability policies and procedures in place. In addition, we have not received evidence that audit logs are generated by the system.

The independent security controls assessment conducted in 2010 did not include tests of several audit-related controls. The test report did indicate that the "audit review" control was tested, but failed because audit log review was only done on an "ad hoc" basis.

NIST SP 800-53 Revision 3 requires that an organization develop a formal, documented audit and accountability policy and procedure (control AU-1). In addition the NIST guide requires agencies to determine which transactions conducted by the system should be audited (control AU-2). Finally, the guide requires system owners to review and analyze information system audit records on a routine basis (control AU-6).

Failure to implement audit and accountability policies and procedures increases the risk of fraudulent or inaccurate transactions being processed undetected.

Recommendation 4

We recommend that RS determine what type of events and transactions performed by SCRD should be logged, and document this in a formal audit policy.

RS Response:

'Retirement Services concurs with this recommendation."

Recommendation 5

We recommend that RS modify SCRD to record audit logs in accordance with the audit policy.

RS Response:

"Retirement Services concurs with this recommendation."

Recommendation 6

We recommend that RS develop and implement procedures for routinely reviewing SCRD audit logs.

RS Response:

"Retirement Services concurs with this recommendation."

b) RA-5 Vulnerability Scanning

NIST SP 800-53 requires an organization to: scan for vulnerabilities in the information system and hosted applications; employ vulnerability scanning tools and techniques; analyze vulnerability scan reports and results; remediate legitimate vulnerabilities; and share information obtained from the vulnerability scanning process with the appropriate security personnel.

We received evidence that RS conducts routine vulnerability scanning on the databases and computer servers supporting SCRD. However, the vulnerabilities detected during these scans are not included on the SCRD POA&M. Failure to analyze the vulnerability scans and track confirmed weaknesses on the system's POA&M increases the likelihood that the vulnerabilities will not be fixed in a timely manner and that attackers will exploit these flaws for malicious attacks.

As part of this audit, we conducted vulnerability scans of SCRD's technical environment, including the Windows server and Oracle database supporting the system. These scans evaluated SCRD for security vulnerabilities, missing patches, and appropriate configuration settings. Our scan results identified numerous weaknesses; the details of the scans were provided to RS personnel but will not be included in this report.

Recommendation 7

We recommend RS implement a process to analyze the results of the SCRD vulnerability scans and document confirmed vulnerabilities on the system's POA&M.

RS Response:

******RS comments removed by OIG; comments were relevant to the draft audit report, but not to the final report recommendation******

Recommendation 8

We recommend RS review the results of the vulnerability scan conducted by the OIG and make the appropriate modifications to SCRD.

RS Response:

"Retirement Services will review the results of the vulnerability scans conducted by the OIG as part of this audit."

XI. Follow-up of Prior Recommendations

In April 2006, a new version of SCRD was released to replace the legacy mainframe service credit system. This system was plagued with problems until a stable replacement was finally put in place in December 2010. We conducted an in depth review of this system during the development and testing phase and issued Report No. 4A-CF-00-10-021 in January 2010. The 2010 report contained eight specific recommendations related to separation of duties, system requirements, and data entry errors.

Throughout this period there was intense focus on the system development process by account holders, the media, Congress, and senior OPM management. The agency was embarrassed and OPM's reputation for incompetent management of its IT systems development projects seemed to be confirmed. Account holders were inconvenienced and agency resources were expended to deal with the problems created by the failed system.

The system that was finally put in place was not a properly developed billing and retirement system, but more of a patchwork effort to correct a system with a fundamentally flawed design. It is clear that at some point in the near future, the current system will need to be scrapped and developed from the ground up based on the many complex requirements of the business process.

However, at the beginning of this audit only two of the eight recommendations from our 2010 report had been fully implemented. One of the most significant of the open recommendations relates to properly managing business requirements. During the original review, we found that the primary cause of the system's failure to properly calculate account balances was the lack of a fully developed requirements traceability matrix. Almost three years after the problems were originally highlighted, the business requirements for this system are still not properly documented.

A fully developed requirements traceability matrix is especially important because of the myriad and complex retirement laws that impact processing service credit cases. In addition, when agency management decides that a new system is in order, the business process must be fully documented or there is a high risk of another failed system development project.

Given the damage caused by the previous system failure to the agency and its stakeholders, it is difficult to understand why more progress has not been made in correcting the fundamental issues that caused the original problems. Many of the recommendations require action from OPM program offices outside of RS, primarily BSG as the technical developers and administrators of the system. Furthermore, as mentioned in section IX, above, these recommendations are not listed on the SCRD POA&M, and therefore their current status cannot be tracked by the OCIO's IT Security and Privacy Group.

In order for progress to be made in implementing the 2010 recommendations, each item needs to be tracked on the SCRD POA&M, and specific program offices need to be assigned responsibility for each task/milestone needed to address the overall weakness. Responsibility for coordinating this remediation effort falls with OPM's IOC.

Recommendation 9

We recommend that IOC work with RS and BSG to develop milestones and assign responsibility for specific tasks related to remediating the recommendations issued in OIG Report No. 4A-CF-00-10-021.

RS Response:

[No comments provided.]

Major Contributors to this Report

This audit report was prepared by the U.S. Office of Personnel Management, Office of Inspector General, Information Systems Audits Group. The following individuals participated in the audit and the preparation of this report:

- [redacted], Group Chief
- [redacted], Senior Team Leader
- [redacted], IT Auditor

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Retirement Services

May 2, 2012

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audits Group

FROM: [redacted]
Chief, Quality Assurance
Retirement Services

SUBJECT: Response to Draft Report re: Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Service Credit Redeposit and Deposit System (Report No. 4A-CF-00-12-015)

This memorandum is in response to the Inspector General's draft report re: the Audit of the Information Technology Security Controls of the Service Credit Redeposit and Deposit System (SCRD).

The statements in the beginning portion of the Executive Summary do not fully reflect the functionality and role of the Service Credit System. In order to receive credit for particular periods of service, either service for which no retirement deductions were withheld or was refunded, an active federal employee can submit an application to pay for the service in order to receive full credit at retirement. SCRD calculates the initial deposit and/or redeposit amount and the system then acts as an accounts receivables system, crediting payments and calculating interest. Based on these payments, credit may be given later, when the retirement benefit is calculated using FACES or RATE and RATF. SCRD does not actually compute any retirement benefits, and consequently does not compute incorrect retirement benefits as stated in the summary.

With regards to the recommendations directed to RS in Draft Report No. 4A-CF-00-12-015, our responses are as follows:

- Recommendation #1 – Retirement Services agrees with the recommendation. We were already contracting an independent tester for the upcoming year's continuous monitoring. RS will ensure a full-scope independent security controls assessment of Service Credit is conducted.

- Recommendation #2 – Retirement Services concurs with this recommendation. Since the SCRD was just revived in December 2010, there was a management decision to not participate in the May 2011 annual OPM disaster recovery testing. Retirement Services is scheduling and preparing to test SCRD in the Annual Disaster Recovery exercise to be executed later this month.

- Recommendation #3 – Retirement Services concurs with this recommendation.

- Recommendation #4 – Retirement Services concurs with this recommendation.

- Recommendation #5 – Retirement Services concurs with this recommendation.

- Recommendation #6 – Retirement Services concurs with this recommendation.

- Recommendation #7 - On December 22nd, 2011, RS originally submitted vulnerability scans as evidence to the OIG. It appears there was a problem with OPM's email service and the evidence was never received by the IG. The vulnerability scan evidence was resent on April 17th, 2012 in four separate emails and RS received confirmation of receipt.

- Recommendation #8 – Retirement Services will review the results of the vulnerability scans conducted by the OIG as part of this audit.

Thank you for the opportunity to provide comments on the draft report, especially in regards to Recommendation #7, which may be moot now with the evidence provided previously. If you have any questions, or want to discuss further, please let me know.