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

Final Audit Report

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System

Report Number 4A-RI-00-15-019

July 29, 2015

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System

Report No. 4A-RI-00-15-019 **July 29, 2015**

Why Did We Conduct the Audit?

The Annuitant Health Benefits Open Season System (AHBOSS) is one of the U.S. Office of Personnel Management's (OPM) critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (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.

What Did We Audit?

The OIG has completed a performance audit of AHBOSS to ensure that the system owner, OPM's Retirement Services (RS) program office, has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information Security Controls Audit Manual and OPM's Office of the Chief Information Officer (OCIO).

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of AHBOSS determined that:

- A Security Assessment and Authorization (SA&A) of AHBOSS was completed in September 2013. We reviewed the authorization package for all required elements of an SA&A, and determined that the package contained all necessary documentation.
- The security categorization of AHBOSS is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."
- The AHBOSS System Security Plan contains the critical elements required by NIST SP 800-18 Revision 1.
- A security control assessment plan and report were completed in September 2013 for AHBOSS.
- RS did not perform an annual security controls test in FY 2014.
- A contingency plan was developed for AHBOSS that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.
- A privacy threshold analysis was conducted for AHBOSS that indicated that a Privacy Impact Assessment (PIA) was required. A PIA was conducted in August 2012.
- The AHBOSS Plan of Acton and Milestones (POA&M) follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool. However, we noted several POA&M items that were over 180 days overdue with a status of "delayed" that did not indicate a new scheduled completion date.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for the AHBOSS. We determined that the majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4. However, we did note several areas for improvement.

ABBREVIATIONS

AHBOSS	**Annuitant Health Benefits Open Season System**
FIPS	**Federal Information Processing Standards**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Management Act**
GDIT	**General Dynamics Information Technology**
IG	**Inspector General**
IT	**Information Technology**
ITSP	**Information Technology Security and Privacy Group**
NIST	**National Institute of Standards and Technology**
OCIO	**Office of the Chief Information Officer**
OIG	**Office of the Inspector General**
OMB	**U.S. Office of Management and Budget**
OPM	**U.S. Office of Personnel Management**
PIA	**Privacy Impact Analysis**
POA&M	**Plan of Action and Milestones**
RS	**Retirement Services**
SA&A	**Security Assessment and Authorization**
SAP	**Security Assessment Plan**
SAR	**Security Assessment Report**
SP	**Special Publication**
SSP	**System Security Plan**

TABLE OF CONTENTS

I. BACKGROUND

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 U.S. 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 audited the information technology (IT) security controls related to the U.S. Office of Personnel Management's (OPM) Annuitant Health Benefits Open Season System (AHBOSS).

AHBOSS 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.

AHBOSS has a web-based application component and an interactive voice response component that allows Federal annuitants to make changes or request information about health benefits coverage during open season. AHBOSS is managed and operated by a contractor, General Dynamics Information Technology (GDIT), and is hosted in [redacted] Colorado.

This was our first audit of the security controls surrounding AHBOSS. We discussed the results of our audit with Retirement Services (RS) representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objective was to perform an evaluation of the security controls for AHBOSS to ensure that RS officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require owners 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 AHBOSS, including:

- Security Assessment and Authorization (SA&A);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- System Security Plan (SSP);
- Security Assessment Plan and Report (SAP) and (SAR);
- Security Controls Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment (PIA);
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53 Revision 4 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 AHBOSS, including IT security controls in place as of April 2015.

We considered the AHBOSS 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 program office and GDIT with AHBOSS security responsibilities, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also 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 AHBOSS 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 internal controls of AHBOSS taken as a whole.

The criteria used in conducting this audit include:

- OPM Information Security and Privacy Policy Handbook;
- 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;
- The Federal Information System Controls Audit Manual;
- 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 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- FIPS 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 OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from December 2014 through June 2015 in OPM's Washington, D.C. office. This was our first audit of the security controls surrounding AHBOSS.

Compliance with Laws and Regulations

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

II. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Assessment & Authorization

A Security Assessment and Authorization (SA&A) of AHBOSS was completed in September 2013. OPM's Chief Information Security Officer reviewed the AHBOSS SA&A package and signed the system's authorization letter on September 26, 2013. The system's authorizing official signed the letter and authorized the operational status of the system on September 30, 2013.

AHBOSS is operating with a valid Authorization.

NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, provides guidance to Federal agencies in meeting security accreditation requirements. The AHBOSS SA&A appears to have been conducted in compliance with NIST requirements.

B. FIPS 199 Analysis

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 AHBOSS FIPS Publication 199 Security Categorization analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. AHBOSS 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 AHBOSS appears to be consistent with FIPS Publication 199 and NIST SP 800-60 requirements, and we agree with the categorization of "moderate."

C. System Security Plan

Federal agencies must implement on each information system the security controls outlined in NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information systems and Organizations. NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in a system security plan (SSP) for each system, and provides guidance for doing so.

The SSP for AHBOSS was created using the OCIO's template that utilizes NIST SP 800-18 Revision 1 as guidance. The template requires that the following elements be documented within the SSP:

- 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.

We reviewed the AHBOSS SSP and determined that it adequately addresses each of the elements required by NIST. Nothing came to our attention to indicate that the system security plan of AHBOSS has not been properly documented and approved.

D. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for AHBOSS in September 2013, respectively, as a part of the system's SA&A process. The SAP and SAR were completed by a contractor that was operating independently from RS and GDIT. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

The SAP outlined the assessment approach and testing methodology. The SAR identified seven control and two technical weaknesses. These weaknesses were appropriately added to the AHBOSS Plan of Action and Milestones (POA&M).

Nothing came to our attention to indicate that the security controls of AHBOSS have not been adequately tested by an independent source, or that weaknesses identified have not been properly documented.

E. Security Controls Self-Assessment

OPM requires that the IT security controls of each contractor-operated application be tested on an annual basis. In the years that an independent assessment is not being conducted on a system as part of an SA&A, the system's owner must ensure that annual controls testing is performed by a government employee or an independent third party.

We were told that a security controls assessment was not conducted in 2014. By not performing an annual test of security controls, the system is not in compliance with OPM policy. Failure to perform routine security control testing increases the risk that unknown vulnerabilities exist within the system that can be exploited.

Recommendation 1

We recommend that RS ensure that the AHBOSS security controls are tested on an annual basis in accordance with OPM policy.

RS Response:

"RS concurs and understands the importance of completing an annual assessment. Due to extenuating circumstances, this system assessment wasn't completed in CY 2014. At the conclusion of the federal health benefit open season work, the contract period of performance expired 3/31/2014. This is when we would have begun the assessment, but didn't since we thought the contract had ended. It wasn't until much later we learned that the contract was extended to get through one more health benefit open season. At that time, the action tasks associated with an assessment would have competed with the same resources necessary to do the mission critical health benefit open season technical support. Going forward, this finding will be addressed when ITSP/ISSO's complete an on-site visit scheduled next quarter FY 2015."

OIG Reply:

As part of the audit resolution process, we recommend that RS provide OPM's Internal Oversight and Compliance division with evidence that it has implemented this recommendation. This statement applies to all subsequent recommendations in this audit report that RS agrees to implement.

F. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information 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 AHBOSS contingency plan documents the functions, operations, and resources necessary to restore and resume AHBOSS when unexpected events or disasters occur. The AHBOSS contingency plan adequately follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

NIST SP 800-34 Revision 1 provides guidance for testing contingency plans and documenting the results. Contingency plan testing is a critical element of a viable disaster recovery capability.

A contingency plan test of AHBOSS was conducted in August 2014. The test involved a discussion based exercise of recovering the system at the backup data center and then returning operations to the regular data center. The testing documentation contained adequate analysis and review of the test results.

G. Privacy Impact Assessment

FISMA requires agencies to perform a screening of Federal information systems to determine if a 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 and document any vulnerabilities of privacy in information systems that have been identified.

RS completed an initial privacy screening or Privacy Threshold Analysis of AHBOSS and determined that a PIA was required for this system. A PIA was conducted in August of 2012 based on the guidelines contained in OPM's PIA Guide. The PIA was reviewed and approved by the AHBOSS system owner, OPM's Chief Information Security Office and Chief Privacy Officer.

H. 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.

We evaluated the AHBOSS POA&M and verified that it follows the format of OPM's standard template and has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, for

evaluation. We determined that the weaknesses discovered during the SA&A security assessment were appropriately included in the POA&M.

However, we noted that 7 of the 13 items on the POA&M that were over 180 days overdue with a status of "delayed" did not indicate a new scheduled completion date. OPM POA&M Standard Operating Procedures states that "If the weakness is not addressed by the scheduled completion date, the new scheduled completion date must be addressed in the Milestone Changes column, along with the updated milestones and dates necessary to achieve the new scheduled completion date."

Failure to update system's POA&M with material changes increases the likelihood of weaknesses not being addressed in a timely manner and therefore exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

Recommendation 2

We recommend RS develop a detailed action plan with estimated due dates to remediate all overdue POA&M items.

RS Response:

"RS concurs with this response. The assigned ISSO has updated the AHBOSS Plans of Actions & Milestones (POA&M) items entered in Trusted Agent. See attachment."

OIG Reply:

In response to the draft audit report, RS has provided evidence that the estimated completion dates for POA&M items have been updated; no further action is required.

I. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the Federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for AHBOSS. We tested approximately 35 security controls outlined in NIST SP 800-53 Revision 4 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. We tested one or more controls from each of the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Contingency Planning
- Identity and Authentication
- Incident Response
- Maintenance
- Media Protection

- Physical and Environmental Protection
- Planning
- Personnel Security
- Risk Assessment
- System and Services Acquisition
- System and Communications Protection
- System and Information Integrity

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

We determined that all tested security controls appear to be in compliance with NIST SP 800-53 Revision 4 requirements with the following exceptions:

1. **Control IA-2 – Identification and Authentication (Organizational Users)**

   GDIT has not implemented multi-factor authentication utilizing PIV cards for access to AHBOSS.

   Multi-factor authentication is not currently required to access AHBOSS.

   OMB Memorandum M-11-11 requires the use of multi-factor authentication to access all federal information systems. NIST SP 800-53 Revision 4 provides additional implementation guidance for this control. Failure to use multi-factor authentication increases the risk that user accounts could be compromised, thereby allowing unauthorized individuals access to sensitive and proprietary information.

   Recommendation 3

   We recommend that RS require GDIT to enforce PIV authentication for all required AHBOSS users.

   RS Response:

   "RS partially concurs with this recommendation. POAM FY15-Q2-AHBOSS-1 has been logged into Trusted Agent. This corrective action is to comply with the OPM issued PIV Policy (HSPD-12). Since annuitants, are a user of this system and do not have a PIV card, RS will request a waiver for this identified system user."

   OIG Reply:

   The intent of the recommendation was for RS and GDIT to determine which AHBOSS users are required to use PIV for authentication. Once that determination has been made, RS should require that GDIT enforce PIV authentication for those users in accordance with OMB Memorandum M-11-11.

2. Control PE-3 – Physical Access Control

The physical access controls in the data center containing ABHOSS servers could be improved.

The data center hosting AHBOSS uses electronic card readers to control access to the building and data center. However, the data center did not contain controls that we typically observe at similar facilities, including:

- Multi-factor authentication to enter the computer room (e.g., cipher lock or biometric device in addition to an access card); and
- Technical or physical control to detect or prevent [redacted].

Failure to implement adequate physical access controls increases the risk that unauthorized individuals can gain access to the data center and the sensitive resources and data it contains. NIST SP 800-53 Revision 4 provides guidance for adequately controlling physical access to information systems containing sensitive data (see control PE-3, Physical Access Control).

Recommendation 4

We recommend that RS ensure that the physical access controls at the data center hosting AHBOSS are improved. At a minimum, we expect to see multi-factor authentication at data center entrances and [redacted].

RS Response:

"RS concurs with this response. The scheduled onsite assessment noted earlier will confirm the physical access controls in place."

3. Control SC-28 – Protection of Information at Rest

RS requires GDIT to maintain annuitant health benefit information on its systems for up to two years. The database containing this information is stored behind a firewall in the datacenter. [redacted]

[redacted]

[redacted]

Recommendation 5

We recommend that RS ensure that GDIT [redacted].

RS Response:
"RS concurs with this recommendation. [redacted]"

4. Control RA-5 Vulnerability Scanning

As part of the audit, vulnerability and configuration compliance scanning was conducted on AHBOSS servers. We analyzed the results of the scans, but for security purposes, the detailed results of the scans will not be described in this report. A high level summary of the results is below.

System Patching

The vulnerability scans performed during the audit indicate that critical patches and service packs are not always implemented in a timely manner for the operating platforms supporting AHBOSS.

Vulnerability scans indicated that patches are not implemented in a timely manner.

FISCAM states that "Software should be scanned and updated frequently to guard against known vulnerabilities." NIST SP 800-53 Revision 4 states that the organization must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly.

Failure to promptly install important updates increases the risk that vulnerabilities will not be remediated and sensitive information could be stolen.

Recommendation 6

We recommend that RS require GDIT to implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.

RS Response:
"RS concurs with this recommendation."

5. Control CM-6 Configuration Settings

AHBOSS is configured according to documented operating system and application baselines. GDIT performs a manual compliance audit of configuration settings on all AHBOSS servers each month. We believe that automated compliance scanning using software tools would be a more effective and thorough method of compliance auditing than the manual process currently in place.

NIST SP 800-53 Revision 4 states that an organization must monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Failure to implement thorough configuration compliance auditing increases the risk that insecurely configured servers exist undetected, creating a potential gateway for malicious virus and hacking activity that could lead to data breaches.

Recommendation 7

We recommend that RS ensure that GDIT utilize automated software tools to perform configuration compliance audits of the AHBOSS servers.

RS Response:

"RS concurs with this recommendation. We understand that the tool [redacted] has been installed but the tool has not been setup to run in an automated fashion."

OIG Reply:

The tool is currently used to perform automated vulnerability scans. The intent of the recommendation was for GDIT to utilize the configuration compliance auditing function within the tool to perform routine configuration audits.

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[redacted], Auditor-In-Charge
[redacted], IT Auditor
[redacted], IT Auditor

[redacted], Group Chief

Appendix

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Retirement Services

JUN 11 2015

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM: KENNETH J. ZAWODNY, Jr.
Associate Director

SUBJECT: Inspector General Report No. 4A-RI-00-15-019
Information Technology Security Controls Audit of
Annuitant Health Benefit Open Season System

This memorandum is in response to the Draft Audit Report of the Information Technology Security Controls Audit of U.S. Office of Personnel Management's Annuitant Health Benefits Open Season System (Report No. 4A-RI-00-15-019) issued June 2, 2015.

Retirements Services (RS) has reviewed the draft report for the Annuitant Health Benefit Open Season System (AHBOSS). We concur with many of the recommendations cited and always strive to improve the security controls for our systems. While we do concur with most of the recommendations, RS feel compelled to explain the circumstances for several findings.

Recommendation #1

> *We recommend that RS ensure that the AHBOSS security controls are tested on an annual basis in accordance with OPM policy.*

RS concurs and understands the importance of completing an annual assessment. Due to extenuating circumstances, this system assessment wasn't completed in CY 2014. At the conclusion of the federal health benefit open season work, the contract period of performance expired 3/31/2014. This is when we would have begun the assessment, but didn't since we thought the contract had ended. It wasn't until much later we learned that the contract was extended to get through one more health benefit open season. At that time, the action tasks associated with an assessment would have competed with the same resources necessary to do the mission critical health benefit open season technical support. Going forward, this finding will be addressed when ITSP/ISSO's complete an on-site visit scheduled next quarter FY 2015.

Recommendation #2

We recommend RS develop a detailed action plan with estimated due dates to remediate all overdue POA&M items.

RS concurs with this response. The assigned ISSO has updated the AHBOSS Plans of Actions & Milestones (POA&M) items entered in Trusted Agent. See attachment.

Recommendation #3

We recommend that RS require GDIT to enforce PIV authentication for all required AHBOSS users.

RS partially concurs with this recommendation. POAM FY15-Q2-AHBOSS-1 has been logged into Trusted Agent. This corrective action is to comply with the OPM issued PIV Policy (HSPD-12). Since annuitants, are a user of this system and do not have a PIV card, RS will request a waiver for this identified system user.

Recommendation #4

We recommend that RS ensure that the physical access controls at the data center hosting AHBOSS are improved. At a minimum, we expect to see multi-factor authentication at data center entrances and [redacted].

RS concurs with this response. The scheduled onsite assessment noted earlier will confirm the physical access controls in place.

Recommendation #5

We recommend that RS ensure that GDIT [redacted].

RS concurs with this recommendation. [redacted]

Recommendation # 6

We recommend that RS require GDIT to implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.

RS concurs with this recommendation.

Recommendation #7

We recommend that RS ensure that GDIT utilizes automated software tools to perform configuration compliance audits of the AHBOSS servers.

RS concurs with this recommendation. We understand that the tool [redacted] has been installed but the tool has not been setup to run in an automated fashion.

Retirement Services appreciates the opportunity to provide comment on the draft report. Again, we concur with most of the recommendations listed in the report and look forward to working with OCIO to address the AHBOSS security control vulnerabilities identified in this audit.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone:

Toll Free Number:	(877) 499-7295
Washington Metro Area:	(202) 606-2423

By Mail:

Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100