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 BENEFITS FINANCIAL MANAGEMENT SYSTEM FY 2010

Report No. 4A-CF-00-10-018

Date: September 10, 2010

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S BENEFITS FINANCIAL MANGEMENT SYSTEM FY 2010

WASHINGTON, D.C.

Report No. 4A-CF-00-10-018

Date: September 10, 2010

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION TECHNOLOGY SECURITY CONTROLS OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S BENEFITS FINANCIAL MANAGEMENT SYSTEM FY 2010

WASHINGTON, D.C.

Report No. 4A-CF-00-10-018

Date: September 10, 2010

This final audit report discusses the results of our review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Benefits Financial Management System (BFMS). Our conclusions are detailed in the "Results" section of this report.

BFMS is one of OPM's 43 critical IT systems and is comprised of multiple applications that provide management and accounting support to OPM programs. Although all of the applications that comprise BFMS are housed on OPM's mainframe environment, it became apparent during this audit that the Office of the Chief Financial Officer (OCFO) does not have a clear understanding of which specific applications are actually a part of the BFMS umbrella of systems. Several iterations of the BFMS inventory were presented to Office of the Inspector General (OIG) auditors throughout the audit, and the versions differed with both the addition and subtraction of applications from the inventory.

The fact that the specific applications that are part of BFMS have not been clearly defined has limited the OCFO's ability to adequately manage several security-related elements required by FISMA. Specifically, the BFMS independent security control test, the internal self assessment of security controls, and the system's contingency plan could not have had accurately defined scopes. We consider this issue to be a significant deficiency in the BFMS control structure.

In addition to the concerns related to the BFMS application inventory, the OIG documented the following opportunities for improvement:

- The information system security plan for BFMS does not contain several critical elements required by National Institute of Standards and Technology (NIST) Special Publication 800-18.
- The security controls classified as common, application specific, or hybrid during the independent security test and evaluation were not consistent with the control classification done by the OCFO during the security control self-assessment.
- The BFMS self-assessment indicated that there were zero security weaknesses in the system. However, an OIG review of the same security controls indicated that weaknesses do exist.
- A contingency plan has been developed for BFMS. However, several areas of the contingency plan could be improved.
- The BFMS Privacy Impact Assessment (PIA) was conducted in accordance with the requirements of OPM's PIA Guide. However, OPM's PIA guide is missing several elements required by the Office of Management and Budget (OMB). Consequently, the BFMS PIA is missing these elements as well. Additionally, there is no evidence that the BFMS PIA has been reviewed by the system owner on an annual basis as required by OMB.
- OIG independently tested 25 of the NIST 800-53 controls for BFMS and found that 6 of these security controls were not in place during the fieldwork phase of the audit.

In addition, the OIG reviewed several elements of the BFMS security program that appear to be in full FISMA compliance:

- A security certification and accreditation (C&A) of BFMS was completed in August 2007 and another C&A is due for completion by August 2010.
- The OIG agrees with the security categorization of moderate for BFMS.
- A risk assessment was conducted for BFMS in 2007 that addresses all the required elements outlined in relevant NIST guidance.
- The BFMS Plan of Action and Milestones (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.

Contents

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) Benefits Financial Management System (BFMS).

Background

BFMS is one of OPM's 43 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.

The Office of the Chief Financial Officer (OCFO) has been designated with ownership of BFMS. The BFMS system provides the management and accounting support for the Civil Service Retirement Disability Fund, the Federal Employees' Group Life Insurance program, and the Federal Employees Health Benefits Program. BFMS is comprised of a set of individual applications that reside in OPM's mainframe environment. The mainframe infrastructure is supported by the agency's Data Center Group within the Office of the Chief Information Officer (OCIO).

This was our second audit of the security controls surrounding BFMS. The findings from the first BFMS audit report, issued in 2004, were closed prior to the start of this audit. We discussed the results of our audit with OCFO representatives at an exit conference and in a draft audit report.

Objectives

Our overall objective was to perform an evaluation of security controls for BFMS to ensure that OCFO officials have implemented IT security policies and procedures in accordance with standards established by OPM's OCIO. These policies and procedures are designed to assist program office officials in developing and documenting IT security practices that are in substantial compliance with FISMA, as well as OMB regulations and the National Institute of Standards and Technology (NIST) guidance.

OPM's IT security policies and procedures require managers of all major and sensitive 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 overall audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for BFMS, including:

- Certification and Accreditation Statement;
- Federal Information Processing Standard 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 OCFO and OCIO officials responsible for BFMS, including IT security controls in place as of April 2010.

We considered the BFMS 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 OCFO and other program officials with BFMS 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 BFMS 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 BFMS system of internal controls taken as a whole.

The criteria used in conducting this audit include:

- OPM IT Security Policy;
- 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 2, 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 Standard 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 December 2009 through April 2010 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

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

Results

I. Applications Included in the Benefit Financial Management System (BFMS)

BFMS is comprised of multiple applications that provide management and accounting support to OPM's Civil Service Retirement and Disability Fund, the Federal Employees' Group Life Insurance Program, and the Federal Employees Health Benefits Program. All BFMS applications reside within OPM's mainframe environment, and inherit many security controls from this infrastructure. However, throughout the fieldwork phase of this audit, it became apparent to OIG auditors that the OCFO does not have a clear understanding of which specific applications are actually a part of the BFMS umbrella of systems.

The 2007 and 2009 versions of the BFMS contingency plan and information system security plan (ISSP) each contain lists of applications that are part of BFMS. Although there were no major system changes during this time frame, the lists of applications vary significantly. The discrepancies in the BFMS inventory can be attributed to the removal of several systems that were actually owned by other OPM program offices or another federal agency, and the addition of an existing system that has a different user interface from the other applications, but shares the same back-end infrastructure.

In January 2010, the OCFO provided the OIG with an updated list of applications that differs from the 2009 documentation with the inclusion of two additional systems. The OCFO provided a subsequent update in March 2010 in which two systems were subtracted from the inventory (not the same two that were added in January 2010). The OCFO stated that the BFMS application inventory continues to be a work in progress.

The fact that the specific applications that are part of BFMS have not been clearly defined has limited the OCFO's ability to adequately manage several security-related elements required by FISMA. Specifically, the BFMS independent security control test, the internal self assessment of security controls, and the system's contingency plan could not have had accurately defined scopes, resulting in several applications not being properly tested. We consider this issue to be a significant deficiency in the BFMS control structure.

Recommendation 1

We recommend that the OCFO develop a clearly defined list of applications that are part of BFMS.

OCFO Response:

"CFO agrees with the recommendation and will provide a clearly defined list of applications related to BFMS by July 31, 2010."

Recommendation 2

We recommend that the OCIO review all applications dropped from the BFMS umbrella of systems and appropriately add them to OPM's system inventory.

OCFO Response:

"CFO agrees with the recommendation and will review all applications in conjunction with the CIO that do not belong to BFMS umbrella of systems by July 31, 2010."

II. Certification and Accreditation Statement

A security certification and accreditation (C&A) of BFMS was completed in August 2007.

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 BFMS C&A appears to have been conducted in compliance with NIST guidance.

OPM's Information Technology Security Officer reviewed the BFMS C&A package and signed the system's certification package on August 10, 2007. OPM's Chief Financial Officer signed the accreditation statement and authorized the continued operation of the system on August 17, 2007.

BFMS is due for a new C&A in August 2010; we will evaluate the new C&A as part of the FY10 FISMA audit.

III. FIPS 199 Analysis

Federal Information Processing Standard (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, Appendixes to 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 BFMS information system security plan (ISSP) categorizes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. BFMS is categorized with a moderate impact level for confidentiality, moderate for integrity, low for availability, and an overall categorization of moderate.

The security categorization of BFMS appears to be consistent with the guidance of FIPS 199 and NIST SP 800-60.

IV. Information System Security Plan

Federal agencies must implement the information system security controls outlined in NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems. NIST

SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems, requires that these controls be documented in an information systems security plan (ISSP) for each system, and provides guidance for doing so.

The ISSP for BFMS 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;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing; and
- Laws, Regulations, and Policies Affecting the System.

The BFMS ISSP contains the majority of the elements outlined by NIST. Although the ISSP lists systems that are interconnected with BFMS, it does not contain several critical details of these connections as required by the NIST guide. Specifically, the BFMS ISSP does not detail the FIPS 199 category, C&A status, or authorizing official of the interconnected systems.

Recommendation 3

We recommend that the system interconnection section of the BFMS ISSP be revised to include important identifiers of the interconnected systems (FIPS 199 categorization, C&A status, and the authorizing official).

OCFO Response:

"CFO agrees with the recommendation and will work with the CIO in conjunction to determine identifiers of the interconnected systems by August 6, 2010."

V. Risk Assessment

A risk management methodology focused on protecting core business operations and processes is a key component of an efficient IT security program. 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 BFMS in 2007 that addresses all of the elements outlined in the NIST guidance.

VI. Independent Security Control Testing

A security test and evaluation (ST&E) was completed for BFMS as a part of the system's C&A process in July 2007. The ST&E was conducted by an OPM contractor who was operating independently from BFMS. The OIG reviewed the controls tested to ensure that they included a review of the appropriate management, operational, and technical controls required for a system with a "moderate" security categorization according to NIST SP 800-53 Revision 2, Recommended Security Controls for Federal Information Systems.

The ST&E labeled each security control as common (inherited from OPM's IT infrastructure), application specific, or hybrid. The application specific and hybrid controls were tested as part of this ST&E, whereas the testing of common controls is the responsibility of OPM's OCIO. However, the controls identified as common controls in the ST&E were not consistent with the common controls identified in the BFMS self-assessment of security controls conducted by the OCFO. OPM's OCIO has not published a list of common controls for which they maintain responsibility, therefore the OCFO was required to make an assumption as to which controls are inherited from the OPM infrastructure. In addition, as mentioned in section I, the OCFO does not have a clearly defined list of the sub-applications that are part of BFMS.

Without clearly defined lists of common, hybrid, and application specific controls, or a clear understanding of the sub-applications that are part of BFMS, the BFMS ST&E could not have had an adequately defined scope. As a result, certain BFMS applications were not subject to proper independent security control testing.

Recommendation 4

We recommend that the OCFO and the OCIO determine whether each NIST SP 800-53 security control applicable to BFMS is common, application specific, or hybrid.

OCFO Response:

"CFO agrees with the recommendation. The CIO Information Technology Security Officer (ITSO) will determine the agency wide common security controls. The CFO will determine whether the security controls are BFMS application specific or hybrid by August 17, 2010."

Recommendation 5

Once the categorization of each security control is defined and the specific applications that are part of BFMS are determined, a new ST&E should be conducted for BFMS.

OCFO Response:

"CFO agrees with the recommendation and will ensure the categorization of each security control is defined and the specific applications that are part of BFMS are determined, a new ST&E will be conducted for BFMS as part of the Re C&A."

VII. Security Control Self-Assessment

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

The designated security officer (DSO) for BFMS conducted a self-assessment of the system in March 2009. The assessment included a review of the relevant management, operational, and technical security controls outlined in the NIST SP 800-53 Revision 2. However, as mentioned in section I, the OCFO does not have a clearly defined list of the sub-applications that are part of BFMS; therefore, the DSO could not have known all specific applications for which to test the security controls.

In addition, although the BFMS self-assessment indicated that there were zero security weaknesses in the system, an OIG review of the same security controls indicated that weaknesses do exist (see section XI, below).

Recommendation 6

Once the specific applications that are part of BFMS are determined, a new self-assessment of security controls should be conducted for BFMS.

OCFO Response:

"CFO agrees with the recommendation and will provide a new assessment of the security controls will be conducted for BFMS by August 6, 2010."

VIII. 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. The OPM IT security policy requires that OPM general support systems and major applications have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The BFMS Contingency Plan documents the functions, operations, and resources necessary to restore and resume BFMS operations when unexpected events or disasters occur. Although the BFMS contingency plan closely follows the format suggested by NIST SP 800-34 guidelines, several areas of the contingency plan could be improved.

The "recovery operations" section of the BFMS contingency plan outlines high level steps required to recover the system using alternate resources in a disaster situation. During the fieldwork phase of this audit, the OCFO described to OIG auditors several procedures that the OCFO is responsible for in a disaster recovery operation, including:

- Running test scripts and comparing "before" and "after" screenshots of the application to ensure the integrity of restored applications;
- Notifying OPM's Data Center Group of the results of these tests; and
- Communicating the status of recovery operations to external parties.

However, the BFMS contingency plan does not contain specific instructions for performing these steps of the recovery operation. Furthermore, as mentioned in section I, the OCFO does not have a clearly defined list of the sub-applications that are part of BFMS, and therefore the recovery procedures could not have had an adequately defined scope. As a result, there are BFMS applications for which the disaster recovery operations have not been tested.

In addition, although recovery teams and personnel have been identified in the BFMS contingency plan, the plan only lists the job title of each member, and does not specify the roles and responsibilities assigned to each individual or team. NIST SP 800-34 states that the "responsibilities" section of a contingency plan must detail the teams and personnel trained to respond to a disaster. Team members must be listed with their corresponding responsibilities and tasks.

Recommendation 7

We recommend that the restoration procedures section of the BFMS contingency plan be expanded to include specific details of each step required by OCFO personnel to recover each sub-application of BFMS in a disaster situation.

OCFO Response:

"CFO agrees with the recommendation and will expand the IT contingency plan to include specific details for each step required by CFO personnel to recover each sub-application of BFMS by August 6, 2010."

Recommendation 8

We recommend that the OCFO document the specific roles and responsibilities of teams and team members assigned contingency response procedures in the responsibilities section of the contingency plan.

OCFO Response:

"CFO agrees with the recommendation and will expand the IT contingency plan to include specific details for each step required by CFO personnel to recover each sub-application of BFMS by August 6, 2010. This will be done in a form of addendum."

Contingency Plan Test

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

In FY 2009, the OCFO conducted a table top review of the BFMS contingency plan. However, the OCFO did not conduct a scenario-based contingency plan test (to include critical elements such as scope, scenario, objectives, logistics, time frame, and participants) as required by NIST.

Recommendation 9

We recommend that the OCFO conduct a scenario-based contingency plan test in accordance with NIST SP 800-34 guidelines.

OCFO Response:

"CFO agrees with the recommendation and will conduct a scenario based contingency plan test in accordance with NIST 800-34 guidelines by August 17, 2010."

IX. Privacy Impact Assessment

The E-Government Act of 2002 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.

The OCFO completed an initial screening of the BFMS system and determined that a PIA was required for this system. In August 2007, a PIA of the system was conducted in accordance with the guidelines and template of the OPM PIA guide. A summary of the BFMS PIA is available on OPM's website.

However, OPM's PIA guide is missing several elements required by the OMB Memorandum. Consequently, the BFMS PIA is missing these elements as well. The OMB Memorandum states that PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. In addition, PIAs for major applications should reflect more extensive analyses of: consequences of collection and flow of information; the alternatives to collection and handling as designed; the appropriate measures to mitigate risks identified for each alternative; and the rationale for the final design choice or business process.

In addition, there is no evidence that the BFMS PIA has been reviewed by the system owner on an annual basis, as required by OMB.

Recommendation 10

We recommend that the OCFO conduct a PIA for BFMS that includes all of the required elements from OMB Memorandum M-03-22.

OCFO Response:

"CFO agrees with the recommendation and will update the PIA to have the required elements for BFMS by August 6, 2010."

Recommendation 11

We recommend that the OCFO review the BFMS PIA on an annual basis and submit evidence of this review to the OCIO.

OCFO Response:

"CFO agrees with the recommendation and will update the PIA to have the required elements for BFMS by August 6, 2010."

X. Plan of Action and Milestones Process

A Plan of Action and Milestones (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 OIG evaluated the BFMS POA&M and verified that it follows the format of OPM's template, and has been routinely submitted to the OCIO for evaluation. We also determined that the POA&M contained action items for all security weaknesses identified through various security control tests and audits.

Nothing came to our attention during this evaluation to indicate that there are any current weaknesses in the OCFO's management of POA&Ms.

XI. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 2, 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, the OIG determined whether a subset of these controls had been adequately implemented for BFMS, including:

- AC-2 Account Management
- AC-7 Unsuccessful Login Attempts
- AC-11 Session Lock
- AC-13 Supervision and Review – Access Control
- AU-2 Auditable Events
- IA-1 Identification and Authentication
- IA-4 Identifier Management
- IA-5 Authenticator Management
- MP-6 Media Sanitization and Disposal
- CM-6 Configuration Settings
- PL-4 Rules of Behavior

- AU-3 Content of Audit Records
- AU-6 Audit Monitoring, Analysis, and Reporting
- AU-8 Time Stamps
- CA-3 Information System Connections
- CM-2 Baseline Configuration
- CM-3 Configuration Change Control
- CM-4 Monitoring Configuration
- PL-6 Security-Related Activity Planning
- PS-2 Position Categorization
- PS-4 Personnel Termination
- PS-5 Personnel Transfer
- PS-6 Access Agreements
- RA-5 Vulnerability Scanning
- SA-3 Life Cycle Support

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

As mentioned in section I, the OCFO does not have a clearly defined list of the sub-applications that are part of BFMS. The OIG's evaluation was based on the OCFO's inventory of BFMS applications during the fieldwork phase of this audit, and therefore may not represent the effectiveness of security controls for all BFMS applications.

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

a) Account Management (AC-2)

The OCFO does not conduct reviews of the user accounts of BFMS applications. Although the initial access established for a BFMS user is reviewed and approved, there are no periodic audits of user accounts to ensure that each user's specific access rights and privileges remains appropriate.

NIST SP 800-53 Revision 2 control AC-2 requires information system owners to periodically (at least annually) review information system accounts. Failure to routinely review user accounts increases the risks that users have access to information that is not directly related to their job function.

Recommendation 12

We recommend that the OCFO establish a formal process for reviewing user accounts for appropriateness for each application that makes up BFMS.

OCFO Response:

"CFO agrees with the recommendation and will revise the BFMS account management to include the lists received by the OCIO IT security team. This should be completed by August 6, 2010."

b) Auditing (AU-2, AU-3, AU-6)

Application level auditing has not been established for BFMS applications.

In order to access BFMS applications, a user must authenticate to the mainframe through its security software, IBM's Resource Access Control Facility (RACF). OPM's OCIO has procedures for logging and auditing users that authenticate to RACF. However, the OCIO does not log user authentications to the BFMS applications, or user activity within those applications. Without such logs, the OCFO is unable to audit user access and activity for BFMS.

NIST SP 800-53 Revision 2 requires that:

- An information system generates audit records for a series of predefined events (*control AU-2, Auditable Events*);
- Audit records " contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events" (*control AU-3, Content of Audit Records*);
- The system owner "regularly reviews/analyzes information system audit records for indications of inappropriate or unusual activity" (*control AU-6 Audit Monitoring, Analysis, and Reporting*).

Failure to adequately log and audit activity within each BFMS application increases the risk that unauthorized user activity occurs undetected.

Recommendation 13

We recommend that the OCFO develop a clearly defined list of user activity that should be logged for each BFMS application and then implement the technical controls to begin logging this activity. Once the logging capability has been implemented, the OCFO should routinely audit/review the log activity.

OCFO Response:

"CFO agrees with the recommendation and will work with CIO/ BS and the security office in determining a mechanism for this process. We will revise the BFMS account management process to include the lists received by the CIO security office. This should be completed by August 6, 2010."

c) Rules of Behavior (PL-4)

All individuals accessing OPM's network environment and the applications that reside within it must sign a "Computer User Responsibilities Statement" that outlines the appropriate use of the agency's IT resources. However, BFMS users are not required to sign a Rules of Behavior document specific to the BFMS applications.

NIST SP 800-53 Revision 2 requires that "The organization establishes and makes readily available to all information system users, a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organization receives signed acknowledgment from users indicating

that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information."

Recommendation 14

We recommend that a formal Rules of Behavior document be developed for each BFMS application and that it be signed by all new and existing users.

OCFO Response:

"CFO agrees with the recommendation to implement rules of behavior for BFMS that is compliant with the CIO policy. This recommendation will be completed by August 6, 2010."

d) Personnel Termination (PS-4)

Five user accounts for one of the BFMS applications, the Federal Financial System, remained active after the individual's employment was terminated. Each of these user's RACF accounts had been deactivated by the OCIO, which would have prevented them from accessing the system after their termination. However, disabling the application level accounts provides an extra layer of control to ensure that unauthorized users cannot access the system.

NIST SP 800-53 Revision 2 control PS-4 states that information system access should be immediately disabled upon termination of an individual.

Recommendation 15

We recommend that the OCFO implement a process for periodically reviewing user accounts for each BFMS application to ensure that no terminated employees have active access.

OCFO Response:

"CFO agrees with the recommendation and will revise the BFMS account management procedures from last year. The revised BFMS account management procedures will contain a separate paragraph for terminating employees. This recommendation will be completed by July 31, 2010."

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

Appendix

U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
WASHINGTON, DC

REPORT NO. 4A-CF-00-10-018

Audit of the Information Technology Security Controls of the US Office of Personnel Management Benefits Financial Management System

CHIEF FINANCIAL OFFICER RESPONSE – JUNE 15, 2010:

CFO Response to OIG Draft Audit Report 4A-CF-00-10-018

Recommendation 1
We recommend that CFO develop a clearly defined list of applications that are part of BFMS.

Action by the CFO:
CFO agrees with the recommendation and will provide a clearly defined list of applications related to BFMS by July 31, 2010.

Recommendation 2
We recommend that the CIO review all applications dropped from the BFMS umbrella of systems and appropriately add them to OPM's system inventory.

Action by the CFO:
CFO agrees with the recommendation and will review all applications in conjunction with the CIO that do not belong to BFMS umbrella of systems by July 31, 2010.

Recommendation 3
We recommend that the system interconnection section of the BFMS ISSP be revised to include important identifiers of the interconnected systems (FIPS 199 categorization, C&A status, and the authorizing official).

Action by the CFO:
CFO agrees with the recommendation and will work with the CIO in conjunction to determine identifiers of the interconnected systems by August 6, 2010.

Recommendation 4
We recommend that CFO and CIO determine whether each NIST SP 800-53 security control applicable to BFMS is common, application specific or hybrid.

Action by the CFO:
CFO agrees with the recommendation. The CIO Information Technology Security Officer (ITSO) will determine the agency wide common security controls. The CFO will determine whether the security controls are BFMS application specific or hybrid by August 17, 2010.

Recommendation 5
We recommend that once the categorization of each security control is defined and the specific applications that are part of BFMS are determined, a new ST&E should be conducted for BFMS.

Action by the CFO:
CFO agrees with the recommendation and will ensure the categorization of each security control is defined and the specific applications that are part of BFMS are determined, a new ST&E will be conducted for BFMS as part of the Re C&A.

Recommendation 6
We recommend once the specific applications are defined for BFMS, a new assessment of security controls should be conducted for BFMS.

Action by the CFO:
CFO agrees with the recommendation and will provide a new assessment of the security controls will be conducted BFMS by August 6, 2010.

Recommendation 7
We recommend that the restoration procedures section of the BFMS contingency plan be expanded to include specific details of each step required by CFO personnel to recover each sub-application of BFMS in a disaster situation.

Action by the CFO:
CFO agrees with the recommendation and will expand IT contingency plan to include specific details for each step required by CFO personnel to recover each sub-application of BFMS by August 6, 2010.

Recommendation 8
We recommend that CFO document the specific roles and responsibilities of teams and team members assigned contingency response procedures in the responsibilities section of the contingency plan.

Action by the CFO:
CFO agrees with the recommendation and will expand IT contingency plan to include specific details for each step required by CFO personnel to recover each sub-application of BFMS by August 6, 2010. This will be done in a form of addendum.

Recommendation 9
We recommend OCFO conduct a scenario based contingency plan test in accordance with NIST SP 800-34 guidelines.

Action by the CFO:
CFO agrees with the recommendation and will conduct a scenario based contingency plan test in accordance with NIST 800-34 guidelines by August 17, 2010.

Recommendation 10
We recommend CFO conduct a PIA for BFMS that includes all of the required elements from OMB memorandum M-03-22.

Action by the CFO:
CFO agrees with the recommendation and will update the PIA to have the required elements for BFMS by August 6, 2010.

Recommendation 11
We recommend CFO review the BFMS PIA on an annual basis and submit evidence of this review to CIO.

Action by the CFO:
CFO agrees with the recommendation and will update the PIA to have the required elements for BFMS by August 6, 2010.

Recommendation 12
We recommend that a formal process for reviewing user accounts for appropriateness for each application that makes up BFMS.

Action by the CFO
CFO agrees with the recommendation and will revise the BFMS account management to include the lists received by the OCIO IT security team. This should be completed by August 6, 2010.

Recommendation 13
We recommend that CFO develop a clearly defined list of user activity that should be logged for each BFMS application and then implement the technical controls to begin logging this activity. Once the logging capability has been implemented, CFO should routinely audit/review the log activity.

Action by the CFO
CFO agrees with the recommendation and will work with CIO/ BS and the security office in determining a mechanism for this process. We will revise the BFMS account management process to include the lists received by the CIO security office. This should be completed by August 6, 2010.

Authentication is performing by RACF but authorization is performed by Natural Security. DC security team will meet with BS and CFO to establish a procedure for this process.

Recommendation 14
We recommend that a formal Rules of Behavior document be developed for each BFMS application, and that it be signed for all new and existing users.

Action by the CFO:
CFO agrees with the recommendation to implement rules of behavior for BFMS that is compliant with the CIO policy. This recommendation will be completed by August 6, 2010.

Recommendation 15
We recommend that the CFO implement a process for periodically reviewing user accounts for each BFMS application to ensure that no terminated employees have active access.

Action by the CFO:
CFO agrees with the recommendation and will revise the BFMS account management procedures from last year. The revised BFMS account management procedures will contain a separate paragraph for terminating employees. This recommendation will be completed by July 31, 2010.

This control is already in place. Data Center security team on a weekly basis receives a Separation file provided by OPM's personnel office. DC security team compares the file received from HR with the information in the RACF database and if there is a match the Userid is removed from the system. DC security team has implemented a procedure by which they pass the information regarding employees separating from OPM and inter-agency employee transfers to the Help Desk and all the program office DSOs for action.