



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
SERENA BUSINESS MANAGER
FY 2013**

Report No. 4A-CI-00-13-023

Date: July 19, 2013

--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
SERENA BUSINESS MANAGER
FY 2013

WASHINGTON, D.C.

Report No. 4A-CI-00-13-023

Date: July 19, 2013



Michael R. Esser
Assistant Inspector General
for Audit

--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
SERENA BUSINESS MANAGER
FY 2013**

WASHINGTON, D.C.

Report No. 4A-CI-00-13-023

Date: July 19, 2013

This final audit report discusses the results of the Office of the Inspector General's (OIG) review of the information technology security controls of the U.S. Office of Personnel Management's (OPM) Serena Business Manager (SBM). Our conclusions are detailed in the "Results" section of this report.

SBM was originally used for software change management control, issue, and defect tracking. In 2004, the Office of the Chief Information Officer (OCIO) recognized an opportunity to use the tool for developing administrative support applications for OPM program offices.

Currently SBM is used by the OCIO to design, develop, test and implement applications used by multiple organizational units within OPM. SBM hosts minor applications that are developed and tested using the SBM platform.

We have ongoing concerns about the security of SBM. The system has been hacked twice in the last year, with both breaches leading to the loss of sensitive data. We issued a flash audit alert to the OPM Director on April 8, 2013 (See Appendix II), recommending that all public-facing elements of SBM be taken offline until the system could be adequately secured.

In response to our alert, the Director instructed the OCIO to shut down the public-facing portion of the system. The OCIO also developed a corrective action plan to address the SBM security flaws (see Appendix III.) We agree with the corrective action plan and will continue to monitor this issue.

In addition, we documented the following opportunities for improvement:

- SBM does not have a standardized process in place to routinely audit user accounts for appropriate access across all applications within the system; and
- SBM currently does not utilize access agreement forms for the information system.

As part of this audit, we determined that the following elements of the SBM security program appear to be in full compliance with the Federal Information Security Management Act:

- A Security Assessment and Authorization of SBM was completed in December 2012;
- SBM is appropriately assigned a security categorization of “moderate”;
- The SBM System Security Plan contains elements required by NIST SP 800-18 Revision 1;
- A Security Assessment Plan has been documented and tested in FY 2013 with the results incorporated into the Security Assessment Report;
- The OCIO conducted a self-assessment of the security controls of SBM in FY 2012;
- A contingency plan was reviewed, updated and tested for the system in FY 2013;
- A Privacy Impact Assessment was completed for SBM in November 2012;
- The SBM Plan of Action and Milestones (POA&M) follows the format of the OPM POA&M guide, and has been routinely submitted to the OCIO for evaluation; and
- A risk assessment was conducted for SBM in FY 2013 that addresses all the required elements outlined in relevant guidance.

Contents

	<u>Page</u>
Executive Summary	i
Introduction.....	1
Background.....	1
Objectives	1
Scope and Methodology	2
Compliance with Laws and Regulations.....	3
Results.....	4
I. Security Assessment and Authorization	4
II. FIPS 199 Analysis.....	4
III. System Security Plan	4
IV. Security Assessment Plan and Report.....	5
V. Security Control Self-Assessment.....	5
VI. Contingency Planning and Contingency Plan Testing	6
VII. Privacy Impact Assessment.....	6
VIII. Plan of Action and Milestones Process	6
IX. NIST SP 800-53 Evaluation.....	7
X. Security Breaches Involving Serena.....	10
Major Contributors to this Report.....	11
Appendix I: OCIO’s April 9, 2013 response to the draft audit report, issued March 1, 2013	
Appendix II: OIG’s April 8, 2013 Flash Audit Alert – Information System Security at the U.S. Office of Personnel Management	
Appendix III: OCIO’s April 10, 2013 Response to the Flash Audit Alert issued April 8, 2013	

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) Serena Business Manager (SBM).

Background

SBM 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 Office of the Chief Information Officer (OCIO) has ownership and managerial responsibility of the SBM system and is also responsible for IT development, support, and maintenance of the system. SBM resides on the OPM Local Area network/Wide Area Network (LAN/WAN) in the Development/Test and Production (DTP) environment.

Serena Business Manager (formerly called TeamTrack) was originally purchased for software change management control, and issue/defect tracking. After the acquisition of TeamTrack, it was realized that the software provided the OCIO the capability to develop administrative applications for a fraction of the cost of developing custom applications.

In 2004, the OCIO recognized an opportunity to use the tool for developing administrative support applications for other OPM program offices. There were many existing administrative support tracking systems throughout OPM that were originally built using various technologies such as MS Access, Powerbuilder, and Coldfusion. Reengineering these systems as SBM applications provided the OCIO an opportunity to build and maintain these applications in one environment where applications shared one browser interface, common software components, and one single place to manage user access and application security.

Objectives

Our objective was to perform an evaluation of the security controls for SBM to ensure that OCIO 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 policy.

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 SBM, including:

- Security Assessment and Authorization;
- FIPS 199 Analysis;
- System Security Plan;
- Security Assessment Plan and Report;
- 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 OCIO personnel responsible for SBM, including IT security controls in place as of February 2012.

We considered the SBM 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 OCIO and other individuals with SBM 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 SBM 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 SBM system of internal controls 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;
- 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 and Organizations;
- 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 2012 through February 2013 in OPM's Washington, D.C. office.

Compliance with Laws and Regulations

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

Results

I. Security Assessment and Authorization

A Security Assessment and Authorization (SA&A) of SBM was completed in December 2012.

OPM's Chief Information Officer reviewed the SBM SA&A package and signed the system's authorization memorandum on December 19, 2012.

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

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 SBM FIPS 199 Security Categorization Template analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. SBM 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 SBM appears to be consistent with FIPS 199 and NIST SP 800-60 requirements, and the OIG agrees with the categorization of moderate.

III. 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 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 SBM was created using the template outlined in NIST SP 800-18. 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.

The SBM SSP adequately addresses each of the elements required by NIST.

IV. Security Assessment Plan and Report

A Security Assessment Plan (SAP) and Security Assessment Report (SAR) were completed for SBM in November and December 2012 respectively as a part of the system's SA&A process. We reviewed the document to verify a risk assessment was conducted in accordance with NIST SP 800-30, Risk Management Guide for Information Technology Systems. 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 3, Recommended Security Controls for Federal Information Systems and Organizations.

The SAP assessment results table labeled each security control as fully satisfied, partially satisfied, not satisfied or not applicable. The SAR identified 23 total control weaknesses. The SBM Plan of Action and Milestones (POA&M) describes the corrective measures that have been implemented or are planned to address these weaknesses.

Nothing came to our attention to indicate that the security controls of SBM have not been adequately tested.

V. 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 SBM system in August 2012. The assessment included a review of a subset of management, operational, and technical security controls outlined in NIST SP 800-53 Revision 3. Nothing came to our attention to indicate that the security controls of SBM have not been adequately tested by the OCIO.

VI. 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 SBM contingency plan documents the functions, operations, and resources necessary to restore and resume SBM operations when unexpected events or disasters occur. The SBM contingency plan closely follows the format suggested by NIST SP 800-34 and contains a majority of the suggested 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 SBM contingency plan was conducted in June 2010. The testing documentation contained an analysis and review of the results. We reviewed the testing documentation to determine if the test conformed with NIST 800-34 guidelines.

VII. 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.

On November 1, 2012 a PIA was conducted on SBM that was based on the guidelines contained in OPM's PIA Guide. The PIA was reviewed by OPM's Chief Privacy Officer and Chief Information Officer.

VIII. 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 SBM POA&M follows OPM's standard template and has been routinely submitted to the OCIO for evaluation. The OIG verified that weaknesses identified as a result of the SA&A security control testing and vulnerability scanning have been documented on SBM's system POA&M.

IX. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 3, Recommended Security 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 40 of these security controls from the following families:

- Access Control;
- Audit and Accountability;
- Security Assessment and Authorization;
- Configuration Management;
- Contingency Planning;
- Identification and Authentication;
- Planning;
- Personnel Security;
- Risk Assessment; and
- System and Information Integrity.

These controls were evaluated by interviewing individuals with SBM 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 Revision 3 security controls have been successfully implemented for SBM, several tested controls were not fully satisfied.

a) AC-6 Least Privilege

NIST SP 800-53 Revision 3 requires that “The organization employs the concept of least privilege, allowing only authorized users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organization missions and business functions.”

SBM does not have a standardized process in place to routinely audit user accounts for appropriate access across all applications on the system. Currently, the owners of all of the various applications within SBM use their own process to audit user account access. The methodology to audit user accounts varies greatly from application to application.

Failure to implement a standardized process to audit user accounts for appropriate access increases the likelihood of an unauthorized user having access to protected organizational information.

Recommendation 1

We recommend the OCIO reevaluate its current methodology and implement a standardized process for auditing user account access across all applications for SBM.

OCIO Response:

“The Report noted that SBM does not have a standardized process in place to routinely audit user accounts for appropriate access across all applications on the system. The following actions have been taken to address the weakness.

- *CIO is currently working on a standardized process to track all account requests to SBM application. CIO will also include a process to review current SBM account access and take corrective actions as needed. This will be performed on a regular basis.*
 - *Specifically, we are currently collecting account data needs to ensure the system owners/administrators are getting the audit results they need and to confirm who is or is not authorized account access. This also would resolve the separation of duties issue where we collect the raw logs and then provide them to the System Owner/Admin for review/validation.*
- *As an interim solution, the DSO/managed administrators will create requests in the SBM ACTS application to track requests. All external users have agreements which are now being uploaded to the CIO CMS system. The assigned Rules of Behavior and the fax copy of the access request are also being uploaded.*
- *In the long-term, we will work with the NM Help Desk; modifying the 1665 so that the Help Desk can field account requests and collect sufficient information to establish new accounts.”*

OIG Reply:

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

b) PS-6 Access Agreements

NIST SP 800-53 Revision 3 states that the organization “ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access” and “reviews and updates the access agreements.”

SBM currently does not utilize access agreement forms when granting individuals access to the information system. Currently, users who require access to SBM applications send an e-mail request to the Designated Security Officer. This current process makes it very difficult to find an individual’s access request when necessary and to audit user accounts for appropriate access as previously discussed in section AC-6, Least Privilege.

Failure to use, review, and update access agreement forms increases the risk of an unauthorized user gaining access to private and proprietary organizational information.

Recommendation 2

We recommend the OCIO implement the use of access agreement forms when granting individuals access to SBM, review the forms on a routine basis, and update them when necessary.

OCIO Response:

“The Report noted that SBM does not utilize access agreement forms when granting individuals access to the information system. Users who require access send an email request to the DSO. The current process makes it difficult not only to find individual access requests, but also audit user accounts to ensure appropriate access. The following action has been taken to address the weakness.

- *OCIO uses the 1665 form for both AD access and access to specific applications. The reconciliation between the 1665 authorization for access and the log files of actual account access should be occurring at the System level where System Owner/Administrators grant authorized access according to their program requirements.*
 - *OCIO will develop a continuous monitoring solution to provide system owners with regular reports on account access for their audits of account access.*
- *SBM uses Active Directory authentication and all access is tied to LAN/WAN accounts. The new process that is currently being designed (described as an interim solution in section AC-6 above) will remediate this problem. The long-term intent is to incorporate standard data collection form/processes for Serena.”*

OIG Reply:

As part of the audit resolution process, we recommend that the OCIO provide IOC with evidence supporting the remediation of the recommendation.

c) RA-5 Vulnerability Scanning

NIST SP 800-53 Revision 3 states that the organization “scans for vulnerabilities in the information system and hosted applications” and “remediates legitimate vulnerabilities in accordance with organizational assessment of risk.”

The SBM information system resides on a server in OPM’s LAN/WAN environment. The OCIO’s Network Security Branch (NSB) conducts routine vulnerability scanning and reports the results to the system owner. After reviewing the report of SBM’s most recent vulnerability scan, we identified several major weaknesses that have not been remediated. We contacted NSB and SBM personnel and discovered that this was a known vulnerability on several servers in the environment.

There is currently a project in place to remediate the vulnerabilities and employ Defense Information Systems Agency: Security Technical Implementation Guide (DISA STIG) compliant configuration settings on all affected servers.

The OIG will follow-up on the status of the implementation project during the FY 2013 General FISMA Audit, and no recommendation will be issued as part of this report.

OCIO Response:

“The Report noted that the OIG review of [the] most recent vulnerability scan identified several major weaknesses that required remediation, but that there is currently a project to remediate the vulnerabilities and employ Defense Information Systems Agency: Security Technical Implementation Guide (DISA STIG) compliant configuration.

CIO currently has scheduled vulnerability scanning on the network. This will be expanded to all web applications.”

X. Security Breaches Involving Serena

In May 2012, a malicious hacker successfully breached SBM and obtained sensitive data. The system was briefly taken down by the OCIO, but was quickly restored and made available on the public Internet.

As mentioned in section IX above, NSB routinely conducts vulnerability scans on the technical infrastructure supporting SBM. The OIG also issued an audit recommendation in FY 2012 that the OCIO routinely audit Oracle database configurations for compliance with an approved baseline (Report No. 4A-CI-00-12-016 Recommendation 3). However, it appears that no action was taken to address the concerns raised by NSB or the OIG, as SBM was breached again in March 2013, again leading to the loss of sensitive data.

These attacks exploited weaknesses that were already known to OCIO personnel, and it is our opinion that the system should not have been placed back online in this insecure state. Our independent test work indicated that the servers and databases supporting SBM continued to operate with critical vulnerabilities as of March 20, 2013. Therefore, we issued a flash audit alert to the OPM Director on April 8, 2013 recommending that all public-facing elements of SBM be taken down until the system could be adequately secured.

In response to our alert, the Director instructed the OCIO to shut down the public-facing portion of the system and develop a corrective action plan to quickly address the SBM security flaws (see Appendix III.) We agree with the corrective action plan and will continue to monitor this issue.

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 I

April 9, 2013

MEMORANDUM FOR [REDACTED]
CHIEF INFORMATION SYSTEMS AUDIT GROUP

THROUGH: [REDACTED]
ACTING CHIEF INFORMATION OFFICER

THROUGH: [REDACTED]
DEPUTY CHIEF INFORMATION OFFICER FOR
OPERATIONS

FROM: [REDACTED]
DIRECTOR, APPLICATION SYSTEMS

Subject: Audit of the Information Technology Security Controls of the
U.S. Office of Personnel Management's Serena Business
Manager (Report No. 4A-CI-00-13-023)

Thank you for the opportunity to provide comments on the Draft Audit Report for Serena Business Manager. Our comments are directed specifically towards Results Section IX, NIST SP 800-53 Revision 3 Evaluation. The Draft Report identifies several tested security controls that were not fully satisfied during the course of the audit.

AC-6 Least Privilege

The Report noted that SBM does not have a standardized process in place to routinely audit user accounts for appropriate access across all applications on the system. The following actions have been taken to address the weakness.

- CIO is currently working on a standardized process to track all account requests to SBM application. CIO will also include a process to review current SBM account access and take corrective actions as needed. This will be performed on a regular basis.
 - Specifically, we are currently collecting account data needs to ensure the system owners/administrators are getting the audit results they need and to confirm who is or is not authorized account access. This also would resolve the separation of duties issue where we collect the raw logs and then provide them to the System Owner/Admin for review/validation.

- As an interim solution, the DSO/managed administrators will create requests in the SBM ACTS application to track requests. All external users have agreements which are now being uploaded to the CIO CMS system. The assigned Rules of Behavior and the fax copy of the access request are also being uploaded.
- In the long-term, we will work with the NM Help Desk; modifying the 1665 so that the Help Desk can field account requests and collect sufficient information to establish new accounts.

PS-6 Access Agreements

The Report noted that SBM does not utilize access agreement forms when granting individuals access to the information system. Users who require access send an email request to the DSO. The current process makes it difficult not only to find individual access requests, but also audit user accounts to ensure appropriate access.. The following action has been taken to address the weakness.

- OCIO uses the 1665 form for both AD access and access to specific applications. The reconciliation between the 1665 authorization for access and the log files of actual account access should be occurring at the System level where System Owner/Administrators grant authorized access according to their program requirements.
 - OCIO will develop a continuous monitoring solution to provide system owners with regular reports on account access for their audits of account access.
- SBM uses Active Directory authentication and all access is tied to LAN/WAN accounts. The new process that is currently being designed (described as an interim solution in section AC-6 above) will remediate this problem. The long-term intent is to incorporate standard data collection form/processes for Serena.

RA-5 Vulnerability Scanning

The Report noted that the OIG review of most recent vulnerability scan identified several major weaknesses that required remediation, but that there is currently a project to remediate thee vulnerabilities and employ Defense Information Systems Agency: Security Technical Implementation Guide (DISA STIG) compliant configuration.

CIO currently has scheduled vulnerability scanning on the network. This will be expanded to all web applications.

If there are additional questions, please contact [REDACTED] at [REDACTED].

Appendix II



Office of the
Inspector General

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

April 8, 2013

MEMORANDUM FOR JOHN BERRY
Director

FROM: PATRICK E. McFARLAND
Inspector General

A handwritten signature in black ink that reads "Patrick E. McFarland".

SUBJECT: Flash Audit Alert – Information System Security at the
U.S. Office of Personnel Management

The U.S. Office of Personnel Management (OPM) Office of the Inspector General (OIG) is issuing this flash audit alert to bring to your immediate attention serious concerns we have regarding information system security at OPM.

In May 2012, a malicious hacker successfully breached OPM's Serena Business Manager system (Serena, formerly known as TeamTrack). The system was briefly taken down by OPM's Office of the Chief Information Officer (OCIO), but was quickly restored and made available on the public Internet.

Over the past year, the OCIO's Network Security Branch has conducted vulnerability scans that detected security flaws in the Serena system. However, it appears that no action was taken by the system administrators to address these issues, as another application on the Serena platform was hacked in March 2013. After both security breaches, the hackers boasted on the Internet about compromising a government computer system, leading to embarrassing publicity for OPM.

As part of our recent audit of Serena, we conducted independent testing of this system and determined that critical security flaws continue to exist on both the servers and the databases supporting this system. As a short term action, ***we recommend that you order all Internet facing elements of Serena to be taken down until the system can be adequately secured.***

Unfortunately, our concerns are not limited to the Serena system, and we believe this issue is indicative of a systemic problem at OPM. It is our understanding that Serena and many other OPM systems operate in a "development" environment and therefore have never been subject to the thorough security and functionality testing that a production system should receive.

Appendix II

Honorable John Berry

2

We will continue to perform audit work related to these concerns, with a focus on the security of Internet facing systems hosted in the “development” environment. We will provide you with additional details in two forthcoming final audit reports:

- Audit of the Information Technology Security Controls of Serena Business Manager (to be issued in April 2013)
- Federal Information Security Management Act Audit – FY 2013 (to be issued in November 2013)

If you have any questions you can contact me, at [REDACTED] or a member of your staff may contact Michael Esser, Assistant Inspector General for Audits, at [REDACTED].

Appendix III



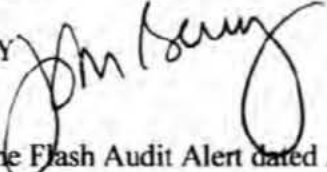
The Director

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT





Washington, DC 20415

APR 10 2013


MEMORANDUM FOR: PATRICK E. MCFARLAND
Inspector General

FROM : JOHN BERRY 
Director

SUBJECT : Response to the Flash Audit Alert dated April 8, 2013

Thank you for bringing this matter to my immediate attention. In response, Chuck Simpson, , and  from the Office of the Chief Information Officer (OCIO) met with Michael Esser, , and  from your staff, on April 9, 2013, to clarify the information system security issues. They mutually agreed on the following actions:

- 1) The external-facing access point to the Internet was disabled for all the Serena Business Manager (SBM) applications as of 5:00 pm April 9;
- 2) The applications on SBM would remain available to internal OPM users;
- 3) OCIO and IG staffs will work collaboratively to review and remediate SBM platforms and applications, based on a phased approach, in order to reopen the access to external users as quickly as possible; and
- 4) OCIO and IG staffs will work together to identify any other sites internal to OPM and remediate.

We will continue to monitor the work on this issue. If you have any questions please call Chuck Simpson, Acting Chief Information Officer, at , or email him at

Charles.Simpson@opm.gov.