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 SHAREPOINT IMPLEMENTATION

Report Number 4A-CI-00-17-030
September 29, 2017

EXECUTIVE SUMMARY

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's SharePoint Implementation

Report No. 4A-CI-00-17-030 **September 29, 2017**

Why Did We Conduct the Audit?

Microsoft's SharePoint software (SharePoint) is one of the U.S. Office of Personnel Management's (OPM) newest information technology (IT) systems. SharePoint was initially implemented within OPM's development and test environment and was not intended for agency-wide production use. However, demand led OPM to begin using the commercial software as a production system in fiscal year 2017. We conducted an audit of OPM's SharePoint implementation to evaluate the system's security controls.

What Did We Audit?

The Office of the Inspector General has completed a performance audit of OPM's SharePoint implementation to ensure that the system's security controls meet the standards established by the Federal Information Security Modernization Act, the National Institute of Standards and Technology, the Federal Information Security Controls Audit Manual and OPM's Office of the Chief Information Officer.

Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

Our audit of the IT security controls of the SharePoint implementation determined that:

- As OPM expanded the use of SharePoint into its production IT environment it did not assess whether the expansion warranted reclassifying the system as a "major" information system that would require a formal Security Assessment and Authorization.
- OPM has not established any policies and procedures specific to SharePoint nor determined whether the expansion of SharePoint warrants updating any of OPM's current policies and procedures.
- SharePoint administrators and/or owners are not provided or required to take training specific to their job position.
- OPM does not have formal procedures for requesting and provisioning SharePoint user accounts.
- OPM does not routinely audit SharePoint's logical access management.
- OPM has not documented formal SharePoint security configuration standards, and therefore cannot effectively audit its system's security settings.
- OPM has not implemented a process to test software security patches and install them on SharePoint servers and databases in a timely manner.

ABBREVIATIONS

Authorization	**Security Assessment and Authorization**
FISCAM	**Federal Information System Controls Audit Manual**
FISMA	**Federal Information Security Modernization Act**
IG	**Inspector General**
IT	**Information Technology**
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**
SharePoint	**OPM's implementation of Microsoft's SharePoint software**
Sites	**Unique SharePoint Repositories**
SP	**Special Publication**

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. 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 2014, Public Law 113-283, the Federal Information Security Modernization Act (FISMA), was established and reaffirmed the objectives of the prior FISMA. As part of our evaluation, we will review the U.S. Office of Personnel Management (OPM)'s FISMA compliance strategy and document the status of their compliance efforts. FISMA requires that the Office of the Inspector General (OIG) perform an audit of the information technology (IT) security controls of all of the agency's systems on a rotating basis. In accordance with FISMA, we audited the IT security controls related to the OPM's implementation of Microsoft's SharePoint software (SharePoint).

SharePoint is one of OPM's newest IT systems. SharePoint was initially implemented within OPM's development and test environment and was not intended for agency-wide production use. However, demand led OPM to begin using the commercial software as a production system in fiscal year 2017.

The SharePoint product is a web-based application primarily used for document management. Documentation is stored, organized, and accessed via unique SharePoint repositories (sites). Sites are unique repositories made up of libraries and lists.[1] The application is supported by several backend servers and databases within OPM's internal network.

OPM's Office of the Chief Information Officer (OCIO) has primary responsibility for implementing and managing the IT security controls of SharePoint. We discussed the results of our audit with the OCIO representatives at an exit conference.

[1] A SharePoint "library" stores and displays files and folders. A SharePoint "list" is similar to a database or spreadsheet.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

Our objective was to perform an evaluation of access controls and security configurations for OPM's SharePoint web portals, applications, and databases in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), and OPM IT security policies and procedures.

The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for SharePoint, including:

- Security management;
- Access controls;
- Configuration management; and
- Vulnerability management.

SCOPE AND METHODOLOGY

This performance audit was conducted in accordance with the Generally Accepted 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 the OCIO officials responsible for SharePoint, including the evaluation of IT security controls in place as of June 2017.

We considered the OPM 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 program office with SharePoint 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.

The findings, recommendations, and conclusions outlined in this report are based on the status of security controls protecting the confidentiality, integrity, and availability of SharePoint as of June 2017 and are located in the "Audit Findings and Recommendations" 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 SharePoint's internal controls taken as a whole.

Various laws, regulations, and industry standards were used as a guide for evaluating SharePoint. These criteria include, but are not limited to, the following publications:

- OPM Information Security and Privacy Policy Handbook;
- OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources;
- P.L. 107-347, Title III, Federal Information Security Management Act of 2002;
- P.L. 113-283, Federal Information Security Modernization Act of 2014;
- The Federal Information System Controls Audit Manual (FISCAM);
- NIST Special Publication (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 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;

- 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 the Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States.

The audit was performed by OPM's OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from February 2017 through June 2017 in OPM's Washington, D.C. office.

COMPLIANCE WITH LAWS AND REGULATIONS

In conducting the audit, we performed tests to determine whether the OCIO's management of SharePoint is consistent with applicable standards. While generally compliant, with respect to the items tested, OPM was not in complete compliance with all standards, as described in section III of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. SECURITY MANAGEMENT

Security management encompasses the policies and procedures that support the OCIO's overall IT security program. We evaluated the OCIO's ability to develop and maintain security policies, manage risk, assign security-related responsibility, and monitor the effectiveness of various system-related controls as they pertain to SharePoint.

1) System Classification

SharePoint was initially implemented on a limited basis within OPM's development and test environment and was not intended for agency-wide use. As the agency's demand for the software increased, OPM expanded the use of SharePoint into its production IT environment and began to load the system with a significant volume of sensitive data. However, as expansion occurred OPM did not assess whether SharePoint had expanded to the point it should be classified as a "major" information system requiring a formal Security Assessment and Authorization (Authorization). In addition, SharePoint is not currently documented on any OPM IT system inventory (i.e., it is not listed as a minor application within the boundary of a separate major information system).

OPM's [redacted] guide states "A new [Authorization] may also be required when there is a significant change to a system or its environment of operation." NIST SP 800-53, Revision 4, requires that "The organization develops and maintains an inventory of its information systems."

Failure to complete an Authorization of an IT system containing sensitive information increases the likelihood of underrepresenting the potential security risk that system faces. The system would not be subject to an independent verification and validation of security controls – a process that almost always identifies significant issues that must be addressed.

Recommendation 1

We recommend that OPM conduct an analysis to determine the appropriate classification of SharePoint as an information system. If it is classified as a major system, OPM should conduct a full Authorization of SharePoint. If it is classified as a minor application, OPM should update the Authorization of the major system that hosts SharePoint to account for its

security control needs and risks. We also recommend that OPM track SharePoint on its system inventories.

OPM Response:

"We concur with the recommendation. OPM will follow its standardized processes for conducting system classification and take appropriate action, in accordance with its policies and procedures, based on the results of the classification."

OIG Comment:

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

2) Policies and Procedures

As stated above, OPM implemented SharePoint in a production environment without subjecting the system to the Authorization process. OPM has not established any policies and procedures specific to SharePoint nor conducted an analysis as to whether the use of SharePoint warrants updating any of OPM's current policies and procedures.

OPM has not established policies and procedures specific to SharePoint.

FISCAM states "Security control policies and procedures should be documented and approved by management." FISCAM also states "Control policies and procedures may be written to be more general at the entity wide level and more specific at the systems (for example, specific configurations) and application levels (for example, user access rules for specific applications)."

Failure to document or update security policies and procedures for a major change or addition to an information system increases the organization's risk to potential threats and hinders its ability to manage and alleviate risk.

Recommendation 2

We recommend that OPM establish policies and procedures to address SharePoint's security controls and the risks associated with operating the software in OPM's production environment.

OPM Response:

"We concur with the recommendation. OPM is working to adapt best practices, to provide governance over SharePoint. The CIO will take appropriate action to develop policies and procedures that address security controls over the application."

3) Specialized Training

OPM currently provides annual IT security awareness training to all agency employees. However, training specific to SharePoint administration and management is not provided or required for SharePoint administrators and/or site owners.[2]

FISCAM states "employees with significant security responsibilities should receive specialized training … ."

Failure to adequately train employees with security responsibilities increases the risk that these individuals would not be prepared to address constantly evolving IT threats, thus increasing the likelihood of the system being compromised.

Recommendation 3

We recommend that OPM require employees with administrative or managerial responsibilities over SharePoint to take specialized training related to the software.

OPM Response:

"We concur with the recommendation. OPM will ensure that individuals with administrative or managerial responsibility over SharePoint have proper training in alignment with their elevated access."

[2] SharePoint administrators are responsible for the overall configuration and security of OPM's SharePoint implementation. Site owners are responsible for managing data and user access within an individual SharePoint site.

B. ACCESS CONTROLS

Access controls are the policies, procedures, and techniques used to prevent or detect unauthorized access to sensitive resources. We examined the logical access controls protecting sensitive information on the SharePoint application as well as its servers and backend databases.

The following sections document opportunities for improvement related to SharePoint's access controls.

1) User Account Provisioning

The process of creating a new SharePoint site begins with a requestor submitting a site access request form to the SharePoint administrator. These request forms are centrally managed within the OCIO, maintained for record retention purposes, and contain the information used to provision access for the site owner's personal account. The process of adding additional users to the sites is managed by the individual site owners, but there is currently no process to document and approve the creation of these accounts. Without a formal access request process, OPM is unable to ensure all of its SharePoint user accounts are configured for least privilege and appropriate segregation of duties, and audited to ensure only required access is maintained.

NIST SP 800-53, Revision 4, states "The organization: … Requires approvals by [organization-defined personnel or roles] for requests to create information system accounts … ."

Failure to document and approve access to information systems increases the risks of unauthorized access and accounts.

OPM could improve its procedures for provisioning SharePoint accounts.

Recommendation 4

We recommend that OPM implement formal procedures for requesting and provisioning SharePoint user accounts.

OPM Response:

"We concur with the recommendation. OPM is working to adapt best practices for requesting and provisioning user accounts within SharePoint. The CIO will take

appropriate action to integrate these requests into current processes for approval and incident tracking."

2) User Account Auditing

As noted above, OPM does not have a formal process in place to document all of the SharePoint user accounts approved and provisioned, and therefore it cannot effectively conduct routine audits to ensure access is being granted, modified, and removed appropriately (i.e., there is no list of approved user access from which to compare the actual user accounts).

NIST SP 800-53, Revision 4, states "The organization: … reviews accounts for compliance with account management requirements … ."

Failure to routinely audit user accounts increases the risk that unauthorized accounts exist or account privileges are misconfigured.

Recommendation 5

We recommend that OPM implement a formal process to routinely audit SharePoint user accounts for appropriateness. This audit should include verifying individuals are still active employees or contractors and their level of access is appropriate.

OPM Response:

"We concur with the recommendation. OPM is working to adapt best practices, to provide governance over SharePoint. The CIO will take appropriate action to develop policies and procedures that address user access controls."

C. CONFIGURATION MANAGEMENT

Configuration management involves the policies and procedures used to ensure that systems are configured according to a consistent and approved risk-based standard. We evaluated OPM's management of the configuration of its SharePoint application, servers, and databases.

The sections below document areas for improvement related to OPM's SharePoint configuration management controls.

1) Security Configuration Standards and Audits

OCIO has not documented formal security configurations standards for its SharePoint application.

The OCIO has not documented formal security configuration standards for its SharePoint application. A security configuration standard is a formally approved document containing details on how security settings should be configured for specific software or operating platforms. Without a configuration standard in place, the OCIO cannot effectively audit its system's security settings (i.e., there are no approved settings to compare against the actual settings).

NIST SP 800-53, Revision 4, states an organization should establish and document "configuration settings for information technology products employed within the information system … that reflect the most restrictive mode consistent with operational requirements . . . . " In addition, NIST SP 800-53, Revision 4, requires an organization to develop, document, and maintain a current baseline configuration of the information system.

Failure to establish approved system configuration settings and to routinely audit the actual settings against this policy increases the risk systems may not be configured in a secure manner.

Recommendation 6

We recommend that OPM document approved security configuration settings for its SharePoint application.

OPM Response:

"We concur with the recommendation. OPM is working to adapt best practices for SharePoint optimization. The CIO will take appropriate action to document the application security configuration settings."

Recommendation 7

We recommend that OPM implement a process to routinely audit the configuration settings of SharePoint to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

OPM Response:

"We concur with the recommendation. OPM is working to adapt best practices for SharePoint optimization. The CIO will take appropriate action to ensure best practice security configurations are in place following OPM's approved application security configuration."

D. VULNERABILITY MANAGEMENT

Vulnerability management is the practice of identifying, classifying, remediating, and mitigating weaknesses in software, and is an integral part of IT and network security. We reviewed OPM's policies and procedures surrounding vulnerability management and performed independent testing of its controls.

1) Patch Management

We conducted credentialed vulnerability and configuration compliance scans on the servers supporting SharePoint. The specific vulnerabilities identified were provided to the OCIO in the form of an audit inquiry, but will not be detailed in this report. The results of our scans indicate that several servers were missing critical patches released more than 90 days before the scans took place that remediate known vulnerabilities. The OCIO's response to our audit inquiry indicated they were aware of these unimplemented patches and the lack of a SharePoint test environment prevents the OCIO from testing patches to identify any adverse effect on the system. Therefore, the OCIO made a risk-based decision to not install many of these patches. However, we believe the risk of leaving a system open to known vulnerabilities outweighs the risk of disrupting the availability and functionality of SharePoint.

NIST SP 800-53, Revision 4, requires organizations to identify, report, and correct information system flaws. It also requires an organization to install security-relevant

software and firmware updates. Failure to remediate vulnerabilities increases the risk hackers could exploit system weaknesses for malicious purposes.

Recommendation 8

We recommend that OPM implement a process to test patches on its SharePoint servers. Once this process has been implemented, we recommend OPM implement controls to ensure all critical patches are installed on SharePoint servers and databases in a timely manner as defined by OPM policies.

OPM Response:

"We concur with the recommendation. OPM is working to appropriately test SharePoint patches before release to production. The CIO will take appropriate action to ensure patches are applied to the current SharePoint instance, following current processes."

APPENDIX

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Chief Information Officer

July 21, 2017

MEMORANDUM FOR [redacted]
CHIEF, INFORMATION SYSTEMS AUDIT GROUP
OFFICE OF THE INSPECTOR GENERAL

FROM: DAVID L. DEVRIES
CHIEF INFORMATION OFFICER

Subject: Office of the Chief Information Officer Response to the Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's SharePoint Implementation (Report No. 4A-CI-00-17-030)

Thank you for the opportunity to provide comments to the Office of the Inspector General (OIG) draft report for the Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's (OPM) SharePoint Implementation. The OIG comments are valuable to the Agency as they afford us an independent assessment of our operations and help guide our improvements to enhance the security of the data furnished to OPM by the Federal workforce, the Federal agencies, our private industry partners, and the public.

We welcome a collaborative dialogue to help ensure we fully understand the OIG's recommendations as we plan our remediation efforts so that our actions and the closure of the recommendations thoroughly address the underlying issues. I look forward to continued discussions during our monthly reviews to help ensure we remain aligned.

Each of the recommendations provided in the draft report is discussed below:

Recommendation 1
We recommend that OPM conduct an analysis to determine the appropriate classification of SharePoint as an information system. If it is classified as a major system, OPM should conduct an Authorization of SharePoint. If it is classified as a minor system, OPM should update the Authorization of the major system that hosts SharePoint to account for its security control needs and risks. We also recommend that OPM track SharePoint on its system

inventories.

Management Response: We concur with the recommendation. OPM will follow its standardized processes for conducting system classification and take appropriate action, in accordance with its policies and procedures, based on the results of the classification.

Recommendation 2
We recommend that OPM establish policies and procedures that address SharePoint security controls and risks associated with operating the software in OPM's production environment.

Management Response: We concur with the recommendation. OPM is working to adapt best practices, to provide governance over SharePoint. The CIO will take appropriate action to develop policies and procedures that address security controls over the application.

Recommendation 3
We recommend that OPM require employees with administrative or managerial responsibilities over SharePoint to take specialized training for the software.

Management Response: We concur with the recommendation. OPM will ensure that individuals with administrative or managerial responsibility over SharePoint have proper training in alignment with their elevated access.

Recommendation 4
We recommend that OPM implement formal procedures for requesting and provisioning SharePoint user accounts.

Management Response: We concur with the recommendation. OPM is working to adapt best practices for requesting and provisioning user accounts within SharePoint. The CIO will take appropriate action to integrate these requests into current processes for approval and incident tracking.

Recommendation 5
We recommend that OPM implement a formal process to routinely audit SharePoint user accounts for appropriateness. This audit should include verification that individuals are still active employees or contractors and that their level of access is appropriate.

Management Response: We concur with the recommendation. OPM is working to adapt best practices, to provide governance over SharePoint. The CIO will take appropriate action to develop policies and procedures that address user access controls.

Recommendation 6
We recommend that OPM document approved security configuration settings for its SharePoint application.

Management Response: We concur with the recommendation. OPM is working to adapt best practices for SharePoint optimization. The CIO will take appropriate action to document the application security configuration settings.

Recommendation 7
We recommend that OPM implement a process to routinely audit the configuration settings of SharePoint to ensure they are in compliance with the approved security configuration standards. Note – this recommendation cannot be implemented until the controls from Recommendation 6 are in place.

Management Response: We concur with the recommendation. OPM is working to adapt best practices for SharePoint optimization. The CIO will take appropriate action to ensure best practice security configurations are in place following OPM's approved application security configuration.

Recommendation 8
We recommend that OPM implement a process to test patches on its SharePoint servers. Once this process has been implemented, we recommend that OPM implement controls to ensure that all critical patches are installed on SharePoint servers and databases in a timely manner as defined by OPM policies.

Management Response: We concur with the recommendation. OPM is working to appropriately test SharePoint patches before release to production. The CIO will take appropriate action to ensure patches are applied to the current SharePoint instance, following current processes.

cc:
[redacted]
Chief Information Security Officer

[redacted]
Acting Director, Security Policy and Governance

[redacted]
Associate Chief Information Officer, Enterprise Infrastructure Solutions

[redacted]
Branch Chief, Server Operations

Mark W. Lambert
Associate Director, Merit Systems Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

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