



**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
GP Plateau Baseline 6 Learning Management System**

**Report Number 4A-HR-00-15-015
July 31, 2015**

-- 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 (<http://www.opm.gov/our-inspector-general>), 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

Audit of the Information Technology Security Controls of the U.S. Office of Personnel Management's GP Plateau Baseline 6 Learning Management System

Report No. 4A-HR-00-15-015

July 31, 2015

Why Did We Conduct the Audit?

The GP Plateau Baseline 6 Learning Management System Portal (GPB6 LMS) is one of the U.S. Office of Personnel Management's (OPM) critical Information Technology (IT) systems. As such, the Federal Information Security Management Act (FISMA) requires that the Office of the Inspector General (OIG) perform an audit of the IT security controls of this system, as well as all of the agency's systems, on a rotating basis.

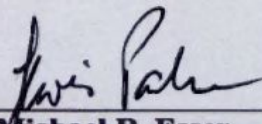
What Did We Audit?

The OIG has completed a performance audit of the GPB6 LMS to ensure that the system owner, Human Resources Solutions (HRS), has managed the implementation of IT security policies and procedures in accordance with the standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information Security Controls Audit Manual and OPM's Office of the Chief Information Officer (OCIO).

What Did We Find?

Our audit of the IT security controls of the GPB6 LMS determined that:

- A valid Authorization to Operate (ATO) was not approved and currently the GPB6 LMS is operating without a valid ATO. This was a contributing factor to a material weakness in OPM's Fiscal Year 2014 FISMA report (4A-CI-00-14-016).
- The security categorization of the GPB6 LMS is consistent with Federal Information Processing Standards 199 and NIST Special Publication (SP) 800-60 requirements, and we agree with the categorization of "moderate."
- The GPB6 LMS System Security Plan contains the critical elements required by NIST SP 800-18 Revision 1.
- A Security Control Assessment Plan and Security Control Report were completed in June and July 2014, respectively, for the GPB6 LMS. However, the scope of the plan and report did not address the entire operating environment.
- HRS has performed regular security control self-assessments of the system in accordance with OPM's continuous monitoring methodology.
- A Contingency Plan was developed for the GPB6 LMS that is in compliance with NIST SP 800-34 Revision 1, and the plan is tested annually.
- A Privacy Threshold Analysis was conducted for the GPB6 LMS that indicated that a Privacy Impact Assessment (PIA) was required. HRS is in the process of finishing the PIA.
- The GPB6 LMS Portal Plan of Action and Milestones (POA&M) has been loaded into Trusted Agent, the OCIO's POA&M tracking tool, but is missing several pieces of information. Additionally, the status of delayed POA&M items was not updated with new scheduled completion dates in accordance with OPM guidance.
- We evaluated the degree to which a subset of the IT security controls outlined in NIST SP 800-53 Revision 4 were implemented for the GPB6 LMS. We determined that a majority of tested security controls appear to be in compliance with NIST SP 800-53 Revision 4. However we did note several areas for improvement.


for Michael R. Esser
Assistant Inspector General
for Audits

ABBREVIATIONS

ATO	Authorization to Operate
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards
FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Management Act
GPB6 LMS	GP Baseline 6 Learning Management System
HRS	Human Resources Solutions
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
PIA	Privacy Impact Analysis
POA&M	Plan of Action & Milestones
SA&A	Security Assessment and Authorization
SAP	Security Assessment Plan
SAR	Security Assessment Report
SP	Special Publication
SSP	System Security Plan

TABLE OF CONTENTS

	<u>Page</u>
ABBREVIATIONS	i
I. BACKGROUND	1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	2
III. AUDIT FINDINGS AND RECOMMENDATIONS	5
A. Security Assessment and Authorization	5
B. FIPS 199 Analysis	6
C. System Security Plan	6
D. Security Assessment Plan and Report	7
E. Continuous Monitoring Self-Assessment	8
F. Contingency Planning and Contingency Plan Testing.....	9
G. Privacy Impact Assessment	9
H. Plan of Action and Milestones Process.....	10
I. NIST SP 800-53 Evaluation.....	11
IV. MAJOR CONTRIBUTORS TO THIS REPORT	16
 APPENDIX: Human Resource Solutions’ May 15, 2015 response to the draft report, issued April 28, 2015	
 REPORT FRAUD, WASTE, AND MISMANAGEMENT	

I. BACKGROUND

On December 17, 2002, President Bush signed into law the E-Government Act (P.L. 107-347), which includes Title III, the Federal Information Security Management Act (FISMA). It requires (1) annual agency program reviews, (2) annual Inspector General (IG) evaluations, (3) agency reporting to the U.S. Office of Management and Budget (OMB) the results of IG evaluations for unclassified systems, and (4) an annual OMB report to Congress summarizing the material received from agencies. In accordance with FISMA, we audited the information technology (IT) security controls related to the U.S. Office of Personnel Management's (OPM) GP Plateau Baseline 6 Learning Management System (GPB6 LMS).

The GPB6 LMS is one of OPM's major IT systems in the Human Resources Solutions (HRS) program office. 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 GPB6 LMS is a web-based employee training platform. The system is designed to provide Federal agencies with an e-learning management system to develop, deliver, and track training for Federal employees. GPB6 LMS is a contractor system managed and operated by GP Strategies in Columbia, Maryland and hosted in a 3rd party data center in Sterling, Virginia.

This was our first audit of the security controls surrounding the GPB6 LMS. We discussed the results of our audit with HRS and GP Strategies representatives at an exit conference.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

Objectives

Our objective was to perform an evaluation of the security controls for the GPB6 LMS to ensure that HRS officials have managed the implementation of IT security policies and procedures in accordance with standards established by FISMA, the National Institute of Standards and Technology (NIST), the Federal Information System Controls Audit Manual (FISCAM) and OPM's Office of the Chief Information Officer (OCIO).

OPM's IT security policies require owners of all major information systems to complete a series of steps to (1) certify that their system's information is adequately protected and (2) authorize the system for operations. The audit objective was accomplished by reviewing the degree to which a variety of security program elements have been implemented for the GPB6 LMS, including:

- Security Assessment and Authorization (SA&A);
- Federal Information Processing Standards (FIPS) 199 Analysis;
- System Security Plan (SSP);
- Security Assessment Plan and Report (SAP) and (SAR);
- Continuous Monitoring Self-Assessment;
- Contingency Planning and Contingency Plan Testing;
- Privacy Impact Assessment (PIA);
- Plan of Action and Milestones Process (POA&M); and
- NIST Special Publication (SP) 800-53 Revision 4 Security Controls.

Scope and Methodology

This performance audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Accordingly, the audit included an evaluation of related policies and procedures, compliance tests, and other auditing procedures that we considered necessary. The audit covered FISMA compliance efforts of HRS officials and GP Strategies' employees responsible for the GPB6 LMS, including IT security controls in place as of March 2015.

We considered the GPB6 LMS 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 HRS program office with GPB6 LMS security responsibilities, interviewed GP Strategies employees, reviewed documentation and system screenshots, viewed demonstrations of system capabilities, and conducted tests directly on the system. We also reviewed relevant OPM IT policies and

procedures, Federal laws, OMB policies and guidance, and NIST guidance. As appropriate, we conducted compliance tests to determine the extent to which established controls and procedures are functioning as required.

Details of the security controls protecting the confidentiality, integrity, and availability of the GPB6 LMS 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 GPB6 LMS 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;
- The Federal Information System Controls Audit Manual;
- NIST SP 800-12, An Introduction to Computer Security;
- NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems;
- NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments;
- NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems;
- NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems;
- NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations;
- NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories;
- NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities;
- FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems; and
- Other criteria as appropriate.

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

The audit was performed by the OPM OIG, as established by the Inspector General Act of 1978, as amended. The audit was conducted from December 2014 through March 2015 in OPM's Washington, D.C. office, and contractor locations in Sterling, Virginia and Columbia, Maryland.

Compliance with Laws and Regulations

In conducting the audit, we performed tests to determine whether HRS's and GP Strategies' practices were consistent with applicable standards. While generally compliant, with respect to the items tested, HRS was not in complete compliance with all standards as described in the "Audit Findings and Recommendations" section of this report.

III. AUDIT FINDINGS AND RECOMMENDATIONS

A. Security Assessment & Authorization

System certification is a comprehensive assessment process, known as SA&A, that attests that a system's security controls are meeting the security requirements of that system, and accreditation is the official management decision to authorize operation of an information system and accept its risks. OMB requirements state that Federal systems must be authorized every three years. NIST SP 800-37 Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems, provides guidance to Federal agencies in meeting security accreditation requirements.

OPM's Fiscal Year 2014 FISMA report (A4-CI-00-14-016) includes a material weakness related to the agency's failure to meet OMB authorization requirements for almost 25% of its major information systems. The GPB6 LMS was one of the OPM systems contributing to this material weakness. The prior authorization for the GPB6 LMS expired in July 2014, and the system does not have a valid SA&A as of the date of this report.

The GPB6 LMS is currently operating without a valid authorization.

Failure to properly authorize a major system means that the program cannot properly manage, mitigate, or accept the security risks for the unauthorized system. As the GPB6 LMS is used by other agencies, the lack of an authorization should be of serious concern to all external parties who utilize this system.

Recommendation 1

We recommend that HRS obtain a valid authorization to operate for GPB6 LMS.

HRS Response:

"We concur. USA Learning® has submitted all of the required documentation to the Chief Information Security Office (CISO) in order to obtain a full authority to operate. We are following the CIO's process to receive the final signed ATO letter."

OIG Reply:

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

B. FIPS 199 Analysis

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

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

The GPB6 LMS FIPS Publication 199 Security Categorization analyzes information processed by the system and its corresponding potential impacts on confidentiality, integrity, and availability. The GPB6 LMS is categorized with a moderate impact level for confidentiality, integrity, and availability, resulting in an overall categorization of “moderate.”

The security categorization of the GPB6 LMS appears to be consistent with FIPS Publication 199 and NIST SP 800-60 requirements, and we do not disagree with the categorization of “moderate.”

C. System Security Plan

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

The SSP for the GPB6 LMS was created using the OCIO’s template that utilizes NIST SP 800-18 Revision 1 as guidance. The template requires that the following elements be documented within the SSP:

- System Name and Identifier;
- System Categorization;
- System Owner;
- Authorizing Official;
- Other Designated Contacts;
- Assignment of Security Responsibility;
- System Operational Status;
- Information System Type;
- General Description/Purpose;
- System Environment;
- System Interconnection/Information Sharing;

- Laws, Regulations, and Policies Affecting the System;
- Security Control Selection;
- Minimum Security Controls; and
- Completion and Approval Dates.

We reviewed the GPB6 LMS SSP and determined that it adequately addresses each of the elements required by NIST. Nothing came to our attention to indicate that the system security plan of the GPB6 LMS has not been properly documented and approved.

D. Security Assessment Plan and Report

A SAP and SAR were completed for the GPB6 LMS in June 2014 and August 2014, respectively, as a part of the system’s SA&A process. The SAP and SAR were completed by Grant Thornton, a contractor that was operating independently from HRS. We reviewed the documents to verify that a risk assessment was conducted in accordance with NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments. We also verified that appropriate management, operational, and technical controls were tested for a system with a “moderate” security categorization according to NIST SP 800-53 Revision 4, Recommended Security Controls for Federal Information Systems.

We reviewed the security assessment results table that contained the detailed results of the independent NIST SP 800-53 Revision 4 controls testing. The table showed that 62 controls were not fully satisfied with 1 being listed as a false positive in the SAR. Thirteen of the weaknesses identified were classified as moderate and 48 were classified as low. The 61 identified control weaknesses were appropriately added to the GPB6 LMS POA&M. (See Section H: Plan of Action & Milestones, below, for further discussion of this topic.)

However, we determined that the SAP did not include the necessary level of detail in listing the specific components of the systems to be tested. The SAP failed to identify specific virtual machines, virtual machine hosts and other network devices that are part of this system. As such, the SAR testing did not cover all of the components of the system inventory. Failure to include the entire infrastructure of the system as part of the testing undermines the assessment results and potentially leads to unidentified risks being accepted by the authorizing official and the agency.

The scope of the GPB6 LMS SAR did not cover the system’s entire inventory.

Recommendation 2

We recommend that HRS update the GPB6 LMS Security Assessment Plan and Report to including all appliances and devices within the system boundary. Any additional weaknesses that are identified should be added to the system’s POA&M.

HRS Response:

“We do not concur. Updating the SAP and SAR with this information is unnecessary as the assessment phase has ended. We do agree that the System Security Plan should be—and has been—updated to include all appliances and devices. The assessment was originally performed by an independent assessor, Grant Thornton, for the period of performance ending in 2014. The missing devices and appliances were identified at the end of the assessment and reported as findings during a review by the CISO’s office. During the OIG assessment, the entire system boundary was scanned and assessed to include the missing devices and appliances. This assessment was provided to the CISO’s Office and accepted as evidence for closure of the existing POA&Ms related to this recommendation. Therefore, updating the SAP and SAR is unnecessary for USALearning® and would incur unnecessary costs (contracted) as the assessment has been finalized.”

OIG Reply:

We continue to recommend that the SAP and SAR be updated to include the entire GPB6 LMS environment. The GPB6 LMS has three main groups in its inventory (Internal Revenue Service servers, Federal Aviation Administration (FAA) servers, and shared infrastructure devices), and two of the three (FAA servers and shared infrastructure devices) were not assessed by the SAP and SAR. Vulnerability scans are not a sufficient replacement for a full security assessment. Furthermore, the OIG vulnerability scans only covered a sample of the appliances and devices in the environment. This recommendation and prior POA&Ms should not be closed until a full security assessment that includes all appliances and devices is conducted.

Recommendation 3

We recommend that the OCIO ensure that HRS update the GPB6 LMS POA&M to reinstate the weaknesses related to the servers and network devices that were not covered by the original SAP and SAR.

HRS Response:

This recommendation was added after the draft report was issued; HRS has not yet had the opportunity to respond.

E. Continuous Monitoring Self-Assessment

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

HRS provided us with evidence that a security controls assessment was conducted in 2013 by HRS personnel. The assessment included a review of some relevant security controls outlined in

NIST SP 800-53 Revision 3. The independent assessment in the SAR conducted in 2014 fulfills the requirement for the annual test.

F. Contingency Planning and Contingency Plan Testing

NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems, states that effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability. OPM's security policies require all major applications to have viable and logical disaster recovery and contingency plans, and that these plans be annually reviewed, tested, and updated.

Contingency Plan

The GPB6 LMS contingency plan documents the functions, operations, and resources necessary to restore and resume the GPB6 LMS operations when unexpected events or disasters occur.

The GPB6 LMS contingency plan adequately follows the format suggested by NIST SP 800-34 Revision 1 and contains the required elements.

Contingency Plan Test

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

A contingency plan test of the GPB6 LMS was conducted in September 2014. The test involved a table top exercise of recovering the system at the backup data center and then returning operations to the regular data center. The testing documentation contained adequate analysis and review of the test results.

G. Privacy Impact Assessment

The E-government Act of 2002 requires agencies to perform a PIA of federal information systems that include or use personally identifiable information. 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. As part of the assessment process, OPM requires a Privacy Threshold Analysis (PTA) to determine which information systems meet the requirements to need a PIA.

HRS completed a PTA of the GPB6 LMS during April 2014 and determined that a PIA was required for this system. HRS has not yet completed an approved PIA for the GPB6 LMS.

Recommendation 4

We recommend that HRS complete a current Privacy Impact Assessment for the GPB6 LMS.

HRS Response:

“We concur. USALearning® has submitted the Privacy Impact Assessment (PIA) to the OPM CISO’s office as required. After the CISO’s office has reviewed the PIA, they will submit it to the Privacy Officer for final approval and signature.”

H. Plan of Action and Milestones Process

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

We evaluated the GPB6 LMS POA&M and it follows the format of OPM’s standard template, but is not complete. The POA&M document has been loaded into Trusted Agent, the OCIO’s POA&M tracking tool, for evaluation. We determined that the weaknesses discovered during the SA&A security assessment were included in the POA&M.

However, the POA&M documentation does not include the following columns of required information: Milestones with Dates, Milestone Changes, Resources Required, and Source of Finding. Failure to include the relevant information in the POA&Ms increases the likelihood of weaknesses not being addressed in a timely manner and therefore exposing the system to malicious attacks exploiting those unresolved vulnerabilities.

In addition, we noted 60 weaknesses on the POA&M that had a status of “delayed” that did not indicate a new scheduled completion date. OPM’s POA&M Standard Operating Procedures state that “If the weakness is not addressed by the scheduled completion date, the new scheduled completion date must be addressed in the Milestone Changes column, along with the updated milestones and dates necessary to achieve the new scheduled completion date.”

Sixty open POA&M weaknesses are in a delayed status and have not been updated

Recommendation 5

We recommend that HRS update the GPB6 LMS POA&M documentation to include all information required by OPM’s POA&M template.

HRS Response:

“We concur. The Trusted Agent FISMA (TAF) system is used to monitor and track POA&Ms. All required information from the GPB6 LMS has been included in OPM’s POA&M template within TAF.”

Recommendation 6

We recommend that HRS update the GPB LMS POA&M to include a new scheduled completion date for all delayed items.

HRS Response:

“We concur. USALearning® has closed several POA&Ms since the completion of the Security Assessment & Authorization (SA&A) and OIG Audit. We will create a new schedule with updated completion dates in accordance with OPM CIO/ISSO policy.”

I. NIST SP 800-53 Evaluation

NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, provides guidance for implementing a variety of security controls for information systems supporting the Federal government. As part of this audit, we evaluated whether a subset of these controls had been implemented for the GPB6 LMS. We tested approximately 40 security controls outlined in NIST SP 800-53 Revision 4 that were identified as being system specific or a hybrid control. Controls identified as common or inherited were omitted from testing because another system or program office is responsible for implementing the control. Furthermore, controls with previously identified weaknesses were also omitted.

We tested one or more controls from each of the following control families:

- Access Control;
- Awareness and Training;
- Audit and Accountability;
- Security Assessment and Authorization;
- Configuration Management;
- Identity and Authentication;
- Incident Response;
- Maintenance;
- Media Protection;
- Physical and Environmental Protection;
- Personnel Security;
- Risk Assessment;
- System and Communications Protection;
and
- System and Information Integrity.

These controls were evaluated by interviewing individuals with GPB6 LMS security responsibilities, reviewing documentation and system screenshots, viewing demonstrations of system capabilities, visiting the hosting site, and conducting tests directly on the system.

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

1. AC-5 Separation of Duties

We reviewed the privileges associated with different groups of users and documented when any one group had too much control over a given process or procedure. There is currently not a technical control preventing [REDACTED]

[REDACTED]

(Related security control CM-5 Access Restrictions for Change)

Recommendation 7

We recommend that HRS implement technical controls that ensure that separation of duties are enforced in the system.

HRS Response:

“We concur. USA Learning® will ensure that the appropriate technical controls are in place and implemented to maintain separation of duties to prevent a user from assuming multiple roles. For example, [REDACTED].”

2. AC-22 Publically Available Content

We discovered sensitive computer configuration and security related information available on the public facing portion of the GPB6 LMS website. For security reasons the specific information discovered will not be discussed in this report but given directly to HRS representatives.

Recommendation 8

We recommend that HRS implement a process to ensure that sensitive information is not publically available on the GPB6 LMS websites.

HRS Response:

“We concur. USA Learning® will notify the vendor and clients about the sensitivity of information available to the public. We will ensure that this information is removed from the public facing web server and will create a schedule to review websites periodically.”

3. RA-5 Vulnerability Scanning

Vulnerability Scans Performed by System Operator

We reviewed the prior vulnerability scans performed on the GPB6 LMS. The prior scans did not appear to include all computers and devices in the entire environment, and therefore vulnerability scanning is not being completed on all components inside the system boundary.

Recommendation 9

We recommend that HRS adjust its current vulnerability scanning process to include the entire system environment, including all virtual machines, hosts, storage, and network devices.

HRS Response:

“We concur. All virtual machines, hosts, storage, and network devices have been updated and have been included as part of the monthly vulnerability scans. We will make a recommendation to the Contracting Office that appropriate language be appended to all future contracts/work orders and BPA calls.”

Vulnerability Scans Performed by OIG - System Patching

We performed automated vulnerability scans on a sample of devices, databases and web applications. The detailed results of the scans were provided to HRS, but for security purposes will not be described in this report. Our scans indicated that critical patches and service packs are not always implemented in a timely manner for the operating platforms supporting the GPB6 LMS.

FISCAM states that “Software should be scanned and updated frequently to guard against known vulnerabilities.” NIST SP 800-53 Revision 4 states that the organization must identify, report, and correct information system flaws and install security-relevant software and firmware updates promptly. (Related security control SI- 2 Flaw Remediation)

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

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

Recommendation 10

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

HRS Response:

“We concur. USALearning® will work with GP Strategies to modify the patch management schedule to ensure timely installation of patches, service packs, and hotfixes as related to their risk rank. This will ensure vulnerabilities to the system are minimized.”

Vulnerability Scans Performed by OIG - Noncurrent Software

Our vulnerability scans indicated that several servers supporting GPB6 LMS contained noncurrent software applications that were no longer supported by the vendors, and have known security vulnerabilities.

FISCAM states that “Procedures should ensure that only current software releases are installed in information systems. Noncurrent software may be vulnerable to malicious code such as viruses and worms.” (Related security control SI- 2 Flaw Remediation)

Failure to promptly remove outdated software increases the risk of a successful malicious attack on the information system.

Recommendation 11

We recommend that HRS implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

HRS Response:

“We concur. USALearning® has contacted vendor (GP Strategies) and requested that all software be reviewed immediately to ensure that current versions are installed. In addition, we are requiring that a system software review be conducted at least quarterly to ensure current versions are obtained and installed on the production servers. Also, we have requested that the software inventory to the SSP be updated to reflect current software versions. We request that contracting language be appended if necessary to enable enforcement by the program office.”

Vulnerability Scans Performed by OIG - Insecure Configurations

Our vulnerability scans indicated that the web application for the GPB6 LMS is insecurely configured in a manner that is susceptible to [REDACTED].

These malicious activities include, but are not limited to:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

Recommendation 12

We recommend that HRS remediate vulnerabilities discovered as a result of the vulnerability scans conducted during this audit.

HRS Response:

“We concur. USA Learning® has responded to each of the recommendations provided by the OIG. The responses outline procedures management must follow to remediate vulnerabilities found during the audit. Remediated vulnerabilities will be reviewed by the CISO’s office for acceptance and documentation.”

IV. MAJOR CONTRIBUTORS TO THIS REPORT

Information Systems Audit Group

[REDACTED], Lead IT Auditor-In-Charge
[REDACTED], Lead IT Auditor
[REDACTED], IT Auditor

[REDACTED], Group Chief

Appendix

OPM Management Response to OIG Draft Audit Reports
GP Plateau Baseline 6 Learning Management System
Report No. 4A-HR-00-15-015
15 May 2015

MEMORANDUM FOR:

[REDACTED]
Chief, Information Systems Audit Group
Office of the Inspector General

FROM:

[REDACTED]
Director, USA Learning®
Human Resources Solutions [REDACTED]

THRU:

Suzanne Logan
Director, Center for Leadership and Development
Human Resources Solutions

Joseph Kennedy
Director, Human Resources Solutions

SUBJECT:

Audit of Information Technology Security Controls
of the U.S. Office of Personnel Management's GP
Plateau Baseline 6 Learning Management System,
Report No. 4A-HR-00-15-01

Thank you for providing us the opportunity to respond to the Office of the Inspector General (OIG) draft report Audit of Information Technology Security Controls of the U.S. Office of Personnel Management's GP Plateau Baseline 6 Learning Management System, 4A-HR-00-15-015.

We recognize that even the most well run programs benefit from external evaluations and we appreciate your input as we continue to enhance our programs. Our responses to your recommendations are provided below.

Recommendation #1: We recommend that HRS obtain a valid authorization to operate for GPB6 LMS.

Management Response

We concur. USA Learning® has submitted all of the required documentation to the Chief Information Security Office (CISO) in order to obtain a full authority to operate. We are following the CIO's process to receive the final signed ATO letter.

Recommendation #2: We recommend that HRS update the GPB6 LMS Security Assessment Plan and Report to include all appliances and devices within the system boundary. Any additional weaknesses that are identified should be added to the system's POA&M.

Management Response

We do not concur. Updating the SAP and SAR with this information is unnecessary as the assessment phase has ended. We do agree that the System Security Plan should be—and has been—updated to include all appliances and devices. The assessment was originally performed by an independent assessor, Grant Thornton, for the period of performance ending in 2014. The missing devices and appliances were identified at the end of the assessment and reported as findings during a review by the CISO's office. During the OIG assessment, the entire system boundary was scanned and assessed to include the missing devices and appliances. This assessment was provided to the CISO's Office and accepted as evidence for closure of the existing POA&Ms related to this recommendation. Therefore, updating the SAP and SAR is unnecessary for USALearning® and would incur unnecessary costs (contracted) as the assessment has been finalized.

Recommendation #3: We recommend that HRS complete a current Privacy Impact Assessment for the GPB6 LMS.

Management Response

We concur. USALearning® has submitted the Privacy Impact Assessment (PIA) to the OPM CISO's office as required. After the CISO's office has reviewed the PIA, they will submit it to the Privacy Officer for final approval and signature.

Recommendation #4: We recommend that HRS update the GPB6 LMS POA&M documentation to include all information required by OPM's POA&M template.

Management Response

We concur. The Trusted Agent FISMA (TAF) system is used to monitor and track POA&Ms. All required information from the GPB6 LMS has been included in OPM's POA&M template within TAF.

Recommendation #5: We recommend that HRS update the GPB LMS POA&M to include a new scheduled completion date for all delayed items.

Management Response

We concur. USALearning® has closed several POA&Ms since the completion of the Security Assessment & Authorization (SA&A) and OIG Audit. We will create a new schedule with updated completion dates in accordance with OPM CIO/ISSO policy.

Recommendation #6: We recommend that HRS implement technical controls that ensure that separation of duties are enforced in the system.

Management Response

We concur. USA Learning® will ensure that the appropriate technical controls are in place and implemented to maintain separation of duties to prevent a user from assuming multiple roles. For example, [REDACTED].

Recommendation #7: We recommend that HRS implement a process to ensure that sensitive information is not publically available on the GPB6 LMS websites.

Management Response

We concur. USA Learning® will notify the vendor and clients about the sensitivity of information available to the public. We will ensure that this information is removed from the public facing web server and will create a schedule to review websites periodically.

Recommendation #8: We recommend that HRS adjust its current vulnerability scanning process to include the entire system environment, to include all virtual machines, hosts, storage, and network devices.

Management Response

We concur. All virtual machines, hosts, storage, and network devices have been updated and have been included as part of the monthly vulnerability scans. We will make a recommendation to the Contracting Office that appropriate language be appended to all future contracts/work orders and BPA calls.

Recommendation #9: We recommend that HRS implement procedures and controls to ensure that servers and databases are installed with appropriate patches, service packs, and hotfixes on a timely basis.

Management Response

We concur. USA Learning® will work with GP Strategies to modify the patch management schedule to ensure timely installation of patches, service packs, and hotfixes as related to their risk rank. This will ensure vulnerabilities to the system are minimized.

Recommendation #10: We recommend that HRS implement a methodology to ensure that only current and supported versions of system software are installed on the production servers.

Management Response

We concur. USA Learning® has contacted vendor (GP Strategies) and requested that all software be reviewed immediately to ensure that current versions are installed. In addition, we are requiring that a system software review be conducted at least quarterly to ensure current versions are obtained and installed on the production servers. Also, we have requested that the

software inventory to the SSP be updated to reflect current software versions. We request that contracting language be appended if necessary to enable enforcement by the program office.

Recommendation #11: We recommend that HRS remediate vulnerabilities discovered as a result of the vulnerability scans conducted during this audit.

Management Response

We concur. USA Learning® has responded to each of the recommendations provided by the OIG. The responses outline procedures management must follow to remediate vulnerabilities found during the audit. Remediated vulnerabilities will be reviewed by the CISO's office for acceptance and documentation.

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact [REDACTED], [REDACTED], or [REDACTED], [REDACTED].

Attachment

cc: [REDACTED]
Human Resources Solutions
Center for Leadership Development
USA Learning® Program Office



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