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

Final Audit Report

Subject:

AUDIT OF THE INFORMATION SECURITY POSTURE OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S USAJOBS SYSTEM FY 2012

Report No. 4A-HR-00-12-037

Date: July 26, 2012

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Audit Report

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION SECURITY POSTURE OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S USAJOBS SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-HR-00-12-037

Date: 07/26/12

Michael R. Esser
Assistant Inspector General
for Audits

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

Office of the
Inspector General

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT

AUDIT OF THE INFORMATION SECURITY POSTURE OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S USAJOBS SYSTEM FY 2012

WASHINGTON, D.C.

Report No. 4A-HR-00-12-037

Date: 07/26/12

The goal of FishNet Security, Inc.'s assessment was to thoroughly document the overall security posture of USAJOBS through a series of tests, to include:

- Network architecture review;
- Internal vulnerability assessment including server and database configuration review;
- External vulnerability and web application assessment;
- Source code review; and
- Mobile application security assessment.

Overall, USAJOBS was found to be in good security standing and does not appear to pose any significant risk to OPM or its constituents. There were no critical vulnerabilities discovered during the multi-discipline assessment that required immediate escalation. Additionally, the large majority of issues found from each assessment phase were of the medium to low/informational severity ranking. Low-severity rated vulnerabilities comprised nearly half of the adverse findings.

FishNet and the OIG believe that there is clear intent by OPM to ensure the confidentiality, integrity, and availability of the USAJOBS environment. Throughout the testing it became obvious that there were some security weaknesses, but nothing that put the USAJOBS environment at immediate risk. Many of the findings are similar to those found in other organizations facing similar operational challenges.

However, throughout the testing of the USAJOBS environment some concerns about the design of the supporting infrastructure were realized. The testers discovered that the domain hosting USAJOBS is shared with other services and applications hosted by OPM's Macon data center.

USAJOBS is widely considered the flagship information system at OPM. Any application with the size, visibility, and public importance of USAJOBS should be operating in a dedicated, multi-tiered environment, thereby creating a defense-in-depth strategy for protecting the confidentiality, integrity, and availability of system resources and data.

Contents

Introduction and Background

USAJOBS is the Federal Government's official one-stop source for Federal jobs and employment information. The USAJOBS website provides public notice of Federal employment opportunities to Federal employees and United States citizens. USAJOBS is cooperatively owned by the Federal Chief Human Capital Officer (CHCO) Council.

In 2003, OPM contracted with Monster Government Services (MGS) to host and maintain the USAJOBS system. In 2010, OPM and the CHCO Council made the decision to not renew its contract with MGS and to bring USAJOBS in-house at OPM. One element of this decision was based on the fact that two separate security breaches at MGS led to the disclosure of sensitive USAJOBS data.

In October 2011, OPM launched USAJOBS 3.0. This new version of USAJOBS was developed by various members of the CHCO council with primary contributions from OPM, the Department of Homeland Security, and the Department of Defense. USAJOBS 3.0 is hosted at OPM's data center in Macon, Georgia.

Objectives

The objectives of this audit were to assess the information security controls of USAJOBS and to evaluate OPM's overall efforts to protect the sensitive data processed by USAJOBS. These objectives were met by reviewing the following elements of USAJOBS:

- Network architecture;
- Internal vulnerabilities including server and database configurations;
- External vulnerabilities and web application;
- Source code; and,
- Mobile application security.

Scope and Methodology

This performance audit was conducted by the Office of the Inspector General (OIG) 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 documented the overall security posture of USAJOBS as of April 2012.

We considered the USAJOBS 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 objectives, we contracted with an information security professional services provider, FishNet Security, Inc. (FishNet) to perform a thorough vulnerability assessment and penetration test of the USAJOBS application and network environment.

Details of the security controls protecting the confidentiality, integrity, and availability of USAJOBS 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 USAJOBS system of internal controls taken as a whole.

The audit was conducted from February through April 2012 in OPM's Washington, D.C. office and FishNet's offices in Herndon, Virginia and Salt Lake City, Utah.

Reporting and Finding Severity

FishNet provided OPM with detailed reports of its findings that referenced specific server names, Internet protocol (IP) addresses, web pages, etc. Due to the highly sensitive nature of FishNet's reports, they will be kept confidential and will not be incorporated into the OIG reporting process.

We submitted a draft audit report to the Office of the Chief Information Officer (OCIO) to elicit their comments on our conclusions. The OCIO provided consolidated comments that included input from two of its divisions: the USAJOBS Program Office that manages the system and the Human Resources Tools and Technology (HRTT) division that supports the system's technical environment. These comments on the draft report were considered in preparing the final report and are attached as the Appendix.

The draft audit report contained an attachment with findings and recommendations related to the specific technical vulnerabilities detected during this audit. Although the attachment does not have the same level of detail as FishNet's reports, it does contain sensitive information and therefore will not be included in this final audit report. Distribution of this document was limited to the USAJOBS program office, the OCIO, and to OPM's Internal Oversight and Compliance Office.

In performing vulnerability assessments and other related work, FishNet's information security assessors rated the severity of its findings. In defining its severity ratings, FishNet combines its own experience from years in the information security professional services industry with widely adopted information assurance industry standards and methodologies in the application of impact ratings to discovered vulnerabilities. The three levels of severity (low, medium, high) are defined below:

- Low – limited impact; confined to a set of resources;
- Medium – tangible impact; potential damage to data and resources; and,
- High – significant impact; probable damage to data and resources.

Compliance with Laws and Regulations

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

Results

The sections below provide a high-level summary of FishNet Security, Inc.'s (FishNet) security vulnerability assessment of OPM's USAJOBS information system. Due to the sensitive nature of the information, the specific findings and recommendations related to the issues identified were communicated separately to the OCIO.

Overall Security Assessment Summary

The goal of FishNet's assessment was to thoroughly document the overall security posture of USAJOBS through a series of tests, to include:

- Network architecture review;
- Internal vulnerability assessment including server and database configuration review;
- External vulnerability and web application assessment;
- Source code review; and
- Mobile application security assessment.

Overall, USAJOBS was found to be in good security standing and does not appear to pose any significant risk to OPM or its constituents. There were no critical vulnerabilities discovered during the multi-discipline assessment that required immediate escalation. Additionally, the large majority of issues found from each assessment phase were of the medium to low/informational severity ranking. Low-severity rated vulnerabilities comprised nearly half of the adverse findings.

FishNet detected three vulnerabilities that it believes warrant a high-severity vulnerability rating. Of these three high-severity vulnerabilities, two dealt with the problem of improper input validation; one instance on the main USAJOBS website and one on the iOS mobile application. The other high-severity vulnerability related to parameter-based redirection that could lead a user to a malicious website. Therefore it could be reasonably said that only two significantly distinct high-severity vulnerabilities were encountered.

Concerning remediation efforts, the vast majority of issues encountered with USAJOBS are considered to be of a minimal level of effort (LOE) to correct. The highest LOE vulnerability was concerned with the overall topology of the USAJOBS application, and in FishNet's and the OIG's opinions, ranks among the most significant findings. While immediate attention should be paid to the two distinct high-severity vulnerabilities, we believe that OPM should also not wait to address what appears to be an undesirable shared infrastructure and move to a dedicated, segregated topology, which cleanly separates the development and production environments.

FishNet and the OIG believe that there is clear intent by OPM to ensure the confidentiality, integrity, and availability of the USAJOBS environment. Throughout the testing it became obvious that there were some security weaknesses, but nothing that put the USAJOBS environment at immediate risk. Many of the findings are similar to those found in other organizations facing similar operational challenges.

The results of each element of this security assessment are outlined below.

OCIO Response:

"The USAJOBS Program Office and HRTT have identified the following points of clarification:

- ***Low-severity rated vulnerabilities and informational items comprised more than half of the adverse findings reported by the independent assessor.***
- ***The independent assessor stated that the overall security of USAJOBS was sound and a credit to the organization's security assessment and authorization process and the hard work of the personnel involved. In addition, the assessor noted that the mobile application was designed and implemented as securely as can reasonably be achieved on a mobile platform.***
- ***At the conclusion of the multi-discipline assessment, the USAJOBS environment had no security weaknesses that put the system assets, OPM, or the public at immediate risk. The identified findings are similar to those found in other organizations facing similar operational challenges."***

OIG Reply:

We acknowledge the work that the USAJOBS Program Office and HRTT have done to secure the USAJOBS system. We would also like to highlight the fact that the Program Office and HRTT have already remediated many of the specific audit recommendations that were outlined in the draft report, including all three related to high-severity vulnerabilities.

The OCIO's comments in response to our draft report (see Appendix) reference the number of audit recommendations that have been successfully implemented since the draft report was issued. Please note that the number of recommendations that we list in this report as remaining open does not exactly match the number referenced by the OCIO in the Appendix. All discrepancies are the result of either 1) the OIG requesting additional evidence or monitoring before supporting closure of the recommendation, or 2) the OIG supporting closure of a recommendation based on the OCIO's acceptable use of the "risk acceptance" process.

A. Network Architecture

Throughout the testing of the USAJOBS environment some concerns about the design of the supporting infrastructure were realized. The testers discovered that the domain hosting USAJOBS is shared with other services and applications hosted by OPM's Macon data center. There were questions about how segregated the application environments actually were based on the shared network address among the DMZ, Private, and OPM-MACON environments. Further analysis showed the integration of the USAJOBS test and development systems within the different environments.

This lack of segregation lends itself to a higher probability of data leakage, unauthorized access to sensitive data, or conflicts of interest between the development team and the production environment. It is critical to consider the interconnectivity of the different

application environments and ensure that user, administrative, and role-based access is granted based on least privilege and separation of duties.

USAJOBS is widely considered the flagship information system at OPM. Any application with the size, visibility, and public importance of USAJOBS should be operating in a dedicated, multi-tiered environment. A multi-tiered environment helps ensure that access to the appropriate resource is granted to the appropriate requestor. It seeks to separate the front-end, mid-level, and back-end services, thereby creating a defense-in-depth strategy for protecting the confidentiality, integrity, and availability of system resources and data.

In addition to segregating the USAJOBS environment, we recommend that OPM analyze what other information systems hosted at the Macon data center warrant segregation, with particular attention paid to Employee Express (a large payroll/personnel system used throughout the federal government).

OCIO Response:

"The USAJOBS web site was designed and deployed as a multi-tiered system to include a web service tier (front-end), application tier (mid-level), and database tier (back-end services). The tiers are separated across logical networks and segregation is enforced by dedicated security service devices (firewalls) with defined network traffic management rules.

A plan has already been developed to further segregate the Macon private network into application specific networks for the major hosted applications and will define separate development/test environment networks for those applications."

OIG Reply:

We agree that OPM's network environment has adequate firewall protection from external threats. However, the current firewall structure does not adequately protect USAJOBS from internal threats. We will continue to monitor the OCIO's efforts to further segregate the USAJOBS environment.

B. Internal Network Assessment

The internal network assessment was performed using a variety of automated tools and manual techniques to determine potential threats to the USAJOBS environment from an attacker with access to OPM's network.

This review covered a specific subset of USAJOBS servers, databases, and network infrastructure. The process consists of the four phases described below:

- Mapping and Target Analysis - determined the USAJOBS visibility from the internal perspective, both as an unauthenticated user and a fully authenticated administrative user, correlated differences between the user types, and identified potential vulnerabilities.

This phase provided insight into both the potential of a successful attack and the likelihood that system administrators would detect such an attack.

- Vulnerability Measurement and Data Collection - the exploitation of network and system vulnerabilities to systematically measure the secure state of the overall environment. The vulnerability data was measured and recorded for each system tested while making every effort to not cause disruption or interference to the systems being probed.

- Data Analysis and Security Design Review - compared test results with operational and security policy requirements to identify deficiencies and develop recommendations.

- Report and Recommendations - provides OPM with an assessment of the existing security posture and actions to be taken to improve any deficiencies.

FishNet's internal network assessment identified five medium-severity and two low-severity vulnerabilities. It is important to note that FishNet categorizes individual findings. For example, three systems each having three missing security patches would be documented into a single "Missing Patch" finding.

Many of the findings in this section revolved around the concepts of patching and account management. These are on-going challenges for nearly all organizations since the IT systems and users that support operations are continuously changing. It is for this reason that these areas undergo a high level of scrutiny to ensure that account credentials do not exceed the necessary level of access and that account credentials are changed periodically, even for service accounts.

OCIO Response:

The OCIO provided the OIG with descriptions and evidence of the work it has done to implement the audit recommendations related to the internal network assessment.

OIG Reply:

We acknowledge that the OCIO has successfully remediated four medium and two low-severity findings. Only a single medium-severity finding remains open in this section. The OCIO has taken steps to address this recommendation, and we have asked for additional evidence before supporting closure of this item.

C. External Network and Web Application Assessment

The external network and web application assessment was performed using a variety of automated tools and manual techniques to determine the potential threat to the USAJOBS environment from an external threat perspective. FishNet's external assessment followed the same four-phase approach described in the internal assessment section above.

The external network assessment identified one high-severity, three medium-severity, eight low-severity and two informational findings.

The high-severity vulnerability relates to a USAJOBS parameter which is not validated by the application. A malicious user would be able to launch a phishing attack to trick a user to follow a crafted URL to a site of their choosing. For example, the malicious site could prompt the user to re-enter their USAJOBS username and password and thereby provide the user's credentials to the attacker.

One medium-severity vulnerability relates to several web pages on the webadmin site that do not validate a user's role. This permits a user to execute application logic that is beyond their role to execute. USAJOBS also utilizes a third party survey service whose administration pages are not appropriately secured. Two session cookies were also identified which do not set the secure flag. Not setting the secure flag permits the session cookie to be transmitted to unencrypted portions of the site over the Internet.

Several low-severity findings relate to an attacker's ability to enumerate valid user accounts and session cookies not being bound to a user's IP address.

OCIO Response:

The OCIO provided the OIG with descriptions and evidence of the work it has done to implement the audit recommendations related to the external network and web application assessment.

OIG Reply:

We acknowledge that the OCIO has successfully remediated one high, one medium, and four low-severity findings. Two medium and four low-severity findings remain open in this section. These open items are either prioritized for upcoming releases of USAJOBS or pending a program office decision of remediation or risk acceptance.

D. Source Code Review

The source code review was conducted by a manual review of the USAJOBS code base and by using IBM's AppScan Source Edition, a leading commercial static code analysis tool. FishNet manually reviewed all AppScan Source Edition results to validate findings and eliminate false positives.

During the source code review, FishNet identified one high-severity, three medium-severity, and three low-severity vulnerabilities.

The high-severity vulnerability relates to a systemic lack of input validation and output encoding, including two pages vulnerable to a cross-site scripting (XSS) attack. Exploitation of this vulnerability would require the attacker to send USAJOBS users a phishing email containing a link with the malicious code attached.

The medium-severity findings are comprised of the ability to lockout a user account through the forgot-password functionality, and internal credentials being stored insecurely. These issues may expose USAJOBS and its users to other types of attacks but do not result in direct compromise.

The low-severity findings include the disclosure of sensitive information, insufficient randomization generating some encryption tokens, and some pages including unnecessary HTML comments.

OCIO Response:

The OCIO provided the OIG with descriptions and evidence of the work it has done to implement the audit recommendations related to the source code review.

OIG Reply:

We acknowledge that the OCIO has successfully remediated all but one medium and one low-severity finding in this section. Of these two remaining findings, one is prioritized for an upcoming release of USAJOBS and the other is pending a program office decision of remediation or risk acceptance.

E. Mobile Application Assessment

The mobile application security assessment of the USAJOBS iOS application was focused on identifying potential security vulnerabilities that, if unresolved, might undermine the security of the USAJOBS system. FishNet assessed the USAJOBS iOS application using both an unauthenticated (i.e., "external hacker") scenario as well as an authenticated (i.e., "malicious user") scenario.

The mobile assessment identified one high-severity, two medium-severity and three low-severity vulnerabilities.

The high-severity issue identified relates to a lack of input validation or output encoding on user input before it is passed back to the backend web service. This is the same high-severity issue identified on the main USAJOBS application during the source code review. This vulnerability, also known as XML Injection, may be used by an attacker to further escalate their attempts at subverting any protections built into the application. At a minimum, it causes multiple requests to be made to the backend web service and interrupts the flow of the application.

The medium-severity vulnerabilities relate to the exposure of configuration information for the backend web services and the ability for attackers to guess valid usernames using the USAJOBS iOS backend web service through the error messages returned due to account lockout. All medium-severity issues should be reviewed in terms of user experience to determine if the sensitivity of the information requires additional protections to be used.

The low-severity vulnerabilities are weaknesses within the application that may give an attacker a foothold to limited amounts of user or architectural information. None currently allow the compromise of the USAJOBS iOS application, but may help an attacker in targeting application users. These vulnerabilities include the exposure of application usernames to attackers with physical access to the iOS device, the lack of an automatic session timeout, and the exposure of platform information on backend web service requests.

OCIO Response:

The OCIO provided the OIG with descriptions and evidence of the work it has done to implement the audit recommendations related to the mobile application assessment.

OIG Reply:

We acknowledge that the OCIO has successfully remediated all but one low-severity finding in this section. Remediation of this last finding is pending a program office decision of remediation or risk acceptance.

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

Appendix

MEMORANDUM FOR: [redacted]
Chief, Information Systems Audits Group

FROM: MATTHEW E. PERRY
Chief Information Officer
USAJOBS 3.0 Authorizing Official

SUBJECT: Response to Draft Report:
Audit of the Information Security Posture of the U.S. Office of Personnel Management's USAJOBS System (Report No. 4A-HR-00-12-037)

The Office of Personnel Management (OPM) USAJOBS Program Office and Human Resource Tools and Technology (HRTT) division acknowledge and appreciate the work of the Office of Inspector General (OIG) and the independent assessor to identify potential information security risks and opportunities to improve the security posture of the USAJOBS information system. This memo serves as official response to the draft report content.

Overall Security Assessment Summary

The USAJOBS Program Office and HRTT have identified the following points of clarification:

- Low-severity rated vulnerabilities and informational items comprised more than half of the adverse findings reported by the independent assessor.
- The independent assessor stated that the overall security of USAJOBS was sound and a credit to the organization's security assessment and authorization process and the hard work of the personnel involved. In addition, the assessor noted that the mobile application was designed and implemented as securely as can reasonably be achieved on a mobile platform.
- At the conclusion of the multi-discipline assessment, the USAJOBS environment had no security weaknesses that put the system assets, OPM, or the public at immediate risk. The identified findings are similar to those found in other organizations facing similar operational challenges.

Network Architecture

The USAJOBS web site was designed and deployed as a multi-tiered system to include a web service tier (front-end), application tier (mid-level), and database tier (back-end services). The tiers are separated across logical networks and segregation is enforced by dedicated security service devices (firewalls) with defined network traffic management rules.

A plan has already been developed to further segregate the Macon private network into application specific networks for the major hosted applications and will define separate development/test environment networks for those applications.

Internal Network Assessment

The current remediation status of documented findings is as follows:

- Four (4) recommendations have been implemented to remediate findings. Corresponding evidence has been provided to the OIG.
- One (1) recommendation is related to a previously identified and mitigated issue regarding patching of embedded non-Microsoft third party software. Evidence of mitigation has been provided to the OIG.
- Two (2) recommendations require further analysis to determine the feasibility of full implementation.

HRTT patches non-Microsoft software products within the USAJOBS system unless doing so would severely compromise system performance and availability. When patching cannot be achieved due to technical constraints, compensating controls are deployed to mitigate risk. It is more accurate to state that formal patch management policy and standard operating procedures should be expanded to include patching and updating non-Microsoft technologies supporting USAJOBS.

External Network and Web Application Assessment

The current remediation status of documented findings is as follows:

- Five (5) recommendations have been implemented to remediate findings. Corresponding evidence has been provided to the OIG.
- Five (5) recommendations are partially implemented or planned for a future release.
- Two (2) recommendations require further analysis to determine the feasibility of full implementation.
- Duplicate recommendations from other sections of the report have been noted.

Source Code Review

The current remediation status of documented findings is as follows:

- Five (5) recommendations have been implemented to remediate findings. Corresponding evidence has been provided to the OIG.
- One (1) recommendation is planned for a future release.
- One (1) recommendation requires further analysis to determine the feasibility of full implementation.

Mobile Application Assessment

The current remediation status of documented findings is as follows:

- Three (3) recommendations are planned for a future release.
- Three (3) recommendations require further analysis to determine the feasibility of full implementation.
- Duplicate recommendations from other sections of the report have been noted.