Audit Report

FY 2011 OFFICE OF INSPECTOR GENERAL FISMA AUDIT OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A110160/O/F/F11008

September 28, 2011

Office of Inspector General
General Services Administration

Office of Audits

FY 2011 OFFICE OF INSPECTOR GENERAL FISMA AUDIT OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A110160/O/F/F11008

September 28, 2011

Date: September 28, 2011

To: Casey Coleman
Chief Information Officer (I)

Reply to Attn of: Carolyn Presley-Doss
Deputy Assistant Inspector General for Finance and Information Technology Audits (JA-F)

Subject: FY 2011 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program, Report Number A110160/O/F/F11008

The General Services Administration's (GSA's) Information Technology (IT) Security Program provides guidance and conducts oversight of efforts to protect GSA systems. The Federal Information Security Management Act of 2002 (FISMA) directs Inspectors General (IGs) to perform an annual independent evaluation of their respective Agency's information technology security program and controls for select systems. This audit report presents the results of the Office of Inspector General's fiscal year (FY) 2011 audit of GSA's IT Security Program and reflects results from three system security audits conducted during the year and other tests. Appendix A provides the objective, scope, and methodology for the audit.

According to FISMA, the Office of Management and Budget (OMB) is responsible for summarizing the results of agency evaluations in a report to Congress. For FY 2011 reporting, IGs are required to assess Agency information security performance in key areas, including risk management, configuration management, security training, incident response and reporting, and identity and access management.

RESULTS OF AUDIT

GSA's Chief Information Officer (GSA-CIO) continues to take steps to improve the Agency-wide IT Security Program. For example, the GSA-CIO has updated GSA's IT Security Policy, published procedural guidance on a variety of information security topics, and expanded the IT Security Program to include additional technical testing requirements. However, we found that additional steps are needed to strengthen GSA's IT Security Program in five key areas: (1) configuration management, (2) social media technologies, (3) security documentation labeling, (4) contractor background investigations, and (5) warning banners.

Further Expansion of Technical Testing Processes Could Improve Configuration Management

Continued improvements are needed to better secure GSA systems and data. In particular, in the two systems that we were able to test,[1] we identified weaknesses relating to security misconfigurations and unpatched database or operating system software. As a result, these systems and their sensitive data were placed at an increased risk of inappropriate access, modification, or destruction.

Weaknesses occurred because system security officials did not ensure that GSA's IT Security Policy requirements for baseline configuration were initially applied and maintained with enough rigor. Additionally, GSA does not require authenticated operating system testing. Our authenticated operating system testing identified multiple weaknesses. Finally, language in GSA's IT Security Policy conflicts with other GSA guidance, which outlines management's IT security responsibilities regarding technical testing frequency requirements. For one of the systems, GSA officials did not conduct quarterly database scanning due to the conflicting requirements. GSA's IT Security Policy requires all information systems to be securely hardened and patched while in operation. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53[2] requires organizations to configure the security settings of IT systems to the most restrictive mode consistent with operational requirements.

Additional Oversight of GSA's Use of Public Social Media Technologies Would Reduce Risks

GSA is implementing social media technologies to communicate with the public to meet goals for a government that is more citizen-centered, transparent, participatory, and collaborative. We reviewed two public GSA social media websites and identified areas needing additional oversight and monitoring to better manage IT security risks.

The first website reviewed was a wiki[3] that was the target for spam postings.[4] These spam postings were available for several months prior to our identification. This website was based on the same platform as a previously identified GSA social site targeted with spam. Additionally, the site allowed new posts to be published without prior review by GSA. Automated programs and malicious users could post inappropriate information in the same manner. According to NIST SP 800-44,[5] these postings "can affect the organization's image where visitors view the

[1] We conducted technical testing for two of the three systems reviewed. We were able to fully conduct technical testing for one system. For the second system, we were able to conduct limited technical testing, but were restricted by the contractor providing the system from performing authenticated operating system testing. For the third system, we were unable to perform any technical testing due to restrictions placed upon us by the contractor providing the system.

[2] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems, Rev. 3,* August 2009

[3] A wiki is a piece of server software that allows users to freely create and edit web page content using any web browser. A wiki supports hyperlinks and has a simple text syntax for creating new pages and crosslinks between internal pages on the fly.

[4] Spam postings are unsolicited bulk messages that often contain malware. Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

[5] NIST SP 800-44, *Guidelines on Securing Public Web Servers, Version 2,* September 2007

submitted content as an endorsement. They may also affect the Web site's availability by making it difficult for users to find necessary content." GSA's social media guidance requires website administrators to "review all comments before posting them." Lack of consistent and scheduled reviews of GSA's public sites may lead to late discoveries of such issues, which may cause reputation and data loss. Further, while this site was included as part of the quarterly reviews of social media websites conducted by the GSA-OCIO, these reviews were not rigorous enough to discover the spam postings.

The second website review identified a configuration weakness that placed the confidentiality of users' private communications at risk. This occurred because system officials did not follow GSA's guidance for web application security. Additionally, this site was not included in the GSA-OCIO's quarterly reviews of social media websites.

A common cause of the identified problems was that both GSA's social media guidance and GSA's IT security guidance do not address security risks to social media platforms. For example, NIST SP 800-44 identifies methods for controlling the impact of spambots[6] in web applications. Additionally, GSA's IT security guidance and social media guidance do not reference each other.

Additional Guidance for Labeling Security Documentation Would Reduce the Risk of Inappropriate Disclosure

During the course of our audits, we identified sensitive documents on a public GSA website, including IT security documentation that placed GSA systems and data at increased risk. The documents lacked restrictive labeling, such as "Controlled Unclassified Information." Excluding guidance for procuring contractor systems, GSA's IT Security Policy and other guidance do not include specific requirements for labeling security documentation for all GSA systems. According to NIST SP 800-53, the organization must protect system security documentation, as required. GSA determined that these documents should not have been disclosed.

Specific Guidance for Conducting Government Background Investigations for Contractors Using Commercial Systems Would Reduce Risk

Contractor personnel supporting two of the contractor systems we reviewed had not undergone government background investigations despite contract and GSA policy requirements. Instead, the contractors conducted background investigations using their internal criteria that did not include all aspects of a government background investigation. Government background investigations are necessary to ensure that contractor personnel are suitable to access GSA systems and data.

Government background investigations were not completed because GSA system officials did not identify individuals requiring background investigations. Additionally, GSA lacks specific

[6] Spambots are an example of web bots which are software applications used to collect, analyze, and index web content. More specifically, spambots crawl web sites for login forms to create free e-mail addresses from which to send spam or to spam blogs, guestbooks, wiki, and forums to boost the search engine rankings of a particular web site.

guidance to assist GSA system officials in identifying personnel requiring government background investigations.

Enhanced Monitoring of Warning Banners Would Aid in Consistent Implementation of Policy

All three reviewed systems deviated from GSA's IT Security Policy regarding warning banners. Two systems displayed warning banners on their main login page that were inconsistent with GSA requirements. The third system did not include any warning banner on its main login page. Warning banners are important since they caution individuals with malicious intent of the potential legal ramifications of their act. According to GSA's IT Security Policy, all systems must display an approved warning banner to all users attempting to access the systems. The GSA-CIO has not provided adequate oversight to ensure appropriate warning banners are in place.

RECOMMENDATIONS

To improve GSA's IT Security Program and to ensure the security of GSA systems, data, and operations, we recommend that the GSA-CIO take actions to:

1. Strengthen configuration management practices by:
    a. Ensuring that authenticated operating system testing is conducted for all GSA systems.
    b. Updating the GSA IT Security Policy and related guidance to clarify technical testing frequency requirements.
2. Improve security of GSA's social media technologies by:
    a. Updating GSA's guidance, including policies, for social media and IT security to address risks specific to social media.
    b. Strengthening the existing reviews of GSA's social media sites to ensure that the inventory is complete and the risks identified in this report are addressed.
    c. Establishing IT security standards for social media platforms widely used at GSA.
3. Clarify labeling requirements for GSA's sensitive security documentation.
4. Improve personnel security of commercial systems used to provide government services by:
    a. Developing guidance to assist GSA system officials in identifying contractor personnel in positions that require government background investigations.
    b. Monitoring whether GSA system officials are adhering to this guidance.
5. Ensure that appropriate warning banners are displayed.

MANAGEMENT COMMENTS

The GSA-CIO concurred with the findings and recommendations outlined in this report. A copy of the GSA-CIO's comments is included in its entirety in Appendix B.

INTERNAL CONTROLS

This audit included a review of elements of GSA's IT Security Program including select management, operational, and technical controls for three GSA systems. We did not test all controls across GSA. The Results of Audit and Recommendations sections of this report state, in detail, the need to strengthen specific processes and controls established within the GSA IT Security Program.

We would like to express our thanks to the GSA-OCIO for their assistance and cooperation during this audit. Please contact me if you have any questions regarding this report.

William Salamon
Audit Manager
Finance and Information Technology Audit Office (JA-F)

APPENDIX A – OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine if the General Services Administration (GSA) has developed, documented, and implemented an Agency-wide information security program. To address this objective we:

- Reviewed policies, procedures, technical guides, and standards established within GSA's IT Security Program.
- Assessed the implementation of GSA's IT Security Program for three select GSA systems. For these systems, we conducted security audits to determine whether management, operational, and technical controls had been implemented to effectively manage risks.
- Met with GSA IT security officials in the Office of the GSA Chief Information Officer, Federal Acquisition Service, and Public Buildings Service.
- Evaluated the implementation of information security program elements from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers*, October 2006.
- Applied the NIST Federal Information Processing Standards Publications and SP 800 series security guidelines.
- Utilized applicable information security regulations, policies, and guidance.
- Examined system certification and accreditation packages, including system risk assessments, security plans, security assessment results, contingency plans, and plans of action and milestones.
- Conducted operating system, database, and web application security testing for the select systems we reviewed.
- Reviewed security controls for two of GSA's public social media websites.
- Reviewed publicly released documents and GSA policies and procedures related to labeling of sensitive security documents.

We conducted this performance audit in accordance with generally accepted government auditing standards between January and August of 2011. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

APPENDIX B – MANAGEMENT COMMENTS

GSA

GSA Office of the Chief Information Officer

September 20, 2011

MEMORANDUM FOR CAROLYN PRESLEY-DOSS
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
FINANCE AND INFORMATION TECHNOLOGY AUDITS (JA-F)

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)
9/20/2011

X Casey Coleman
CASEY COLEMAN
Chief Information Officer

SUBJECT: Draft FY 2011 Office of Inspector General FISMA Audit of GSA'S Information Technology Security Program Report Number A110160/O/F/

This is in response to the OIG draft audit on FY 2011 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program.

My staff has reviewed the draft audit report and we concur with your audit findings and recommendations.

If you or your staff have any questions or require additional information, please contact Kurt Garbars, on 202-208-7485.

U.S. General Services Administration
1275 First Street NE
Washington, DC 20417
Telephone: (202) 501-1000
www.gsa.gov

FY 2011 OFFICE OF INSPECTOR GENERAL
FISMA AUDIT OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A110160/O/F/F11008

APPENDIX C – REPORT DISTRIBUTION

	Copies*
GSA Chief Information Officer (I)	1
Senior Agency Information Security Officer (IS)	1
Director, GAO and IG Audit Response Branch (BCBB)	1
Assistant Inspector General for Auditing (JA)	1
Director, Audit Planning, Policy, and Operations Staff (JAO)	1
Deputy Assistant Inspector General for Investigations (JID)	1

*Provided Electronically