Office of Audits
Office of Inspector General
U.S. General Services Administration

FY 2012 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program

Report Number A120125/O/F/F12005
September 28, 2012

Office of Audits
Office of Inspector General
U.S. General Services Administration

REPORT ABSTRACT

OBJECTIVE

The objective of this audit was to determine if GSA developed, documented, and implemented a comprehensive agency-wide information security program that addresses risks in the current information technology environment. If not, what additional actions are needed to strengthen GSA's Information Technology Security Program and protect the confidentiality, integrity, and availability of GSA's systems and data?

Finance & Information Technology Audit Office
1275 First Street, NE, Room 227
Washington DC 20002
202-357-3620

FY 2012 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program

Report Number A120125/O/F/F12005
September 28, 2012

WHAT WE FOUND

We identified the following during our audit:

Finding 1 – Systems faced increased threats because security patching for high-risk vulnerabilities were not performed timely.

Finding 2 – For newly deployed systems, PBS lacks procedures to ensure that system officials will be able to recover data and restore the system in the event of a contingency.

Finding 3 – The Office of the Chief Information Officer (OCIO) lacks comprehensive guidance for the secure development of mobile applications to mitigate mobile threats.

WHAT WE RECOMMEND

Based on our audit findings we recommend the GSA Chief Information Officer (CIO):

1. Conduct additional oversight of patch management implementations to ensure that system officials are addressing vulnerabilities on GSA systems in a timely manner.
2. Work with PBS to ensure that PBS develops and implements a process for testing the restoration of system backups before new systems are deployed.
3. Create guidance to assist GSA system officials in securely developing applications for mobile platforms.

MANAGEMENT COMMENTS

Management agreed with our findings and recommendations. The GSA CIO's complete response is presented in ***Appendix B***.

Office of Audits
Office of Inspector General
U.S. General Services Administration

DATE: September 28, 2012

TO: Casey Coleman
Chief Information Officer (I)

FROM: William Salamon
Audit Manager, (JA-F)

SUBJECT: FY 2012 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program
A120125/O/F/F12005

This report presents the results of our FY 2012 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program. Our findings and recommendations are summarized in the Report Abstract. Instructions regarding the audit resolution process can be found in the email that transmitted this report.

Your written comments to the draft report are included in ***Appendix B*** of this report.

If you have any questions regarding this report, please contact me or the Auditor-in-Charge at the following:

William Salamon	Audit Manager	william.salamon@gsaig.gov	(202) 357-3634
Terry Williams	Auditor-in-Charge	terry.williams@gsaig.gov	(202) 357-3641

On behalf of the audit team, I would like to thank you and your staff for your assistance during this audit.

Table of Contents

Introduction

The General Services Administration's (GSA) Information Technology (IT) Security Program provides guidance and oversight to protect GSA systems and data. The Federal Information Security Management Act of 2002 (FISMA) directs Inspectors General 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 2012 audit of GSA's IT Security Program and reflects results from evaluations of four selected systems conducted during the year by our office.

According to FISMA, the Office of Management and Budget is responsible for summarizing the results of agency evaluations in a report to Congress. For fiscal year 2012 reporting, Inspectors General are required to assess agency information security performance in key areas, including risk management, configuration management, remote access management, incident response and reporting, and identity and access management.

The objective of this audit was to determine if GSA developed, documented, and implemented a comprehensive agency-wide information security program that addresses risks in the current IT environment. If not, what additional actions are needed to strengthen GSA's IT Security Program and protect the confidentiality, integrity, and availability of GSA's systems and data?

See ***Appendix A*** – Purpose, Scope, and Methodology for additional details.

Results

Finding 1 – Systems faced increased threats because security patching for high-risk vulnerabilities were not performed timely.

During the course of our audits, three of the systems we reviewed did not implement system security patches to address vulnerabilities consistent with GSA requirements. The identification and remediation of known security threats via security patches attempts to prevent vulnerabilities from being exploited and compromised. Oftentimes, vendors are proactive in developing and releasing fixes to known vulnerabilities to the public. To prevent exploitation, GSA system officials must ensure that they capture all relevant fixes as they are released, test their implementation for adverse effects, and implement them, if deemed appropriate, after testing is concluded. GSA requires all high-risk vulnerabilities to be mitigated within 30 days. For two systems, timely patching was not completed because the organizations managing them have developed and implemented patch management processes that exceeded GSA requirements, allowing system officials 60 days or more to resolve vulnerabilities. The third system had not completed adequate vulnerability scanning, resulting in multiple database patching-related vulnerabilities dating back to 2009.

Finding 2 – For newly deployed systems, PBS lacks procedures to ensure that system officials will be able to recover data and restore the system in the event of a contingency.

PBS does not have assurance that newly deployed systems are recoverable from backup media. According to the National Institute of Standards and Technologies (NIST) Special Publication (SP) 800-53, system officials must test backup information to verify media reliability and information integrity.[1] However, PBS does not ensure that each system is tested in the environment before they are deployed. Instead, PBS identifies common platforms (operating systems and corresponding databases) throughout the organization and annually tests one system for each standardized platform as a representative sample. Residual risk remains to newly deployed systems, since PBS lacks procedures to ensure that backups are properly written to disks or that other recovery methods are working prior to deployment.

Backups are performed primarily for recovery purposes and therefore serve one of the key elements of contingency planning. Without adequate testing, PBS has to rely on backup methods that have not been tested to verify the reliability and integrity of the information to be restored for newly deployed systems. If these backup methods fail, administrators would be unable to perform system restoration.

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

Finding 3 – The OCIO lacks comprehensive guidance for the secure development of mobile applications to mitigate mobile threats.

GSA has developed five custom mobile applications that it makes available to the public. However, the GSA Office of the Chief Information Officer (OCIO) does not have a specific policy or other guidance for the secure development of custom mobile applications. Specifically, the GSA OCIO does not outline the required controls and assessments that system security officials should perform to ensure that mobile applications (for both public and internal use) are secure before being put into operation. Instead of developing and enforcing pre-defined security requirements, GSA OCIO officials stated that they expect to be notified by system officials of development of mobile applications during the security assessment and authorization process. GSA's approach is reactive and relies upon (1) Apple's iOS and Google's Android platform application evaluation procedures and (2) scanning of GSA mobile devices to identify any new mobile applications (whether developed by GSA or external parties).

According to the NIST SP 800-53, the organization must manage the information system using a system development life cycle methodology that includes information security considerations. Mobile platform risks differ from those associated with traditional computing. These include poor session handling, reduced authorization and authentication requirements, and increased potential for data leakage due to loss or theft of devices. To prevent exploitation, security officials need to understand the additional risks mobile applications introduce into the existing architecture. Without proper guidance, the development and deployment of GSA mobile applications can occur within GSA without adequate consideration for aspects of security that are not part of the platform vendor's mobile application evaluations. This could result in degradation of confidentiality, availability, or integrity for entities interacting with the application, including: GSA systems, GSA users, or the public.

Recommendations

Based on our audit findings we recommend the GSA Chief Information Officer:

1. Conduct additional oversight of patch management implementations to ensure that system officials are addressing vulnerabilities on GSA systems in a timely manner.

2. Work with PBS to ensure that PBS develops and implements a process for testing the restoration of system backups before new systems are deployed.

3. Create guidance to assist GSA system officials in securely developing applications for mobile platforms.

Management Comments

Management agreed with our findings and recommendations. The GSA CIO's complete response is presented in ***Appendix B***.

Conclusion

We found that additional steps are needed to strengthen GSA's IT Security Program in three key areas: (1) timely patching, (2) contingency plan testing for newly deployed systems within PBS, and (3) policies for mobile application development.

Additional oversight of patching processes for GSA systems could reduce threats from known security vulnerabilities. We also found that PBS needs to ensure that newly deployed systems are recoverable from backup media. Finally, additional guidance is needed to direct agency development of secure mobile applications. We believe that making the security improvements recommended in this report will better enable GSA's OCIO to ensure the confidentiality, availability, and integrity of the agency's systems and data.

Appendix A – Purpose, Scope, and Methodology

Purpose

The Federal Information Security Management Act of 2002 (FISMA) requires an annual independent evaluation of the General Services Administration's (GSA) Information Technology (IT) Security Program. To meet the FISMA requirements, the Office of Inspector General conducted an audit encompassing assessments of the security program and controls for select systems.

Scope

The audit's scope included assessments of controls for GSA's IT Security Program and reflects results from evaluations of four selected systems conducted throughout the fiscal year by our office. In addition, the scope includes evaluations of the Office of the Chief Information Officer's oversight of the implementation of IT security controls for GSA systems and data.

Methodology

To accomplish our objectives, we:

- Met with GSA IT security officials in the Office of the GSA Chief Information Officer, Federal Acquisition Service, and Public Buildings Service.
- Applied the NIST Federal Information Processing Standards Publications and SP 800-series security guidelines.
- Reviewed applicable information security regulations, policies, and guidance.
- Assessed the results of the completed system security reviews for three systems.
- Performed an assessment of select CyberScope questions for a fourth system by examining the system assessment and authorization package, including the system risk assessment, security plan, security assessment results, contingency plan, and plan of action and milestones. To determine implementation of certain CyberScope controls for the system, we chose a random sample of minor applications.

We conducted the audit between April 2012 and August 2012 in accordance with generally accepted government auditing standards. 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.

Internal Controls

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

Appendix B – Management Comments

GSA

GSA Office of the Chief Information Officer

August 30, 2012

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

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: FY 2012 Office of Inspector General FISMA Audit of
GSA'S Information Technology Security Program
Report Number A120125

This is in response to the FY 2012 Office of Inspector General FISMA Audit of GSA's Information Technology Security Program.

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

If you have any questions, please contact Daryle Seckar, Director, Office of Enterprise Management Services (IE), on 202-208-5054.

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

Appendix C – Report Distribution

GSA Chief Information Officer (I)

Senior Agency Information Security Officer (IS)

Commissioner, Public Buildings Service (P)

Division Director, GAO/IG Audit Response Division (H1C)

Audit Liaison, Office of the Chief Information Officer (I)

Audit Liaison, Public Buildings Service (P)

Assistant IG for Auditing (JA)

Deputy Assistant IG for Investigations (JID)

Director, Audit Planning, Policy, and Operations Staff (JAO)