

Audit Report

**FY 2010 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A100085/O/F/F11001**

December 8, 2010

**Office of Inspector General
General Services Administration**



Office of Audits

**FY 2010 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A100085/O/F/F11001**

December 8, 2010



Date: December 8, 2010

To: Casey Coleman
Chief Information Officer (I)

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

Subject: FY 2010 Office of Inspector General FISMA Review of GSA's IT Security
Program, Report Number A100085/O/F/F11001

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 security program and controls for select systems. This audit report presents the results of the Office of Inspector General's fiscal year 2010 review of the General Services Administration's (GSA's) information technology (IT) security program and reflects results from five system security audits conducted during the year. Appendix A provides the objective, scope, and methodology for the audit.

On April 21, 2010, the Office of Management and Budget (OMB) issued annual FISMA reporting instructions¹ for agencies and IGs. OMB directed IGs to assess agency information security performance in key areas, including certification and accreditation, configuration management, security training, incident response, remote access, and identity management. Further, OMB has directed Agencies and IGs to use Cyberscope, an Internet-based tool to respond to OMB's FISMA questions.

RESULTS OF AUDIT

GSA's Chief Information Officer (CIO) continues to take steps to develop, document, and implement an agency-wide IT security program. For example, the 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 cover cloud computing technologies. However, we found that additional steps are needed to strengthen GSA's IT security program in four key areas: (1) secure configuration of agency systems, (2) oversight of audit logging and monitoring practices, (3) implementation of multifactor authentication for systems processing sensitive information, and (4) encryption of data on agency laptop computers.

¹ OMB Memorandum M-10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, April 21, 2010



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 for GSA systems by:
 - a. Increasing oversight of security officials' application of baseline configuration requirements, and
 - b. Expanding technical testing processes to include authenticated scanning.
2. Work with system security officials to prioritize the implementation of audit logging and monitoring controls for GSA systems.
3. Ensure that all systems that are remotely accessed implement multi-factor authentication, as appropriate.
4. Implement an encryption solution for agency laptops that integrates into GSA's network environment.

EXPLANATION OF FINDINGS

Expanding technical testing processes could improve configuration management of agency systems

While the GSA-CIO has implemented a testing program with tools that identify vulnerabilities, improvements are needed to better secure agency systems and data. Specifically, we identified numerous weaknesses in all five systems reviewed resulting from security misconfigurations of database or operating system software. These weaknesses included database and operating system software that was not patched or securely configured and lax password management practices for database administrator accounts. As a result, these systems and their sensitive data were placed at an increased risk of inappropriate access, modification, or destruction. GSA's IT Security Policy requires all information systems be securely hardened and patched while in operation. National Institute of Standards and Technology (NIST) Special Publication 800-53² requires organizations to configure the security settings of IT systems to the most restrictive mode consistent with operational requirements.

Weaknesses occurred for two primary reasons. First, system security officials were not applying GSA's IT Security Policy requirements for baseline configuration. Second, technical testing conducted by the GSA-CIO as part of GSA's oversight was not comprehensive. To strengthen configuration management of GSA systems, we recommend that the GSA-CIO: (1) increase oversight of security officials' application of baseline configuration requirements, and (2) expand technical testing processes by performing authenticated scans. Authenticated scanning would provide a more comprehensive view as to the implementation of GSA's IT Security Policy and hardening guides by system security officials.

² NIST SP 800-53, Rev. 2, *Recommended Security Controls for Federal Information Systems*, December 2007

Additional oversight by GSA's IT security program could assist in ensuring that audit logging and monitoring controls are implemented for GSA systems

While the GSA-CIO has published policy on audit logging and monitoring, we found inconsistent implementation of the policy for three of five systems reviewed, specifically:

- Database audit records, which would capture information such as the modification and deletion of data and administrative actions, were not generated for one system that contains Privacy Act information.
- Operating system audit records that monitor baseline system data, such as system performance, were not enabled for another system containing Privacy Act information.
- System security officials were not reviewing audit records for suspicious activity for another system containing sensitive information.

As a result of not appropriately implementing audit logging and monitoring, system security officials may be unable to identify unauthorized activity or when GSA systems are compromised. Further, investigatory actions in response to security incidents may be hindered. GSA's IT Security Policy requires that security auditing capabilities be employed on all GSA information systems and that audit records be reviewed frequently for signs of unauthorized activity and other security events.

Inconsistent implementation occurred primarily because GSA, in its efforts toward enterprise-wide continuous monitoring, has not prioritized the management of audit records for systems that contain sensitive information. To better detect potential security incidents, we recommend that the GSA-CIO work with system security officials to prioritize the implementation of audit logging and monitoring for GSA systems.

Better planning could help ensure successful implementation of multifactor authentication for GSA systems

Multifactor authentication involves accessing IT systems with two or more of the following: something a user knows (e.g., username and password), something a user has (e.g., smartcard), or something a user is (e.g., biometrics). None of the five systems that we reviewed were using multifactor authentication for remote access to sensitive information. All permit access with only a username and password. Further, three of the systems contained sensitive data. As a result, these systems were placed at an increased risk of unauthorized access, disclosure of sensitive information, and having their data compromised.

The lack of multifactor authentication was not addressed as part of the security assessments for all five systems reviewed. One system identified this as a requirement, but implementation of multifactor authentication was not tracked and prioritized on the system plan of action and milestones. NIST requires multifactor authentication for remote access to these systems. To better ensure the security of system data and to enhance access controls, we recommend that the GSA-CIO ensure that all systems that are remotely accessed implement multifactor authentication, as appropriate.

GSA must overcome technical challenges for successful implementation of an encryption solution for agency laptops

GSA has not implemented a solution to encrypt agency laptops, a condition we originally reported in 2008.³ In response to a 2006 security incident in which a laptop containing personally identifiable information for 26.5 million U.S. military veterans was stolen, the Office of Management and Budget now requires agencies to encrypt sensitive data on all mobile devices.⁴ Encryption refers to converting data into a form that is not easily understood by unauthorized individuals. When data on agency laptops is not encrypted, sensitive information may be at increased risk of disclosure and misuse in the event that the laptops are lost or stolen.

GSA laptops are not encrypted because GSA has experienced significant technical problems in integrating the chosen encryption solution in the GSA's network. To ensure that sensitive information is adequately protected on agency laptops, we recommend that the GSA-CIO implement an encryption solution for agency laptops that integrates into GSA's network environment.

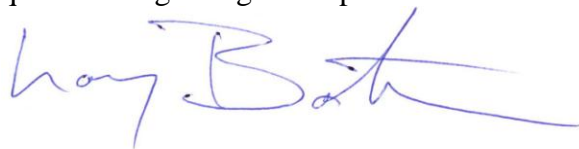
MANAGEMENT COMMENTS

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 five 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-CIO's staff for their assistance and cooperation during this audit. Please contact Michael Nussdorfer, Auditor-in-Charge, or me if you have any questions regarding this report.



Larry Bateman
Audit Manager
Finance and Information Technology Audit Office (JA-F)

³ FY 2008 Office of Inspector General FISMA Review of GSA's IT Security Program, Report Number A080081/O/T/F08016, dated September 11, 2008

⁴ OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006

FY 2010 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A100085/O/F/F11001

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. If not, what additional actions are needed to strengthen information security risk management practices for GSA? 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 five 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, Public Buildings Service, and the Office of Governmentwide Policy. We also met with GSA's external auditor, KPMG.
- Considered results of information systems controls testing performed for the financial statement audit.
- 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 system- and program-level plans of action and milestones.
- Conducted operating system, database, and web application security testing for the select systems we reviewed.

We conducted this performance audit in accordance with generally accepted government auditing standards between January and October of 2010. 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.

FY 2010 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A100085/O/F/F11001

APPENDIX B – MANAGEMENT COMMENTS



GSA Office of the Chief Information Officer

November 23, 2010

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

FROM: CASEY COLEMAN *Casey Coleman*
CHIEF INFORMATION OFFICER (I)

SUBJECT: Draft FY 2010 Office of Inspector General FISMA Review of
GSA'S Information Technology Security Program
Report Number A100085

This is in response to the IG draft audit on FY 2010 Office of Inspector General FISMA Review 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
1800 F Street, NW
Washington DC 20405-0002
www.gsa.gov

FY 2010 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A100085/O/F/F11001

APPENDIX C – REPORT DISTRIBUTION

	<u>Electronic Copies</u>
Chief Information Officer (I)	3
Senior Agency Information Security Officer (IS)	1
Commissioner, Public Buildings Service (P)	1
Commissioner, Federal Acquisition Service (Q)	1
Associate Administrator, Office of Governmentwide Policy (M)	1
Internal Control and Audit Division (BEI)	1
Assistant Inspector General for Auditing (JA)	1
Director, Audit Operations (JAO).....	1
Deputy Assistant Inspector General for Acquisition Audits (JA-A)	1
Deputy Assistant Inspector General for Real Property Audits (JA-R).....	1
Director, Administration and Data Systems (JAS).....	1
Assistant Inspector General for Investigations (JI).....	1