Audit Report

FY 2007 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A070108/O/T/F07015

September 17, 2007

Office of Inspector General
General Services Administration

Office of Audits

FY 2007 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A070108/O/T/F07015

September 17, 2007

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 17, 2007

To: Casey Coleman
Chief Information Officer (I)

Reply to Attn of: Gwendolyn A. McGowan
Deputy Assistant Inspector General for Information Technology Audits (JA-T)

Subject: FY 2007 Office of Inspector General FISMA Review of GSA's Information Technology Security Program, Report Number A070108/O/T/F07015

INTRODUCTION

Background

The Federal Information Security Management Act of 2002 (FISMA) provides a framework for securing Federal information systems including: (1) ensuring the effectiveness of information security controls over information resources; (2) development and maintenance of minimum controls required to protect Federal information and information systems; and (3) a mechanism for improved oversight of agency information security programs. This audit report presents the results of the Inspector General's Fiscal Year (FY) 2007 independent evaluation of the General Services Administration's (GSA) agency-wide Information Technology (IT) Security program and controls for select systems, as required by FISMA. This audit report is provided for inclusion as an appendix in GSA's FY 2007 FISMA report and FY 2009 budget submission to the Office of Management and Budget (OMB).

Objectives, Scope, and Methodology

The objective of this audit was to assess the effectiveness of GSA's IT security program and practices for select systems in meeting FISMA requirements and is based on the results of four independent audits of the following systems: Region 8 FTS LAN, Region 8 PBS LAN, GSAjobs, and the Fleet Management System. Our response to specific questions in the OMB FY 2007 reporting template for FISMA, attached as Appendix A, includes a fifth system evaluated as part of an ongoing audit.

In 2007, we conducted independent IT system security audits of four GSA systems, two of which were operated by contractors. System security controls were reviewed to assess implementations of GSA's IT security program. Appendix B lists the four systems reviewed as part of this audit, and the fifth system used to prepare responses in the attached OMB reporting template. To answer Question 6 in the OMB reporting template, we relied on an ongoing audit of GSA's efforts to protect sensitive information. The Results of Audit section of this report also refers to significant IT system security weaknesses identified in two additional IT system audits conducted in 2007, which identified issues consistent with our FISMA system security audits. We reviewed applications and data repositories for inclusion in the IT system security control process. FISMA audit work relied on GSA's IT security policy[1] and procedures, standards, and guidelines for implementing GSA's IT security program. We met with Agency IT security officials in the Office of the GSA Chief Information Officer (GSA-CIO) and in Services, Staff Offices, and Regions (S/SO/R), including the GSA Senior Agency Information Security Officer (SAISO), Information System Security Managers (ISSMs), and Information System Security Officers (ISSOs) for select systems. To assess controls implementing commonly accepted IT security principles and practices, we used the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publications, and Special Publication (SP) 800 Series security guidelines. Limited control tests from thirteen chapters of NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006, were included in the review of GSA's IT security program. To assess the effectiveness of GSA's IT security program implementation, we examined system risk assessments, system security plans, system security assessment results, certification and accreditation (C&A) letters, contingency plans, and system-level Plans of Action and Milestones (POA&M) for each system. In addition to reviewing the comprehensiveness of documentation, we evaluated additional management, technical, and operational controls using: vulnerability scanning, database configuration testing, and reviews of environmental and physical security, background investigations, and training. IT system security audits for FISMA also included a detailed analysis of web applications. In addition to FISMA, NIST, and GSA guidance, we used other applicable regulations and policies, including: *OMB Circular A-130 Revised, Appendix III, Security of Federal Automated Information Resources*, November 2000; and *Homeland Security Presidential Directive (HSPD) 12, Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004. Audit work was performed between February and August 2007 in accordance with generally accepted government auditing standards.

[1] *GSA Order CIO P 2100.1C - GSA Information Technology Security Policy*, February 17, 2006 and the revised *GSA Order CIO P 2100.1D - GSA Information Technology Security Policy*, June 21, 2007.

RESULTS OF AUDIT

GSA's IT security program has taken steps to establish an inventory of GSA systems, designate system security roles and responsibilities, and incorporate NIST guidance. Since the implementation of FISMA, the GSA-CIO has taken further steps to identify and reduce risks through designations of additional management, operational, and technical controls outlined in GSA's IT security policy and procedures. Despite these efforts, GSA's IT security program has not been fully effective in ensuring that risks for all applications, data repositories, and services within system boundaries are identified and mitigated. Oversight of contractor-supported systems was not comprehensive where systems were not secured, and contractor background investigations were not consistently conducted. Configuration management should be strengthened in the area of configuration settings, and Agency policies and procedures are in need of improvement in some cases. As a result, GSA's information assets have been exposed to undue risks of inappropriate disclosure, destruction, and alteration. The IT security program has not been fully successful due to the lack of a program implementation plan. The GSA-CIO should assist senior management in developing and adopting an implementation plan with performance goals and measures for system security officials. Accountability is important for the success of GSA's IT security program and should guide an implementation plan that will assist with managing GSA's changing risk environment. At the system level, we also concluded that an effective implementation plan for GSA's IT security program should include a more detailed inventory process, improved contractor oversight, and more comprehensive configuration management.

Appendix A contains our responses to specific FISMA questions, as requested by OMB. Our responses include assessments of the security for GSA's major applications and general support systems, as noted in Appendix B.

GSA IT System Security Risks and Related Controls Are Not Comprehensively Addressed for All Applications, Data Repositories, and Services Within System Boundaries

GSA's information assets have been exposed to risks of inappropriate disclosure, destruction, and alteration when weaknesses were not identified and appropriately mitigated for all applications, data repositories, and services within system boundaries. OMB Circular A-130, Appendix III, requires that agencies "implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications." System security audits in 2007 identified a major application with multiple web applications not addressed with the system security plan. A general support system used across the Agency contained databases where risks were not identified and addressed as part of the certification and accreditation process, inappropriately exposing sensitive GSA data to undue risks. Another major application implemented an external reporting module without assessing the risk and security of the module, which also inappropriately exposed sensitive GSA data to undue risks. Despite efforts to clarify and enhance GSA's IT system security policy, system certification and accreditation efforts are not consistently comprehensive and effective.

With our FISMA audit work since 2004, we have repeatedly identified and reported that system security officials have not adequately addressed all functionality and data within systems. In 2004, we identified that the GSA system inventory was incomplete, and the GSA-CIO took steps to address the risks and complete the Agency inventory. We also reported that for the systems we reviewed, the C&A process was not implemented consistently, not updated after major system changes, or not completed. We recommended strengthening policy and procedures to better manage risks by incorporating controls to ensure that C&A documentation, including risk assessments, security plans, and security plan testing and evaluations are current and complete. In 2005, we found that one general support system had deployed Voice over Internet Protocol without updating its risk assessment and security plan, and another general support system moved to a new operating system and combined two networks without addressing the changes in a subsequent update to the security plan. We also reported that the C&A process was not consistently implemented and recommended that the GSA-CIO improve security over GSA's data and IT assets by taking actions to increase oversight of the implementation of GSA's IT security policy and procedures related to C&A. GSA's C&A process was revised to include oversight by the SAISO and a requirement for a review of C&A documents, but did not focus on accountability and the inventory of data and applications. In 2006, we again found inconsistent implementation of the C&A process where we identified incomplete risk assessments, system security plans, security assessments, and contingency plans for systems reviewed. C&A documentation for a general support system was not updated to address additional functionality of the reviewed component. A contractor-provided system did not follow GSA procedural guides when developing C&A documentation. Similar deficiencies identified in 2007 are evidence that an approach that goes beyond the current policy is needed to successfully implement FISMA. The inability of GSA system officials to consistently ensure effective implementation of FISMA and GSA's IT security policy is due, in part, to a lack of a comprehensive inventory of the applications, data repositories, and services residing on their systems, as well as accountability for identifying and mitigating risks for items in the inventory. The GSA IT security policy states that system owners are "management officials within GSA who bear the responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems." Since the system owner is responsible for integrating and explicitly identifying funding for information systems and programs into IT investment and budgeting plans, that individual should be aware of all applications, databases, and services within the information system. The GSA-CIO's IT security program currently relies on a budget-based inventory of systems, which is not at the level of detail needed to manage system level risks. An inventory process that will require system owners to identify and periodically report on all applications, data repositories, and services maintained with their systems is needed to ensure that the certification and accreditation process is comprehensively and completely performed as part of management's IT security implementation plan.

Oversight of Contractor-Supported Systems Should Be More Comprehensive

GSA's management of risks and oversight of contractor-supported systems should be more comprehensive, as evidenced in two areas of risk: (1) inadequately secured contractor-provided solutions had weaknesses not detected by GSA system security officials; and (2) the lack of contractor background investigations is a problem this year and has been reported as an area of risk with our FISMA and GISRA audits since 2002. FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Our repeated findings confirm that despite GSA's efforts and implementation of a program that includes policies, procedures, and assigned roles and responsibilities, the program has not successfully ensured that contractor-supported systems comply with established requirements.

Contractor-Provided Solutions

GSA's IT security program has not been effective in engaging GSA management to consistently enforce policy and procedures for contractor-provided solutions supporting GSA programs and maintaining GSA data. In 2007, audit tests of a contractor-provided major application revealed that oversight of IT security for the system was not adequately performed by GSA system security officials, who did not ensure that the contractor had applied GSA's IT security policy and procedural guidance. Enforcement of existing task order clauses would have identified system security weaknesses and alerted GSA management to vulnerabilities identified during our audit of the system. In 2006, contractors providing solutions for GSA were not provided with GSA’s IT security policy and procedures by the ISSO, were not adequately monitored for compliance with the Agency IT security policy, and were unaware of several vulnerabilities detected during our review. In 2004 and 2005, we reported on contractor-provided solutions that were not compliant with the Agency IT security policy and procedures required by their contracts with GSA. These repeated findings confirm that efforts to implement management action plans in response to prior audit recommendations did not consistently improve system owners’ efforts to secure contractor-provided solutions.

Contractor Background Investigations

Controls currently in place and those planned under HSPD-12 will not ensure that contractor background investigations are requested and completed before access is granted to GSA systems. We identified contractor personnel security issues with all systems included in this year’s FISMA review, which place GSA systems and data at increased risk from contractors granted access to systems before investigations are completed. For one system, 25 contractors were granted access before background investigations were requested, although the task order stated that “no access shall be given to the government computer information systems and government sensitive information without a background investigation being verified or in process.” Two contractor-supported systems granted temporary access to contractors, but full investigations were not requested for all of the contractors, and there were no procedures in place to ensure that investigations were completed. GSA’s IT security policy designates responsibilities for ensuring that users have the required background investigations to the ISSO, Authorizing Official, Data Owner, and Contracting Officers/Contracting Officer’s Technical Representative. Without a single point of responsibility and accountability within GSA for ensuring completion of background investigations, background investigations remain an oversight challenge. The lack of background investigations being completed for contractors is also a recurring weakness and has been included in FISMA and GISRA reports issued since 2002 and is a significant system security risk. Management's response to prior recommendations deferred resolution to implementation of HSPD-12, which requires all Federal governmental departments and agencies to conduct background investigations, adjudicate the results, and issue identity credentials to Federal employees and contractors who require long-term access to its federally controlled facilities and information technology systems. However, this issue is not being addressed by HSPD-12 since contractors supporting GSA systems are often not housed in government facilities or accessing Government managed systems.

Opportunities to Strengthen Configuration Management Were Identified

During the past several years GSA has stressed the need to expand testing of system configurations to include databases and web applications as our audit tests were expanded to address emerging IT security threats in these areas. In 2007, we identified opportunities to strengthen configuration management and reduce risks to GSA systems and data in two areas. First, insecure configuration settings were identified in system reviews of web application security, database security, and operating system security that could affect the confidentiality, integrity, and availability of those GSA systems. Second, Agency configuration management policies and procedures for handling of unsuccessful login attempts and warning banners were conflicting and not in conformance with best practices.

Configuration Settings

System vulnerabilities in the four systems reviewed this year resulted from configuration settings that were not in full conformance with GSA guidance. System testing identified insecure configuration settings in web applications, databases, and operating systems. Web application configurations deviated from GSA's procedural guidance in three systems, including two systems with critical vulnerabilities. One web application was susceptible to a denial-of-service attack that could affect system availability. A number of configuration weaknesses were identified with Lotus Domino database servers that were not configured in accordance with best practices. Lotus Domino is widely used by the Agency, but GSA has not developed procedural guidance for Lotus Domino. An Oracle database on another system was not configured in accordance with GSA's Oracle database hardening guide[2]. Operating system vulnerabilities were identified in three of the four systems we reviewed.

Configuration settings weaknesses resulted when applications, data repositories, and services are not identified and addressed. While the GSA-CIO has issued guidance on web application security and has initiated a centralized program for evaluating web application security, this has not effectively ensured that guidance is being applied to all of GSA's web applications. To address configuration settings weaknesses in Lotus Domino, a procedural or hardening guide is needed. System security officials are responsible for applying secure configurations in all applications, data repositories, and services within their systems.

Configuration Management Policies and Procedures

GSA's configuration management policies and procedures contain conflicts in handling invalid login attempts for web applications, and requirements for warning banners are not comprehensive. The GSA IT security policy conflicts with the GSA Procedural Guide on Web Application Security on the handling of unsuccessful login attempts. GSA's IT security policy requires user lockout after ten unsuccessful attempts, while the procedural guide incorporates best practices and specifies delaying the login time between unsuccessful login attempts. Delaying invalid login attempts for web applications can prevent certain denial-of-service attacks. Agency guidance on the use of warning banners should also be updated for publicly accessible systems and web applications. GSA's IT security policy requires the use of a specific warning banner, but is not consistent with the *System Use Notification* control in NIST SP 800-53, which describes different requirements for publicly accessible systems. Additionally, we identified web applications in our review this year that did not include warning banners, and

[2] *GSA IT Security Procedural Guide: Oracle Database Hardening, CIO-IT Security-05-28*, March 2005

concluded that the GSA web application security procedural guide could be strengthened by referring to banner requirements from the GSA IT security policy.

Conclusion

Conditions reported in 2007 and prior years indicate that management actions have not been fully effective in mitigating risks and securing GSA's systems. The need for a successful security program implementation plan, adopted by senior management, is evidenced by these recurring findings. GSA relies on a budget-based inventory of systems, which is not at the level of detail needed to identify and manage system level security risks. An inventory process that requires system owners to identify and periodically report on all applications, data repositories, and services maintained with their systems is needed as part of an IT security program implementation plan. We conclude that management accountability remains important for successful implementation of FISMA and the success of GSA's IT security program. Specific steps to assist senior management officials in developing and adopting performance goals and measures for system security officials, consistent with IT security program implementation plan goals are needed to move GSA towards more secure systems and data.

RECOMMENDATIONS

To strengthen GSA's IT security program and improve the security of information technology assets, we recommend that the GSA, Chief Information Officer take actions to:

1. Develop an implementation plan to be adopted by management that incorporates agency-wide objectives and measures of progress necessary to meet IT security program goals.
2. Improve management accountability by developing an inventory process that will require system owners to identify and periodically report on all applications, data repositories, and services maintained with their systems.
3. Enhance management's oversight of contractor supported systems by:
   a. Developing processes that promote and measure enforcement of existing task order clauses.
   b. Establishing a single point of contact for contractor background investigations.
4. Strengthen configuration management of GSA's systems by updating the GSA IT security policy and related procedural guidance to address:
   a. Handling successive unsuccessful login attempts in web applications.
   b. Warning banner requirements for both publicly accessible systems and web applications.
   c. Secure configuration of Lotus Domino.
5. Assist senior management officials in developing and adopting performance goals and measures for system security officials, consistent with the IT security program implementation plan.

MANAGEMENT COMMENTS

The GSA-CIO's 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 C.

INTERNAL CONTROLS

As discussed in the Objectives, Scope, and Methodology section of this report, the objective of our review was to assess the effectiveness of GSA's IT security program and practices for select systems in meeting FISMA requirements. This audit included a review of selected management, operational, and technical controls for GSA's IT security program. The Results of Audit and Recommendations sections of this report state in detail the need to strengthen specific controls with the GSA IT security program.

We would like to express our thanks to the GSA-CIO and her staff for their assistance and cooperation during the audit. An electronic copy of this report comprised of two files is being provided for inclusion in the GSA FISMA report to OMB and Congress. Please contact me if you have any questions regarding this report.

Larry Bateman
Director, Information Technology Security Audit Services
Information Technology Audit Office (JA-T)

**FY 2007 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A070108/O/T/F07015**

APPENDIX A

GSA, OFFICE OF INSPECTOR GENERAL RESPONSES TO THE OFFICE OF MANAGEMENT AND BUDGET'S FISMA QUESTIONS

The following EXCEL Workbook is transmitted in a separate file using the format directed by the Office of Management and Budget.

Section C - Inspector General: Questions 1 and 2

Agency Name: General Services Administration **Submission date:** **September 17, 2007**

Question 1: FISMA Systems Inventory

1. As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

In the table below, identify the number of agency and contractor information systems, and the number reviewed, by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems reviewed by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

		Question 1						Question 2					
		a. Agency Systems		b. Contractor Systems		c. Total Number of Systems (Agency and Contractor systems)		a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
Bureau Name	**FIPS 199 System Impact Level**	Number	Number Reviewed	Number	Number Reviewed	Total Number	Total Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Public Buildings Service (PBS)	High	0		0		0	0						
	Moderate	10		0		10	0						
	Low	0		0		0	0						
	Not Categorized	0		0		0	0						
	Sub-total	**10**	**0**	**0**	**0**	**10**	**0**	**0**		**0**		**0**	
Federal Acquisition Service (FAS) - Formerly FSS	High	0		0		0	0						
	Moderate	1		9	1	10	1	1	100%	1	100%	1	100%
	Low	2		3		5	0						
	Not Categorized	0		0		0	0						
	Sub-total	**2**	**0**	**12**	**1**	**14**	**1**	**1**	100%	**1**	100%	**1**	100%
Federal Acquisition Service (FAS) - Formerly FTS	High	0		1		1	0						
	Moderate	2		4		6	0						
	Low	0		2		2	0						
	Not Categorized	0		0		0	0						
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**		**0**		**0**	
Office of the Chief Acquisition Officer (OCAO)	High	0		0		0	0						
	Moderate	0		4		4	0						
	Low	2		2		4	0						
	Not Categorized	0		0		0	0						
	Sub-total	**2**	**0**	**6**	**0**	**8**	**0**	**0**		**0**		**0**	
Office of Governmentwide Policy (OGP)	High	0		0		0	0						
	Moderate	1		4		5	0						
	Low	3		2		5	0						
	Not Categorized	0		0		0	0						
	Sub-total	**4**	**0**	**6**	**0**	**10**	**0**	**0**		**0**		**0**	
Office of the Chief Information Officer (OCIO)	High	0		0		0	0						
	Moderate	15	2	0		15	2	2	100%	2	100%	2	100%
	Low	0		0		0	0						
	Not Categorized	0		0		0	0						
	Sub-total	**15**	**2**	**0**	**0**	**15**	**2**	**2**	100%	**2**	100%	**2**	100%
Office of the Chief Financial Officer (OCFO)	High	0		0		0	0						
	Moderate	1		3	1	4	1	1	100%	1	100%	1	100%
	Low	0		0		0	0						
	Not Categorized	0		0		0	0						
	Sub-total	**1**	**0**	**3**	**1**	**4**	**1**	**1**	100%	**1**	100%	**1**	100%
Office of the Chief Human Capital Officer (OCHCO)	High	0		0		0	0						
	Moderate	0		2	1	2	1	1	100%	1	100%	1	100%
	Low	0		0		0	0						
	Not Categorized	0		0		0	0						
	Sub-total	**0**	**0**	**2**	**1**	**2**	**1**	**1**	100%	**1**	100%	**1**	100%
Office of Inspector General (OIG)	High	0		0		0	0						
	Moderate	1		0		1	0						
	Low	0		0		0	0						
	Not Categorized	0		0		0	0						
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Office of General Counsel (OGC)	High	0		0		0	0						
	Moderate	0		0		0	0						
	Low	1		0		1	0						
	Not Categorized	0		0		0	0						
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Board of Contract Appeals (BCA)	High	0		0		0	0						
	Moderate	0		0		0	0						
	Low	1		0		1	0						
	Not Categorized	0		0		0	0						
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Office of Citizen Services and Communications (OCSC)	High	0		0		0	0						
	Moderate	0		0		0	0						
	Low	0		2		2	0						
	Not Categorized	0		0		0	0						
	Sub-total	**0**	**0**	**2**	**0**	**2**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**0**	**0**	**1**	**0**	**1**	**0**	**0**		**0**		**0**	
	Moderate	**31**	**2**	**26**	**3**	**57**	**5**	**5**	100%	**5**	100%	**5**	100%
	Low	**9**	**0**	**11**	**0**	**20**	**0**	**0**		**0**		**0**	
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**40**	**2**	**38**	**3**	**78**	**5**	**5**	100%	**5**	100%	**5**	100%

Section C - Inspector General: Question 3

Agency Name: **General Services Administration**

Question 3: Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

3.a.	**The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.** Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance. Response Categories: - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Sometimes (51-70% of the time)
3.b.	**The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.** Response Categories: - The inventory is approximately 0-50% complete - The inventory is approximately 51-70% complete - The inventory is approximately 71-80% complete - The inventory is approximately 81-95% complete - The inventory is approximately 96-100% complete	Inventory is 96-100% complete
3.c.	**The IG generally agrees with the CIO on the number of agency-owned systems. Yes or No.**	Yes
3.d.	**The IG generally agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.**	Yes
3.e.	**The agency inventory is maintained and updated at least annually. Yes or No.**	Yes

3.f. **If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.**

Component/Bureau	System Name	Exhibit 53 Unique Project Identifier (UPI)	Agency or Contractor system?

Number of known systems missing from inventory:	

Section C - Inspector General: Questions 4 and 5

Agency Name: General Services Administration

Question 4: Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestones (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:

- **Rarely- for example, approximately 0-50% of the time**
- **Sometimes- for example, approximately 51-70% of the time**
- **Frequently- for example, approximately 71-80% of the time**
- **Mostly- for example, approximately 81-95% of the time**
- **Almost Always- for example, approximately 96-100% of the time**

4.a.	The POA&M is an agency-wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	Almost Always (96-100% of the time)
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	Almost Always (96-100% of the time)
4.c.	Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).	Almost Always (96-100% of the time)
4.d.	Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	Almost Always (96-100% of the time)
4.e.	IG findings are incorporated into the POA&M process.	Almost Always (96-100% of the time)
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.	Almost Always (96-100% of the time)

POA&M process comments: The General Services Administration, Chief Information Officer, has developed an agencywide POA&M process. All five systems reviewed have a POA&M and most known IT security weaknesses were being managed in the POA&Ms. However, the POA&M for one major application did not include 3 of 10 weaknesses.

Question 5: IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems" (February 2004) to determine a system impact level, as well as associated NIST document used as guidance for completing risk assessments and security plans.

5.a.	**The IG rates the overall quality of the Agency's certification and accreditation process as:** Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory	
5.b.	**The IG's quality rating included or considered the following aspects of the C&A process:** (check all that apply)	Security plan	X
		System impact level	X
		System test and evaluation	X
		Security control testing	X
		Incident handling	X
		Security awareness training	X
		Configurations/patching	X
		Other:	

C&A process comments: GSA's C&A process is satisfactory, but weak implementaion by system owners result in a program that has not effectively ensured that risks for all applications, data repositories, and services within system boundaries are identified and mitigated. Most conditions identified in 2007 were also reported in prior years indicating that management actions in response to prior year FISMA audit reports have not been fully effective in mitigating risk and securing GSA's systems, due in part, to a continuing lack of accountability. We concluded that effective implementation of GSA's IT Security Program at the system level is dependent upon a more detailed and granular inventory process and increased accountability.

Section C - Inspector General: Questions 6 and 7

Agency Name: **General Services Administration**

Question 6: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process

6.a.	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D II.4 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
	Comments: GSA has appointed a senior official for privacy, issued a privacy benchmark report, updated policy, taken steps toward improving the protection of PII, and implemented a PIA process. Controls for encryption of PII stored on mobile devices or accessing PII from personally owned computers are not yet implemented.	
6.b.	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15, "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Poor
	Comments: GSA has not comprehensively assessed the adequacy of implementation for existing privacy controls in GSA PII systems and does not identify roles and responsibilities for verifying the implementation of those controls. Contracts for systems with PII do not yet consistently include privacy related Federal Acquisition Regulation (FAR) clauses, and technical scanning on a sample of PII systems revealed that patches have not been consistently applied, leaving some databases vulnerable to known exploits. Controls have been implemented to support least privilege access, but one system inappropriately allowed users to view sensitive information about government facilities. Controls for encryption of PII stored on mobile devices or accessing PII from personal computers are not yet implemented.	

Question 7: Configuration Management

7.a.	**Is there an agency-wide security configuration policy? Yes or No.**	Yes
	Comments: GSA's IT Security Policy requires all agency systems to use GSA technical guidelines, NIST guidelines, or industry best practices for purposes of security configuration and hardening.	
7.b.	**Approximate the extent to which applicable information systems apply common security configurations established by NIST.** **Response categories:** - Rarely- for example, approximately 0-50% of the time - Sometimes- for example, approximately 51-70% of the time - Frequently- for example, approximately 71-80% of the time - Mostly- for example, approximately 81-95% of the time - Almost Always- for example, approximately 96-100% of the time	Mostly (81-95% of the time)

Section C - Inspector General: Questions 8, 9, 10 and 11

Agency Name: **General Services Administration**

Question 8: Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

8.a.	**The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.**	Yes
8.b.	**The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)**	Yes
8.c.	**The agency follows documented policies and procedures for reporting to law enforcement. Yes or No.**	Yes
	Comments: The GSA-CIO has developed a procedural guide that outlines the policies and procedures for incident handling and reporting across the Agency. Incident handling and reporting were generally consistent with this guide for the five systems we reviewed.	

Question 9: Security Awareness Training

Has the agency ensured security awareness training of all employees, including contractors and those employees with significant IT security responsibilities? **Response Categories:** **- Rarely- or approximately 0-50% of employees** **- Sometimes- or approximately 51-70% of employees** **- Frequently- or approximately 71-80% of employees** **- Mostly- or approximately 81-95% of employees** **- Almost Always- or approximately 96-100% of employees**	Almost Always (96-100% of employees)

Question 10: Peer-to-Peer File Sharing

Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

Question 11: E-Authentication Risk Assessments

The agency has completed system e-authentication risk assessments. Yes or No.	Yes

FY 2007 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A070108/O/T/F07015

APPENDIX B

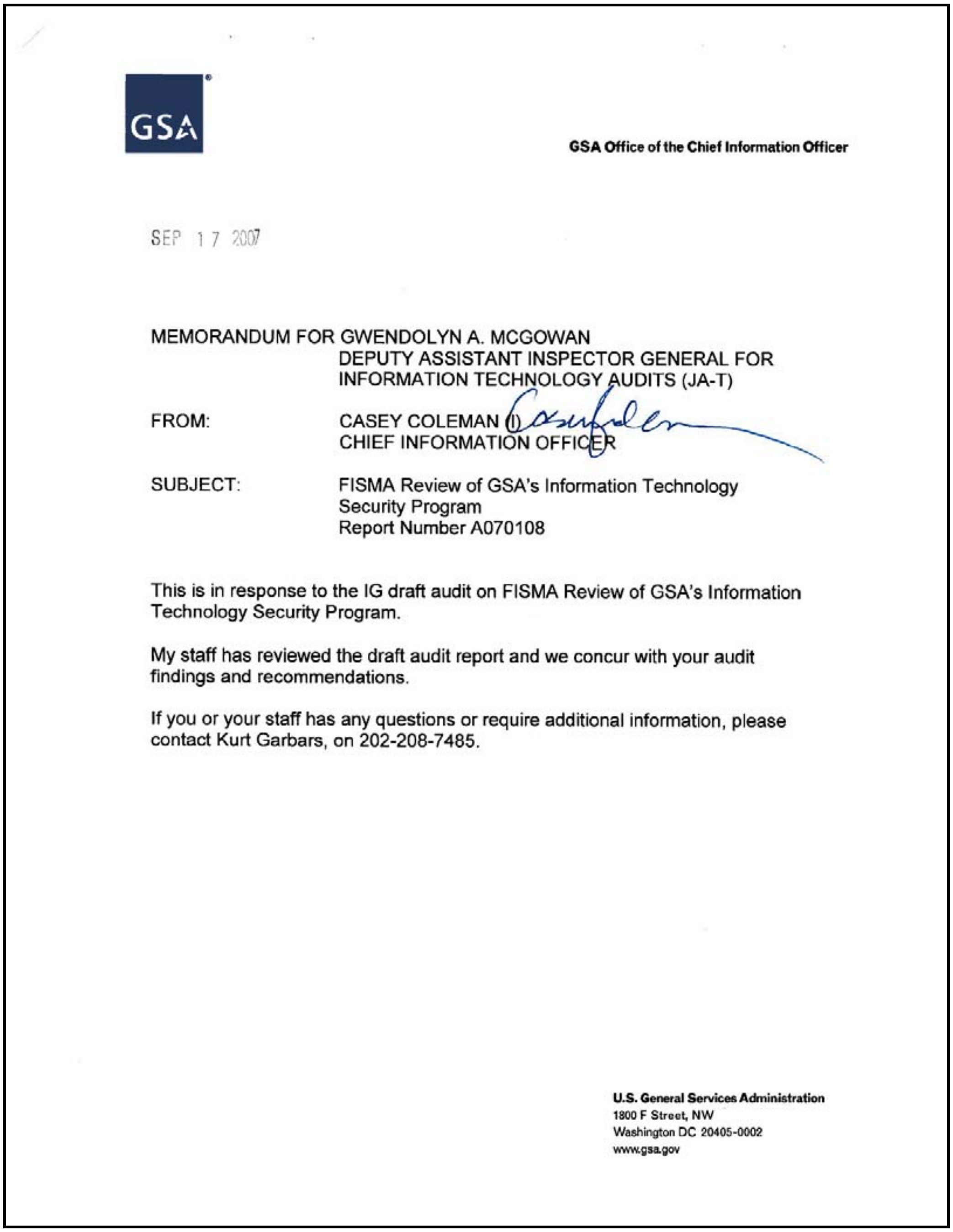
SYSTEMS WHOSE CONTROLS WERE EVALUATED BY THE OFFICE OF INSPECTOR GENERAL IN 2007 AND INCLUDED IN RESPONSES TO THE OMB REPORTING TEMPLATE IN APPENDIX A

System	Owner	Description
Region 8 FTS LAN	Office of the Chief Information Officer (I) Formerly Rocky Mountain Region 8 Denver, Colorado (8A)	The Region 8 FTS LAN functions, personnel, hardware, and software were transferred from the region to the GSA-CIO as part of the Agency's IT infrastructure consolidation initiative in early 2007. The Region 8 FTS LAN is a general support system, which supports users at the Denver Federal Center. This system provides connectivity in support of workflow processing, email, and procurement-related services. The Region 8 FTS LAN is an Agency system categorized as moderate risk.
Region 8 PBS LAN	Office of the Chief Information Officer (I) Formerly Rocky Mountain Region 8 Denver, Colorado (8A)	The Region 8 PBS LAN functions, personnel, hardware, and software were transferred from the region to the GSA-CIO as part of the Agency's IT infrastructure consolidation initiative in early 2007. The Region 8 PBS LAN supports users across six states, incorporates Voice over Internet Protocol (VoIP), and is administered from regional offices in Denver, Colorado. The LAN is a general support system categorized as moderate risk and provides connectivity in support of workflow processing, e-mail, and procurement related services. The Region 8 PBS LAN is an Agency system categorized as moderate risk.
GSAjobs	Office of the Chief Human Capital Officer (C)	GSAjobs is owned and operated by Monster Government Solutions and provides services to GSA under terms of a multiple award schedule contract task order. This contractor-provided solution is a Privacy Act system containing the personally identifiable information of job applicants and is categorized as moderate risk.
Fleet Management System (FMS)	Federal Acquisition Service (Q)	FMS is a contractor-supported system used to manage GSA's fleet of 200,000 motor vehicles and is categorized as moderate risk. The system includes a number of web applications used to report mileage, report vehicles for sale, log accidents, and track vehicles from the GSA Automotive Center.
Pegasys	Office of the Chief Financial Officer (B)	Pegasys is GSA's web-based core financial management system, supported by contractors and is categorized as moderate risk. The system provides detailed and summary financial information in a multitude of formats and has more than twenty interfaces with other GSA applications/systems. Results from an ongoing audit of Pegasys are included in responses to the OMB Reporting Template but are not addressed in the body of this report.

FY 2007 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A070108/O/T/F07015

APPENDIX C

GSA CIO'S RESPONSE TO DRAFT AUDIT REPORT



GSA

GSA Office of the Chief Information Officer

SEP 17 2007

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
INFORMATION TECHNOLOGY AUDITS (JA-T)

FROM: CASEY COLEMAN (I)
CHIEF INFORMATION OFFICER

SUBJECT: FISMA Review of GSA's Information Technology
Security Program
Report Number A070108

This is in response to the IG draft audit on 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 has 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 2007 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A070108/O/T/F07015

APPENDIX D

REPORT DISTRIBUTION

	Copies
Chief Information Officer (I)	3
Chief Financial Officer (B)	2
Commissioner, Federal Acquisition Service (Q)	1
Chief Human Capital Officer (C)	1
Regional Administrator, Rocky Mountain Region (8A)	1
Audit Follow-up and Evaluation Branch (BECA)	1
Assistant Inspector General for Auditing (JA and JAO)	2
Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F)	1
Deputy Assistant Inspector General for Acquisition Audits (JA-A)	1
Deputy Assistant Inspector General for Information Technology Audits (JA-T)	1
Administration and Data Systems Staff (JAS)	1
Assistant Inspector General for Investigations (JI)	1
Regional Inspector General for Auditing, Heartland Region (JA-6)	1
Regional Inspector General for Investigations, Heartland Region (JI-6)	1