Audit Report

**FY 2008 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A080081/O/T/F08016**

September 11, 2008

Office of Inspector General
General Services Administration

Office of Audits

FY 2008 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A080081/O/T/F08016

September 11, 2008

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date:	September 11, 2008
Reply to Attn of:	Gwendolyn A. McGowan Deputy Assistant Inspector General for Information Technology Audits (JA-T)
To:	Casey Coleman Chief Information Officer (I)
Subject:	FY 2008 Office of Inspector General FISMA Review of GSA's Information Technology Security Program, Report Number A080081/O/T/F08016

The Federal Information Security Management Act of 2002 (FISMA) provides a framework for securing Federal information systems including: (1) assurance of 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) 2008 independent evaluation of the General Services Administration's (GSA) agency-wide Information Technology (IT) Security Program, as required by FISMA, and reflects results from our system security audits. Our response to specific questions in the OMB FY 2008 reporting template for FISMA is attached as Appendix A. To clarify our assessment of privacy controls addressed by the FISMA reporting template, we are also providing a copy of our recent report on the GSA Privacy Program[1]. Both audit reports are provided for inclusion as an appendix in GSA's FY 2008 FISMA report to be submitted to the Office of Management and Budget (OMB) by October 1, 2008. Our assessment of the GSA IT Security Program also considered audit findings from two recent IT audits[1,2] issued in FY 2008.

Objectives, Scope, and Methodology

The objective of this audit was to assess the effectiveness of controls over GSA systems and data and to address specific questions and reporting requirements identified by OMB. We reviewed four GSA systems, including one contractor system, to assess implementation of GSA's IT Security Program. Appendix B provides additional information on the systems reviewed. We considered results from these system security audits, along with other recent audit work, with our responses to the OMB FISMA reporting template. FISMA audit work relied on GSA's IT Security Policy[3], procedures, standards, and guides 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,

[1] *Improvements to the GSA Privacy Act Program Are Needed to Ensure that Personally Identifiable Information (PII) Is Adequately Protected*, Report Number A060228/O/T/F08007, March 31, 2008.

[2] *Work Remains in Implementing a Fully Integrated Pegasys Financial Management System*, Report Number A070094/B/T/F08009, June 23, 2008.

[3] *GSA Order CIO P 2100.1D - GSA Information Technology (IT) Security Policy*, June 21, 2007.

Staff Offices, and Regions (S/SO/R), including the Office of the Chief Acquisition Officer, Office of the Chief Human Capital Officer (CHCO), Federal Acquisition Service, Office of General Counsel, and Public Buildings Service. We also met with the GSA Senior Agency Information Security Officer (SAISO), and the Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs) for select systems. To assess security controls, we applied the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publications[4] and Special Publication (SP) 800 series security guidelines. In our review of GSA's IT Security Program, we evaluated the implementation of information security program elements from NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006. To assess the effectiveness of GSA's IT Security Program implementation, we examined system risk assessments, security plans, security assessment results, certification and accreditation (C&A) letters, contingency plans, and system- and program-level Plans of Action and Milestones (POA&M). We also conducted vulnerability scanning and database configuration testing, and reviewed environmental and physical security, background investigations, and training. System security audits included a detailed assessment of web applications. To assess security over GSA's publicly facing web applications, we tested for encryption of logins, use of government domains, and use of validated cryptography. We tested for leakage of GSA information using peer-to-peer file sharing networks and a search engine. In addition to FISMA, NIST, and GSA guidance, we applied other applicable regulations and policies, including *Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004, and the following OMB memoranda: M-05-04, *Policies for Federal Agency Public Websites*, December 2004; M-06-16, *Protection of Sensitive Agency Information*, May 2006; M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 2007; and M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 2007.

We also considered information from an interim audit memorandum, dated September 3, 2008, which alerted GSA Management that sensitive but unclassified information is being maintained by application service providers (ASP) and there does not appear to be an inventory of the projects using these applications. The memorandum noted that neither the GSA Office of the Senior Agency Information Security Officer nor the Service Office of the CIO had any record of these applications or whether they meet all GSA security requirements. These ASPs were not procured through an IT vehicle and have no visibility through annual OMB Exhibit 53 submissions developed for GSA's IT investment portfolio.

We conducted this performance audit 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.

[4] FIPS Publication 199, S*tandards for Security Categorization of Federal Information and Information Systems*, February 2004, requires systems to be categorized as high, moderate, or low impact. FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006, specifies minimum security requirements for information and information systems supporting the executive agencies of the federal government and a risk-based process for selecting the security controls necessary to satisfy the minimum security requirements.

RESULTS OF AUDIT

GSA's Information Technology (IT) Security Program incorporates designated security roles and responsibilities and NIST guidance into Agency policies and procedures. In addition, GSA has taken steps to identify and reduce risks through implementation of additional management, operational, and technical controls. However, inconsistent implementation of controls and insufficient management oversight of contractors continue to hinder GSA's IT Security Program from being fully effective in identifying and managing risks for all GSA systems and data. Deficiencies in the following four areas adversely impact the effectiveness of GSA's IT Security Program: 1) contractor oversight, 2) protection of sensitive information, 3) security of publicly facing websites, and 4) controls for minor applications. Management oversight of contractor-supported systems reviewed this year had not ensured that risks were adequately managed, since task-order requirements and deliverables were not comprehensive. To protect sensitive information, steps are needed to implement encryption of mobile devices and two-factor authentication for remote access, and to establish a complete breach notification policy. GSA has not consistently secured its public web presence through: the protection of login credentials, support for required encryption, and consistent use of government domains. We also found minor applications where security controls were not adequate to address risk. Consistent implementation and sufficient management oversight of IT security requirements are essential for effectively securing GSA's diverse and decentralized IT environment. To enhance and strengthen GSA's IT Security Program and to more consistently secure vital systems and sensitive data, we recommend that the GSA Chief Information Officer (GSA-CIO) take additional steps to enhance management, operational, and technical controls for each of these areas. Appendix A provides responses to specific Office of Inspector General (OIG) questions identified in the annual OMB FISMA template, including supplemental information as needed. Additional information on select systems reviewed is included in Appendix B.

Contractor Oversight Was Inadequate

GSA's oversight of contractor-supported systems could be more comprehensive, as evidenced in two areas of risk: (1) inadequately secured contractor-supported systems had configuration management weaknesses; and (2) inconsistent contractor background investigations were performed for contractors supporting three of four systems reviewed. GSA's IT Security Policy requires all systems to be securely hardened and patched. Technical testing of operating system, database, and web application security found that all of the reviewed systems had configuration management weaknesses in at least one of these areas. System security officials did not effectively monitor contractors performing system security services and did not ensure that system security controls were appropriately implemented. Assessments of task order requirements related to system support services revealed that the task orders for two systems included inadequate deliverables and did not enable system officials to identify instances where hardening and patching requirements were not met. Delays in hardening and patching resulted in configuration management weaknesses and exposed the affected systems to undue risks that could affect the confidentiality, integrity, or availability of GSA systems and data. To address risks with contractor oversight, the GSA-CIO should collaborate with the Office of the Chief Acquisition Officer to develop and implement performance-based deliverables for contract and task order requirements needed to direct system acquisition and IT support services.

Background investigations were not appropriately performed for contractors supporting three of four systems we reviewed. Background investigations were not completed in a timely manner for one system, and background investigations performed for two other systems were inconsistent with the GSA IT Security Policy. The system without timely background investigations had contract task orders without background investigation requirements. The failure to perform appropriate and timely background investigations means that contractors for the affected systems were granted privileged access without appropriate background investigations, placing GSA systems and data at risk of insider attack. We found that there is confusion on the requirements for background investigations. For instance, the GSA IT security policy states that "*Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall be IAW the OCHCO/OCIO HSPD-12 Personal Identity Verification and Credentialing Standard Operating Procedure (SOP) and GSA Handbook ADM 9732.1C, 'Suitability and Personnel Security'*." However, GSA Handbook ADM 9732.1C is currently expired without a replacement, and there is a conflict between the HSPD-12 SOP and the *FPS Implementation Plan for NonPBS-Contractors*. The HSPD-12 SOP requires a Minimum Background Investigation (MBI)/Limited Background Investigation (LBI) for moderate risk positions, but contractor investigation requirements in the *FPS Implementation Plan for NonPBS-Contractors* also allow for an NACIC investigation for moderate risk positions. Further, we found that there are not specific background investigation task order requirements in the Federal Acquisition Regulation (FAR) and General Services Administration Acquisition Regulation. Inconsistent implementation of background investigation procedures has been a risk identified with our FISMA and Government Information Security Reform Act audits since 2002. To address known weaknesses with GSA's background investigation process, the GSA-CIO should resolve inconsistencies with background investigation requirements in policies, procedures, and task orders, through careful collaboration with the Office of the Chief Acquisition Officer and the Office of the CHCO.

<u>Additional Steps Are Needed to Protect Sensitive Information</u>

The GSA Chief Human Capital Officer (CHCO) and GSA-CIO have not completed all actions necessary to ensure the adequate protection of sensitive information including the implementation of a comprehensive breach notification policy and OMB Memorandum M-06-16 requirements. Issued in June 2006, M-06-16 requires that all agencies encrypt data on mobile devices, implement a 30-minute timeout for remote access and mobile devices, use two-factor authentication for remote access, and log all computer-readable data extracts from databases holding Personally Identifiable Information (PII), ensuring that those extracts are erased within 90 days. Subsequently issued in May 2007, OMB Memorandum M-07-16 requires agencies to develop and implement a breach notification policy within 120 days of the memorandum's issuance and to develop that policy with the proper safeguards in place to protect the information, including M-06-16 requirements. The breach notification policy, completed by the CHCO in response to OMB Memorandum M-07-16, has not comprehensively addressed the timeliness of breach notifications, the source in the Agency of those notifications, and the notification of other agencies or the posting of notifications on the web. This means that GSA officials may not respond to a data breach in a timely, effective, and comprehensive manner.

Incomplete implementation of M-06-16 requirements was reported in a March 2008 audit report on GSA's Privacy Act Program, which recommended implementing remaining controls required by M-06-16 for systems maintaining PII. The audit report also recommended that the CHCO work closely with the CIO to: 1) ensure that the Privacy Act Program is integrated with the Agency's security program and assesses risk with and identifies controls for all PII, including PII residing outside of major IT systems; 2) periodically assess the need for and potential uses of automated content management and data leakage tools or other procedures to assist in identifying and protecting PII within GSA's IT and system environment; 3) confirm that required security hardening guides are being followed and that vulnerabilities are promptly recorded and mitigated for major IT systems that collect and store PII; and 4) develop a plan that includes the key activities, milestones, and performance measures necessary to guide GSA in discontinuing the collection and storage of social security numbers in IT systems where no longer required. Subsequent to the Privacy Act Program report, the GSA CHCO issued a new rules and consequences policy[5] instructional letter on July 29, 2008. Our FISMA review did not consider implementation of this new policy.

Within GSA, primary management control responsibilities for protecting sensitive information, including PII, are dispersed among several key officials. The CHCO is the Senior Agency Official for Privacy, the GSA official responsible for establishing and overseeing the Agency's Privacy Act Program and for ensuring GSA's compliance with privacy laws, regulations and GSA policy. The GSA-CIO has overall responsibility for the Agency's IT Security Program. The GSA-CIO has included M-06-16 requirements in the GSA IT Security Policy and implemented a 30-minute timeout for remote access and mobile devices. However, GSA has not implemented encryption of mobile devices and two-factor authentication for remote access. GSA's laptops with encryption are primarily new devices or those that have been identified as containing PII. Without an emphasis on completing mobile device encryption, the remaining laptops containing unidentified PII or other types of sensitive data may be at risk in the event a laptop is lost or stolen. As of August 2008, two years after M-06-16 was issued, less than 1,800 of the 8,000 laptop computers identified by GSA have been encrypted. At the current rate, GSA will not accomplish the encryption solution roll-out planned to be completed by December 2008. Further, GSA's scheduled implementation of two-factor authentication is dependent on the full deployment of Personal Identity Verification (PIV) cards required by HSPD-12. However, only 35 percent of employees and 2 percent of contractors have received their PIV cards, as of June 2008. This places GSA in jeopardy of missing the planned completion date of September 2009 for implementing two-factor authentication. To promptly fulfill implementation responsibilities for M-06-16 and M-07-16 and address these system security weaknesses, the GSA-CIO should expedite efforts to effectively protect all sensitive information, including PII.

Publicly Facing Web Sites Were Not Consistently Secured

GSA has not consistently secured its public web presence through: 1) the protection of login credentials, 2) support for required encryption, and 3) consistent use of government domains. First, we assessed 38 of GSA's publicly facing web applications and identified nine that did not employ encryption to protect login credentials. Without encryption, these credentials may be susceptible to compromises of privacy and confidentiality of data, regardless of whether it is being transmitted or stored on a computer when encrypted. Specifically, when proper protection mechanisms are not used, transmitted usernames and passwords are susceptible to eavesdropping attacks, disclosing the credentials to attackers. NIST SP 800-53 (control IA-5) states that password-based authentication should protect passwords from unauthorized disclosure and modification when stored and transmitted. In addition, there is an increased risk of compromise of other systems, if individuals use the same password on multiple systems. Second, our assessment identified an additional nine GSA publicly facing web applications that did not support the use of Transport Layer Security (TLS) encryption in conformance with FIPS 140-2 requirements. OMB M-07-11 requires that agencies adopt the Federal Desktop Core Configuration (FDCC) common security configurations for Windows XP or Vista devices, which include web browser settings that will only allow secure connections through TLS encryption. NIST SP 800-53 (control IA-7) requires that information systems employ authentication methods that meet the requirements of the federal standard for authentication to a cryptographic module is FIPS 140-2 (as amended). GSA customers and other system users who have adopted FDCC requirements will not be able to connect to GSA's nine non-compliant sites. Lastly, our assessment identified six GSA publicly facing web applications hosted on *.com* domains, which are not approved for federal websites. The consistent use of government domains is required to provide added confidence and quality to the information provided by Federal

[5] HCO IL-08-1, *GSA Rules of Behavior for Handling Personally Identifiable Information (PII),* July 29, 2008.

agencies. Additionally, the use of non-government domains could increase risks of phishing attacks where deception is used to play on the public's trust of the legitimate entity. OMB M-05-04 states that unless specified by the agency head, all federal agencies are only to use *.gov*, *.mil*, or *Fed.us* domains. These vulnerabilities could be prevented through improved application development processes and enhanced monitoring of GSA's public web presence. To mitigate the risks associated with the Agency's external web presence, the GSA-CIO should enhance monitoring of GSA's public web presence, and ensure that all of GSA's publicly facing web applications: 1) encrypt login credentials, 2) support FIPS 140-2 encryption, and 3) use approved Government domains for GSA web applications.

Risks With Minor Applications Were Not Always Addressed

System officials did not adequately address security requirements for minor applications[6]. For one of the four systems included in this year's FISMA review, the certification and accreditation process did not identify significant risks associated with four reviewed minor applications in the following areas:

1) Databases, web applications, and operating systems were not hardened;
2) The certification and accreditation process did not identify all interconnections and did not identify risk with single sign-on; and
3) The system owner did not perform e-authentication risk assessments.

A contributing cause for control weaknesses in minor applications with this system was that the task order procuring system services contained security requirements, but did not contain sufficient performance-based deliverables that would have alerted system security officials to gaps in adherence to GSA's IT Security Policy, procedures, and hardening guidelines. Specifically, procurement deliverables did not demonstrate that web applications were appropriately secured for the system. Compliance with the GSA IT Security Policy and its requirements is mandatory for all systems, including minor applications. This means that hardening of minor applications should follow NIST and/or GSA guidance to the greatest extent possible. Minor applications should also be covered by e-authentication risk assessments in accordance with OMB M-04-04 when allowing authentication of users for the purpose of conducting government business electronically. Weaknesses in securing minor applications occurred when system owners focused on the major components within their system boundaries and the GSA IT Security policy and its related procedures, including procedural guides for conducting system certifications and accreditations, do not explicitly address minor applications.

In June 2008, an audit of GSA's financial management system identified systematic access control weaknesses with 45 minor web applications that put sensitive data at increased risk for disclosure. The June 2008 financial management system audit report recommended that the Chief Financial Officer work with GSA Services, Staff Offices, and Regions to improve security and privacy controls for sensitive system data, including: 1) strengthening system certification and accreditation processes to ensure that risks with and controls for system interfaces, data criticality and sensitivity, and information sharing are addressed; 2) defining and identifying sensitive Agency, customer, and vendor data maintained in the system and related web applications and feeder systems; 3) considering the use of encryption and/or masking of sensitive data that resides, or is transmitted to, web applications; 4) establishing appropriate access controls for web applications that interface with and/or process system data; and 5) evaluating whether unauthorized access to sensitive system data, including PII residing on financial web applications, was obtained as a result of weaknesses in

[6] According to NIST SP 800-37, a minor application is an application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

security and privacy controls. To ensure system officials address risks with minor applications, the GSA-CIO should carefully consider the adequacy of the Agency’s IT Security Policy and related procedures and more thoroughly address requirements for securing minor applications.

Conclusion

To address deficiencies adversely impacting the effectiveness of GSA’s IT Security Program, additional actions are needed in four areas. More consistent implementation of controls and management oversight of contractors will assist GSA's IT Security Program in more effectively identifying and managing risks for all systems and data. The implementation of a comprehensive breach notification policy and expedited actions to implement OMB requirements will improve protection of sensitive information. Enhanced monitoring of GSA's external web presence will reduce associated risks. Updating policies and procedures to specifically address minor applications will result in improved security.

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. Work with the Office of the Chief Acquisition Officer to develop standard requirements and deliverables for IT service contracts and task orders that promote compliance with GSA IT Security Policy and procedures.
2. Work with the Office of the Chief Acquisition Officer and the Office of the Chief Human Capital Officer to ensure consistent background investigation requirements in policies, procedures, and task orders.
3. Expedite actions to implement encryption of mobile devices and two-factor authentication, and work with the Office of the Chief Human Capital Officer to promptly fulfill responsibilities for implementing a comprehensive breach notification policy.
4. Enhance monitoring of GSA's public web presence and ensure that all of GSA's publicly facing web applications:
   a. Encrypt login credentials.
   b. Support Federal Information Processing Standards (FIPS) Publication 140-2 encryption.
   c. Use approved Government domains for GSA web applications.
5. Ensure that the IT Security Policy thoroughly addresses requirements for the need for securing minor applications.

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 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 controls over GSA systems and data and to address specific questions and reporting requirements identified by OMB. While this audit included a review of management, operational, and technical controls for four GSA systems, we did not test all system controls across the Agency. The Results of Audit and Recommendations sections of this report state, in detail, the need to strengthen specific management, operational, and technical 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 three 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 2008 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A080081/O/T/F08016

APPENDIX A

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

The EXCEL Workbook displayed here is transmitted in a separate file using the format directed by the Office of Management and Budget. Supplemental information submitted with responses to this EXCEL Workbook is also displayed here.

Section C - Inspector General: Questions 1 and 2

Agency Name:	**General Services Administration**	**Submission date:**	**September 11, 2008**

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						
	Moderate	11	1			11	1	1	100%	1	100%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**11**	**1**	**0**	**0**	**11**	**1**	**1**	100%	**1**	100%	**1**	100%
Federal Acquisition Service (FAS)	High			1		1	0						
	Moderate	2		21	1	23	1	1	100%	1	100%	1	100%
	Low	1		3		4	0						
	Not Categorized					0	0						
	Sub-total	**3**	**0**	**25**	**1**	**28**	**1**	**1**	100%	**1**	100%	**1**	100%
Office of the Chief Acquisition Officer (OCAO)	High					0	0						
	Moderate			4		4	0						
	Low	2		1		3	0						
	Not Categorized					0	0						
	Sub-total	**2**	**0**	**5**	**0**	**7**	**0**	**0**		**0**		**0**	
Office of Governmentwide Policy (OGP)	High					0	0						
	Moderate	1		5		6	0						
	Low	4		2		6	0						
	Not Categorized					0	0						
	Sub-total	**5**	**0**	**7**	**0**	**12**	**0**	**0**		**0**		**0**	
Office of the Chief Information Officer (OCIO)	High					0	0						
	Moderate	15	1			15	1	1	100%	1	100%	1	100%
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**15**	**1**	**0**	**0**	**15**	**1**	**1**	100%	**1**	100%	**1**	100%
Office of the Chief Financial Officer (OCFO)	High					0	0						
	Moderate	1		3		4	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**1**	**0**	**3**	**0**	**4**	**0**	**0**		**0**		**0**	
Office of the Chief Human Capital Officer (OCHCO)	High					0	0						
	Moderate			2		2	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**2**	**0**	**2**	**0**	**0**		**0**		**0**	
Office of Inspector General (OIG)	High					0	0						
	Moderate	1				1	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Office of General Counsel (OGC)	High					0	0						
	Moderate					0	0						
	Low	1	1			1	1	1	100%	1	100%	1	100%
	Not Categorized					0	0						
	Sub-total	**1**	**1**	**0**	**0**	**1**	**1**	**1**	100%	**1**	100%	**1**	100%
Board of Contract Appeals (BCA)	High					0	0						
	Moderate					0	0						
	Low	1				1	0						
	Not Categorized					0	0						
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**		**0**		**0**	
Office of Citizen Services and Communications (OCSC)	High					0	0						
	Moderate					0	0						
	Low			2		2	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**2**	**0**	**2**	**0**	**0**		**0**		**0**	

Section C - Inspector General: Questions 1 and 2

Agency Name:	**General Services Administration**	**Submission date:**	**September 11, 2008**

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
Office of Emergency Response and Recovery (OERR)	High					0	0						
	Moderate			1		1	0						
	Low					0	0						
	Not Categorized					0	0						
	Sub-total	**0**	**0**	**1**	**0**	**1**	**0**	**0**		**0**		**0**	
Agency Totals	**High**	**0**	**0**	**1**	**0**	**1**	**0**	**0**		**0**		**0**	
	Moderate	**31**	**2**	**36**	**1**	**67**	**3**	**3**	100%	**3**	100%	**3**	100%
	Low	**9**	**1**	**8**	**0**	**17**	**1**	**1**	100%	**1**	100%	**1**	100%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**		**0**		**0**	
	Total	**40**	**3**	**45**	**1**	**85**	**4**	**4**	100%	**4**	100%	**4**	100%

🟨 = Data Entry Cells

⬜ = Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

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

Frequently (71-80% 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) {must be 23-digits}	Agency or Contractor system?
	See supplemental information.		

Number of known systems missing from inventory:	

🟨 = Data Entry Cells

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 four systems reviewed have a POA&M and system and Agency POA&Ms included 125 of 128 weaknesses (97.6%). While almost all identified IT security weaknesses are managed in the POA&M process, a weakness identified by an OIG audit report related to the protection of PII was not included in the Agency POA&M. See attached supplemental information.	

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 certification and accreditation (C&A) process includes FIPS 199 system impact level determinations, security assessments, security control testing, incident handling, security awareness and training, and establishes standards for secure configurations. However, inconsistent implementation and insufficient management oversight of contractors continue to prevent GSA's IT security program from being fully effective in identifying and managing risks for all systems and data. One of four systems reviewed this year did not adequately address minor applications in the C&A process. See attached supplemental information.

Section C - Inspector General: Questions 6, 7, and 8

Agency Name:	**General Services Administration**	
	Question 6-7: IG Assessment of Agency Privacy Program and Privacy Impact Assessment (PIA) Process	
6	**Provide a qualitative assessment of the agency's Privacy Impact Assessment (PIA) process, as discussed in Section D Question #5 (SAOP reporting template), including adherence to existing policy, guidance, and standards.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
Comments:	GSA has a written policy or process for PIAs that addresses determining whether a PIA is needed, conducting a PIA, completing the PIA Report, ensuring that systems owners and privacy and information technology experts participate in conducting the PIA, making PIAs available to the public in the required circumstances, and making PIAs available in other than required circumstances. For each of the systems reviewed, a PIA has been completed that adheres to existing policy, guidance, and standards, if applicable. However, the Privacy Act Program has not yet ensured that PII stored on laptops and servers or in databases or applications that are not considered part of a major IT system is identified and protected. See attached supplemental information.	
7	**Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-07-16 Safeguarding Against and Responding to the Breach of Personally Identifiable Information.** Response Categories: - Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	Satisfactory
Comments:	While a breach notification policy has been developed and implemented, the breach notification policy does not address the timeliness of the notification of individuals affected by breaches and does not address who will notify affected individuals. Further, three of four M-06-16 requirements reiterated in M-07-16 are not yet met. GSA conducted a survey of the use of PII/SSNs, which identified systems where the use of PII/SSNs was superfluous, and those systems were informed that the use of PII/SSNs should be halted. See attached supplemental information.	
	Question 8: Configuration Management	
8.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. See attached supplemental information. See attached supplemental information.	
8.b.	**Approximate the extent to which applicable systems implement common security configurations, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.** **Response categories:**	Mostly (81-95% of the time)
	- 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	
8.c.	**Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:**	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

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

Agency Name:	General Services Administration

Question 9: 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.

9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov)	Yes
9.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 four systems we reviewed. See attached supplemental information.	

Question 10: 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 11: Collaborative Web Technologies and Peer-to-Peer File Sharing

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

Question 12: E-Authentication Risk Assessments

12.a. Has the agency identified all e-authentication applications and validated that the applications have operationally achieved the required assurance level in accordance with the NIST Special Publication 800-63, “Electronic Authentication Guidelines”? Yes or No.	No
12.b. If the response is “No”, then please identify the systems in which the agency has not implemented the e-authentication guidance and indicate if the agency has a planned date of remediation.	One reviewed system, PBS Corporate, has not validated the operational assurance level of an e-authentication application, and has a planned remediation date of January 30, 2009. See attached supplemental information.

Supplemental Information – FY 2008 GSA OIG FISMA Reporting Template

This supplemental information provides a brief explanation of the basis for our responses to each question in the FY 2008 GSA OIG FISMA reporting template.

Question 1

The GSA inventory of systems is maintained by the GSA-CIO.

Question 2

Responses to question 2 are based on our representative subset of four GSA systems.

Question 3

Question 3.a –We identified deficiencies with evaluated NIST SP 800-53 security controls for one contractor system in our representative subset of GSA systems. Overall, insufficient management oversight of contractors continue to prevent GSA's IT Security Program from being fully effective in identifying and managing risks for all systems and data, as evidenced by configuration management weaknesses and inconsistent contractor background investigations.

Question 3.b – We did not identify any Exhibit 53 systems that are not included on the inventory. However, not all system interconnections were appropriately identified with systems reviewed this year. One of the four systems we reviewed did not identify interfaces with other GSA systems. Additionally, an FY 2008 audit of a GSA financial management system determined that the certification and accreditation process for the system did not ensure that risks with sensitive data and system interfaces were assessed and necessary controls implemented.

Question 3.c – We did not identify any Exhibit 53 systems that are not included on the inventory.

Question 3.d – We did not identify any Exhibit 53 systems that are not included on the inventory. However, instances of application service providers maintaining GSA data outside of the Exhibit 53 process have been identified. Since these application service providers were not procured through an IT vehicle, they have no visibility in GSA's annual OMB Exhibit 53, which identifies GSA's IT investment portfolio. Neither the GSA Office of the Senior Agency Information Security Officer nor the Service Office of the CIO had any record of these applications.

Question 3.e – The agency inventory has been updated at least annually.

Question 3.f – We did not identify any Exhibit 53 systems that are not included on the inventory. See comments in Question 3.d above.

Question 4

Question 4.a – System and Agency POA&Ms included 125 of 128 weaknesses (97.6%). While almost all identified IT security weaknesses are managed in the POA&M process, a weakness identified by an OIG audit report related to the protection of PII was not included in the Agency POA&M.

Question 4.b – Across the four systems we reviewed, a total of 121 of 123 weaknesses (98.4%) were included on system POA&Ms.

Question 4.c – For each of the systems in our representative subset of GSA systems, the POA&M is updated quarterly with the latest vulnerabilities and remediation progress.

Question 4.d – All reviewed systems submitted POA&Ms on at least a quarterly basis.

Question 4.e – The Agency POA&M included 34 of 35 (97.1%) IG findings related to GSA's Agency-wide Program. A weakness identified by an OIG audit report related to the protection of PII was not included in the Agency-wide POA&M.

Question 4.f – Weaknesses were prioritized on all reviewed system POA&Ms.

Question 5

Question 5.a – GSA's certification and accreditation (C&A) process includes FIPS 199 system impact level determinations, security assessments, security control testing, incident handling, security awareness and training, and establishes standards for secure configurations. However, inconsistent implementation and insufficient oversight continue to prevent GSA's IT security program from being fully effective in identifying and managing risks for all systems and data. One of four systems reviewed this year did not adequately address minor applications in the C&A process.

Question 5.b – Our qualitative assessment included or considered the following aspects of the C&A process: security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, and configurations/patching.

Question 6

GSA has a written policy or process for PIAs that addresses determining whether a PIA is needed, conducting a PIA, completing the PIA Report, ensuring that systems owners and privacy and information technology experts participate in conducting the PIA, making PIAs available to the public in the required circumstances, and making PIAs available in other than required circumstances. For each of the systems reviewed, a PIA has been completed that adheres to existing policy, guidance, and standards, if applicable. However, the Privacy Act Program has not yet ensured that PII stored on laptops and servers or in databases or applications that are not considered part of a major IT system is identified and protected.

Question 7

While a breach notification policy has been developed and implemented, the breach notification policy does not address the timeliness of the notification of individuals affected by breaches and does not address who will notify affected individuals. Further, three of four M-06-16 requirements reiterated in M-07-16 are not yet met. GSA conducted a survey of the use of PII/SSNs, which identified systems where the use of PII/SSNs was superfluous, and those systems were informed that the use of PII/SSNs should be halted.

Question 8

Question 8.a - 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.

Question 8.b – Across the four systems we reviewed, we assessed implementation of common security configurations for operating systems on 72 devices and found two not appropriately secured. In the same four systems, we assessed implementation of common security configurations for six databases and found three not appropriately secured. For this sample, 73 of 78, or 94% of applicable NIST common security configurations were applied.

Question 8.c.1 – An agency FDCC standard configuration has been established and deviations have been documented and reported to OMB.

Question 8.c.2 - FDCC settings have been established only for Windows XP and Vista. The FAR language referenced is effective March 31, 2008. GSA's common security settings-related contract was established before the March 31, 2008 FAR clause, and, therefore, GSA has not issued any contracts that require the new FAR 2007-004 language.

Question 8.c.3 - Not all GSA Windows XP computing systems have implemented FDCC security settings.

Question 9

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 four systems we reviewed.

Question 10

As of September 9, 2008, the Office of the CIO confirmed that all users have completed security and awareness training. GSA's CIO administered security and awareness training program is limited to the 14,957 individuals with an active GSA email account. System owners are responsible for separately providing GSA's security training to those without GSA email accounts and this process is not being managed by the GSA IT security program. Fourteen contractors without an active GSA email were identified that did not complete GSA's security and awareness training. All contractors who should be receiving IT security training have not been identified.

Question 11

GSA's IT security awareness training explains policies regarding the use of collaborative web technologies and peer-to-peer file sharing.

Question 12

One reviewed system, PBS Corporate, has not validated the operational assurance level of an e-authentication application, and has a planned remediation date of January 30, 2009.

FY 2008 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A080081/O/T/F08016

APPENDIX B

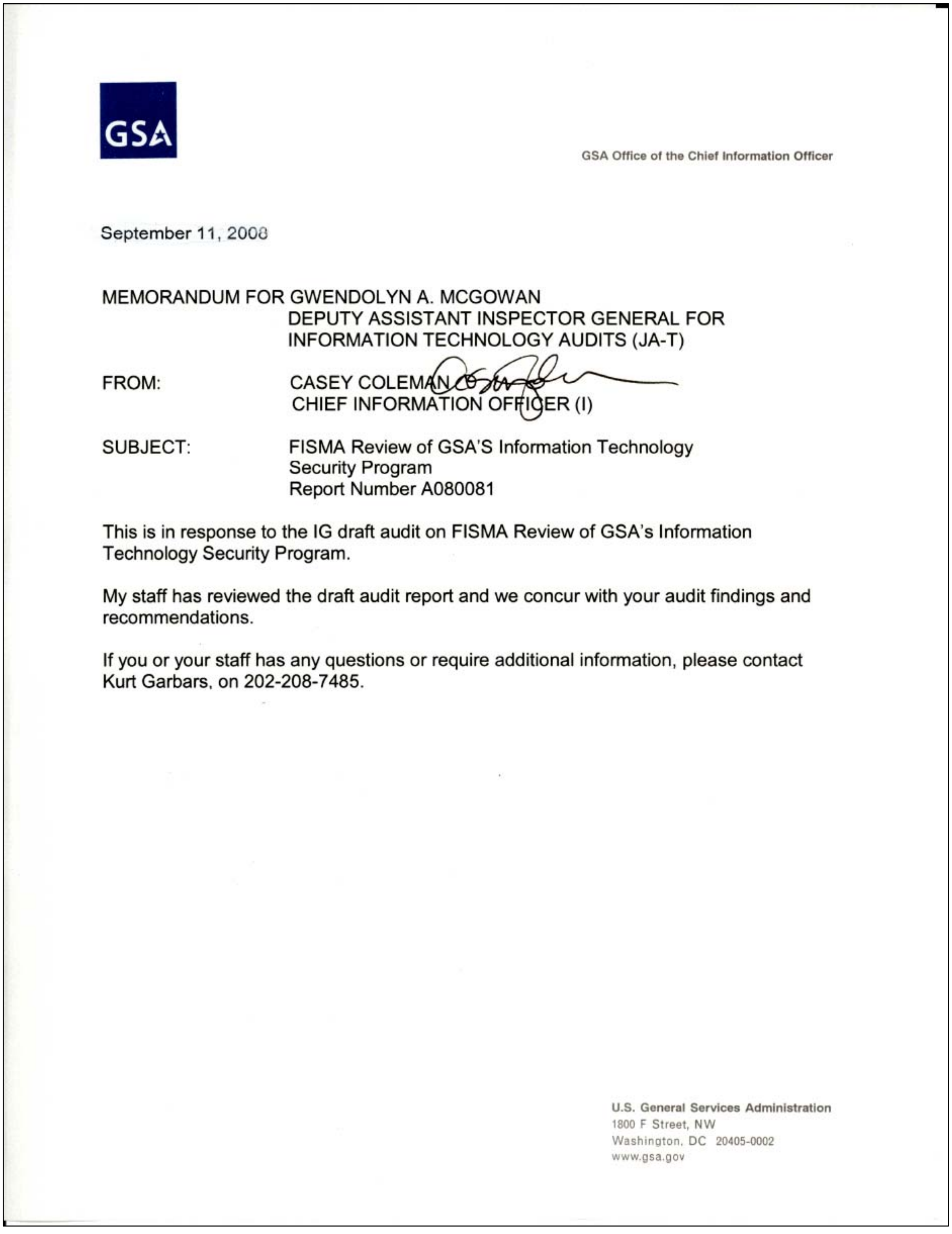
SYSTEM SECURITY AUDITS CONDUCTED BY THE OFFICE OF INSPECTOR GENERAL IN 2008

System	Owner	Description
PBS Corporate	Public Buildings Service (P)	PBS Corporate, also known as the Enterprise Service Center (ESC), is a general support system categorized as moderate risk. PBS Corporate is a federal system that is operated by contractors and owned by the Public Buildings Service. The system includes 41 minor applications and hosts PBS's national applications, including eLease, IRIS, and OA Tool. PBS Corporate provides the hardware and the necessary facilities for the operation of all of its applications and provides common security controls for PBS national applications.
Region 7 LAN	Office of the Chief Information Officer (I)	The Region 7 LAN provides network connectivity services within the Ft. Worth, Texas, Regional Office Building and for field offices throughout the five state region, and encompasses user workstations, telecommunications equipment (including hubs and switches), and test platforms. The Region 7 LAN is a general support system categorized as moderate risk owned by the GSA Office of the CIO.
Office of General Counsel (OGC) LAN	Office of General Counsel (L)	The OGC LAN supports activities for the OGC and the Office of Civil Rights by providing connectivity and electronic communications for the purpose of legal research, word processing, document management, file sharing, and Internet connectivity. The OGC LAN is a general support system categorized as low risk, owned and operated by the OGC. The system includes approximately 17 application, database, web portal, and file servers.
Regional Business Applications (RBA)	Federal Acquisition Service (Q)	RBA supports GSA's acquisition-related, financial processing worth billions of dollars to GSA. RBA is made up of two components, IT Solutions Shop (ITSS) and Integrated Task Order Management System (ITOMS), which are supported by the Common Oracle Database (CODB) as the data repository for both systems. RBA is a contractor system owned by the FAS, Office of the Chief Information Officer, and is a major application categorized as a moderate risk system.

FY 2008 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A080081/O/T/F08016

APPENDIX C

GSA CIO'S RESPONSE TO DRAFT AUDIT REPORT



GSA

GSA Office of the Chief Information Officer

September 11, 2008

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

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: FISMA Review of GSA'S Information Technology
Security Program
Report Number A080081

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 2008 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A080081/O/T/F08016

APPENDIX D

REPORT DISTRIBUTION

	Copies
Chief Information Officer (I)	3
Commissioner, Public Buildings Service (P)	1
Commissioner, Federal Acquisition Service (Q)	1
General Counsel (L)	1
Chief Acquisition Officer (V)	1
Chief Human Capital Officer (C)	1
Regional Administrator, Greater Southwest Region (7A)	1
Internal Control and Audit Division (BEI)	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 Real Property Audits (JA-R)	1
Deputy Assistant Inspector General for Acquisition Audits (JA-A)	1
Administration and Data Systems Staff (JAS)	1
Assistant Inspector General for Investigations (JI)	1