# FY 2005 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A050174/O/T/F05024

**September 21, 2005**

**U.S. GENERAL SERVICES ADMINISTRATION**
Office of Inspector General

Date: September 21, 2005

Reply to Attn of: Deputy Assistant Inspector General for Auditing
Information Technology Audit Office (JA-T)

To: Michael W. Carleton
Chief Information Officer (I)

Subject: FY 2005 Office of Inspector General FISMA Review of GSA's
Information Technology Security Program
Report Number A050174/O/T/F05024

This audit report presents the results of our annual independent evaluation of the General Services Administration (GSA's) progress in implementing the Federal Information Security Management Act (FISMA), which was passed as part of the E-Government Act of 2002 (Public Law 107-347). While steps have been taken to improve GSA's IT Security Program, we found inconsistent implementation of the program by system owners for the systems we reviewed. Since last year, your office has initiated new measures to better secure GSA systems including updating GSA's IT Security policy and procedures based on recent federal guidance, reviewing certification and accreditation packages for consistency with agency policy and procedures, and updating the agency's inventory of IT systems covered under the IT Security Program to include all IT investments. However, our review of ten GSA systems and the agency's IT Security Program identified key areas where additional improvements are needed. Our response to the Office of Management and Budget's (OMB's) specific FISMA questions is included as Appendix A. Written comments that you provided to our draft report are included as Appendix E.

I wish to express my appreciation to you, your staff, and officials with system security responsibilities, whose cooperation enabled us to meet the tight timeframes for reporting to the OMB and the Congress. If you have any questions regarding our FISMA review, please contact me or Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits on 703-308-1223.

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

# FY 2005 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## TABLE OF CONTENTS

APPENDICES

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## EXECUTIVE SUMMARY

### Purpose

This audit report presents the results of the Inspector General's Fiscal Year (FY) 2005 independent evaluation of the General Services Administration's (GSA) Information Technology (IT) Security Program and controls for select systems as required by the Federal Information Security Management Act of 2002 (FISMA). The objective of the audit was to assess the effectiveness of GSA's IT Security Program and practices for select systems, and respond to specific questions posed in the Office of Management and Budget's (OMB) FY 2005 reporting guidance for FISMA. This audit report is provided for inclusion as an appendix in GSA's FY 2005 FISMA report and FY 2007 budget submission to the OMB.

### Background

FISMA provides a comprehensive framework for (1) ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; (2) development and maintenance of minimum controls required to protect Federal information and information systems; and (3) improved oversight of agency information security programs.

### Results-in-Brief

While steps have been taken to improve GSA's IT Security Program, our review found management, operational, and technical control weaknesses that require management attention. System owners had not consistently implemented GSA's IT Security Program, thus exposing agency systems to undue risk. System certification and accreditation packages were not always complete and testing of contingency plans continues to be an area of risk. Patch management processes were not in place to ensure the timely mitigation of known vulnerabilities for contractor maintained devices that had not been securely configured. Oversight and evaluation of security controls for subcontractors and third party system interconnections was not consistently performed by system owners for contractor provided solutions. Finally, background checks were not performed for contractors before they were granted access to GSA systems, a condition reported in 2003 and 2004. Overall, system owners continue to demonstrate that more consistent implementation of GSA's IT Security Program and increased system monitoring is needed. Responses to specific OMB FISMA questions are included in Appendix A.

## Recommendations

To improve security over GSA's data and information technology assets, we recommend that the GSA-CIO take actions to:

1) Increase oversight of GSA's Information Technology Security Policy and procedure implementation related to certification and accreditation to ensure that:
   a) Security for third party interconnections is assessed and evaluated as part of system certification and accreditation.
   b) Certification and accreditation documentation, including risk assessments, security plans, security plan testing and evaluations, and plans of action and milestones are current and complete.

2) Develop and implement procedures to ensure completion and maintenance of system contingency plans as part of the Certification and accreditation process, and clarify roles, responsibilities, and requirements for comprehensive system contingency plan testing.

3) Develop an enterprise-wide approach to patch management and vulnerability scanning to include identification of tools and processes to clarify roles and responsibilities for system owners in managing risks for their systems, including devices maintained by vendors.

4) Expand the quarterly technical vulnerability scanning program provided by the Office of the Senior Agency Information Security Officer to include oversight and evaluation of system owners' application of hardening guides for routers, switches, and devices maintained by vendors.

5) Identify and promote the adoption of compensating controls across GSA to minimize risks where persons were granted access to systems or data prior to the completion of required background checks.

## Management Comments

The GSA-CIO concurred with the findings and recommendations outlined in this report.

# INTRODUCTION

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) 2005 independent evaluation of the General Services Administration's (GSA) agencywide Information Technology (IT) Security Program and controls for select systems as required by FISMA.

## 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. Our response to specific questions outlined in the Office of Management and Budget (OMB) FY 2005 reporting guidance for FISMA is included in Appendix A. This audit report is provided for inclusion as an appendix in GSA's FY 2005 FISMA report and FY 2007 budget submission to the OMB.

We met with agency IT security officials in the GSA Office of the Chief Information Officer and Services, Staff Offices, and Regions (S/SOs/R), including the GSA Chief Information Officer (GSA-CIO), Senior Agency Information Security Officer, and Information System Security Managers and Officers (ISSMs and ISSOs) for select systems. An assessment of security controls for 10 systems across GSA's S/SOs/R was also conducted. Appendix B lists the 10 systems reviewed as part of this audit. We reviewed GSA's agencywide IT Security Policy[1] and procedures, standards, and guidelines for implementing GSA's IT Security Program. To obtain information on 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 800 series security guidelines. We also reviewed GSA's annual financial statement audit report for FY 2004, including management letters and penetration test results.

To assess the effectiveness of GSA's IT Security Program, we reviewed security controls for seven major applications and three general support systems. We examined risk assessments, security plans, system testing and evaluation results, certification and accreditation letters, contingency plans, and system-level Plans of Action and Milestones (POA&M) for each system. We also performed vulnerability scanning on the 10 systems using the StillSecure Vulnerability Assessment and Management tool.

In addition to FISMA, we used other applicable regulations and policies including: OMB Circular A-130 Revised, Appendix III, Security of Federal Automated Information Resources, November 2000; GSA Order CIO P 2100.1B - GSA Information Technology Security Policy, November 4, 2004; GSA's procedural guides on conducting risk assessments, certification and accreditation, incident handling, and related technical hardening guides and standards, available on the GSA-CIO's IT Security Intranet site; NIST Federal Information Processing Standards Publications, and 800 series special publications; and Homeland Security Presidential Directive

[1] GSA Order CIO P 2100.1B - GSA Information Technology Security Policy, November 4, 2004.

(HSPD) 12 “Policy for a Common Identification Standard for Federal Employees and Contractors,” August 27, 2004.

Audit work was performed between April 2005 and September 2005 in accordance with generally accepted government auditing standards.

# RESULTS OF AUDIT

While steps have been taken to improve the General Services Administration's (GSA) Information Technology (IT) Security Program, our review found management, operational, and technical control weaknesses that require management attention. GSA's IT Security Program, including the agencywide policy, procedural and technical guides, and security awareness and training, have been updated to reflect NIST, OMB, and Office of Personnel Management guidance. The GSA-Chief Information Officer (GSA-CIO) has implemented a process to review system Certification and Accreditation (C&A) documentation for consistency with agency policy and NIST guidance and has updated its inventory of information systems covered under the IT Security Program to include all IT investments. The GSA-CIO also employs a vulnerability scanning program to verify implementation of the agency's security configuration policy for approximately 2,000 servers across all agency systems. However, system owners for 10 select systems we reviewed had not consistently implemented GSA's IT Security Program, thus exposing agency systems to undue risk. System C&A packages did not always include a complete risk assessment, security plan, Security Test and Evaluation (ST&E), and Plan of Action and Milestones (POA&M). One general support system had not updated C&A documentation to include controls to mitigate risk with Voice over Internet Protocol (VoIP), and scanning identified several critical level vulnerabilities within the VoIP infrastructure. Testing of contingency plans continues to be an area of risk, as three of ten systems we reviewed did not have tested contingency plans in place. For five of the remaining seven systems, testing was not comprehensive or did not cover critical components of the contingency plans. POA&Ms for two major applications and one general support system did not include specific known system security weaknesses and, as such, it was unclear how risk was being managed for these systems. GSA's IT Security Program was not consistently implemented, as evidenced by risk assessments and security plans that were not comprehensive and by incomplete POA&Ms, both of which were reported as areas needing improvement in 2004. Contractor maintained devices on two general support systems had not been securely configured, including network enabled printers and VoIP servers, which had several critical and major vulnerabilities. Patch management processes were not in place to ensure the timely mitigation of known vulnerabilities for contractor maintained devices. Oversight and evaluation of security controls for subcontractors and third party system interconnections was not consistently performed by system owners for three contractor provided solutions. Finally, background checks were not performed for contractors before granting them access to GSA systems, a condition reported in 2003 and 2004. Overall, system owners continue to demonstrate that more consistent implementation of GSA's IT Security Program and increased system monitoring is needed. Appendix A contains our response to specific FISMA questions, as requested by OMB, which was included with our assessment of the effectiveness of GSA's IT security program and practices for a subset of systems.

**GSA's Certification and Accreditation Process Was Not Consistently Utilized**

The GSA-CIO has developed an IT systems security C&A process, however, the process was not consistently implemented across the systems reviewed. C&As were not updated to reassess risks after major changes for two of ten systems. Risk assessments, security plans, or ST&E results were incomplete and, in one instance, outdated for the systems we reviewed. POA&Ms were not consistently used to manage IT security weaknesses. These conditions confirm that GSA's IT Security Program controls over the C&A process should be strengthened to effectively manage risks.

A general support system in our sample deployed Voice over Internet Protocol (VoIP) without updating its risk assessment and security plan. As a result, technical security weaknesses with the VoIP implementation went undetected. Another general support system moved to a new operating system and combined two networks, but did not address these changes in a subsequent update to the security plan. The impact on security of the system's change in hardware and software was unclear without a reassessment of security controls. GSA's IT Security Policy requires all GSA major applications and general support systems to be certified and accredited at least every three years or whenever there is a significant change to the system's security posture. Information System Security Officers (ISSOs) are responsible for monitoring system security and maintaining security documentation. Post accreditation activities are necessary to maintain the system accreditation status throughout the system life cycle.[2] The current quality control process for C&As has not always been effective in identifying major changes with GSA systems that require a reassessment of risks and controls.

Two major applications and a general support system did not include a threat-likelihood level matrix in their system risk assessment. For one system, which is part of a major application, the C&A did not address specific risk areas and security controls. Another major application's ST&E was over three years old and the ST&Es for one major application and one general support system did not contain plans for correcting or addressing weaknesses.

The GSA-CIO has implemented an agencywide process to track program and system-level POA&M activities on a quarterly basis. However, program officials did not consistently use a POA&M to manage IT security weaknesses. Specifically, two major applications and one general support system supporting GSA did not include security weaknesses identified through the C&A process in their POA&M. One general support system was recording weaknesses from the ST&E in another document, but this document was not noted as being used on the POA&M. For another major application, identified weaknesses were not mitigated within specified timeframes as required in the system accreditation letters. A recent Statement on Auditing Standards 70 (SAS 70) review noted that these weaknesses were removed from the system POA&M, but were not yet resolved. Similar findings with the POA&M process were reported in 2003 and 2004.

Office of Management and Budget (OMB) guidance on FISMA directs agency CIOs and program officials to develop, implement, and manage POA&Ms for all programs and systems

[2] NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," May 2004.

that they operate and control. When using a risk-based approach, security weaknesses with the greatest and most immediate potential impact are addressed first. GSA's IT Security Policy and procedures on POA&Ms are consistent with OMB guidance. POA&Ms should include all security weaknesses found during any other review done by, for, or on behalf of the agency, including Government Accountability Office audits, financial system audits, and critical infrastructure vulnerability assessments. System-level POA&Ms were not always used to effectively manage risks because specific security weaknesses were not identified and tracked.

The GSA-CIO continues to rely on the Information System Security Managers (ISSMs) and ISSOs across the agency to implement the GSA IT Security Policy. Even though the GSA-CIO published the POA&M Implementation Guide in May 2005 to clarify requirements, weaknesses identified through the C&A process were not consistently being recorded on POA&Ms in a timely manner for seven of the ten systems we reviewed. Inconsistent use of the POA&M process resulted in security weaknesses not being promptly tracked and mitigated.

## Contingency Plans Were Not Developed and Tested For Three Systems

Three of ten systems reviewed that were certified and accredited had not developed an IT contingency plan but two had addressed some limited elements of contingency planning in Continuity of Operations Plans (COOP). One contingency plan for a major application did not address all system components and data center sites. While IT contingency plans had been developed for the seven other systems we reviewed, the plans for those systems were missing key elements of contingency planning as outlined by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34.[3] Three of ten systems included in our review had not tested their contingency plans, while the other seven systems had performed limited testing of their contingency plans. The GSA-CIO requires that NIST SP 800-34 be used when performing tasks related to contingency planning. GSA's C&A process, consistent with NIST SP 800-37, does not require the formal development of IT contingency plans as part of C&A, even though contingency plans are essential to system availability and security.

GSA's IT Security Policy requires the development of a contingency plan for each system in accordance with OMB Circular A-130, Appendix III. Two general support systems that provide IT communications and data processing infrastructure for GSA associates in two Regions did not have a documented IT contingency plan developed, but had noted this weakness in their POA&Ms. Security officials for these two general support systems provided a COOP in lieu of an IT Contingency Plan. However, the COOPs did not address recovery procedures for IT operations, and as such, it is unclear how these two general support systems will be able to recover and restore IT operations in the event of a contingency.

While IT contingency plans had been developed for seven of ten systems reviewed, most of these plans were missing key elements of contingency planning as recommended by NIST. Five of seven contingency plans did not include a business impact analysis to identify and prioritize critical system components and identify disruption impacts and appropriate system downtimes. Without a business impact analysis, it is unclear how contingency planning requirements and recovery processes would be prioritized. One contingency plan for a major application did not

[3] NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

address all system components and data center sites. Another major application did not include detailed procedures for system recovery. These conditions could negatively impact the ability to recover from a contingency situation.

Contingency plan testing is a critical component of the contingency planning process that enables plan deficiencies to be identified and addressed, and helps to evaluate the ability of recovery personnel to implement the plan efficiently. NIST recommends that contingency plan testing include all elements of the contingency plan and address six areas: (1) system recovery on an alternate platform, (2) coordination amongst recovery teams, (3) internal and external connectivity, (4) system performance using alternate equipment, (5) restoration of normal operations, and (6) notification procedures. Seven of ten systems had tested their contingency plans, however, testing was not comprehensive in accordance with NIST guidance.

## **System Owners Were Not Comprehensively Identifying and Managing Technical Security Weaknesses**

While the Office of the GSA-CIO has employed a technical vulnerability scanning program to verify implementation of required security configurations for approximately 2,000 servers across the agency, we found that system owners were not routinely identifying and managing technical security weaknesses for their systems. We found technical security vulnerabilities on servers and other network devices that were not included in the scanning performed by the Office of the GSA-CIO. Our scanning identified contractor maintained devices on GSA's network that had not been hardened according to GSA's IT Security Policy. These devices had several critical vulnerabilities that exposed GSA's network to unnecessary risks. Further, there was no patch management process in place for two general support systems to ensure that security vulnerabilities were mitigated in a timely manner. Summary results of technical vulnerability scanning for systems are included in Appendix C.

GSA's IT Security Policy requires ISSOs to evaluate known vulnerabilities, to ensure their systems are patched, and to harden their systems according to GSA-CIO procedural guides. For two general support systems we reviewed, ISSOs were relying on the quarterly vulnerability scanning of servers performed by the Office of the GSA-CIO to identify known vulnerabilities and were not ensuring that their systems were patched and security hardened as required by GSA's IT Security Policy. One Regional office employed VoIP, which included a voicemail server with several critical vulnerabilities that, if exploited, could impact the confidentiality, integrity, and availability of the VoIP system. While system owners advised us that they were in the process of implementing patch/configuration management tools for the Regions, a patch management process to securely configure and harden all system devices to address security vulnerabilities in a timely manner was not in place for these general support systems. As a result, GSA's IT environment was exposed to unnecessary risks.

Vulnerability scans conducted on three contractor provided eGovernment systems behind contractors' firewalls revealed that one contractor was running an HP-UX server that had not been hardened as required. Our scanning found several critical level vulnerabilities on this server that, if exploited, could affect the confidentiality, integrity, and availability of this eGovernment system. The GSA-CIO was not aware that any agency systems were running HP-UX and the ISSO had not ensured that the HP-UX server was hardened and patched in accordance with industry best practices as required by the GSA IT Security Policy. As a result, two actions are needed for system owners to identify and manage technical security weaknesses. An enterprise-wide approach to patch management, as well as technical vulnerability scanning by system owners is needed. More comprehensive monitoring by the GSA-CIO of system devices other than servers would assess the effectiveness of hardening guides and measure the extent of their implementation. These actions would improve security over GSA's data and information technology assets.

## Comprehensive Oversight and Evaluation of Contractors Remains an Issue

While the GSA-CIO has taken steps to ensure the security of contractor provided solutions and services, we found that the ISSO for three contractor provided eGovernment systems that process, store, and transmit Privacy Act information had not ensured that GSA security policies and procedures were being followed by subcontractors and third party system interconnections processing sensitive government data. System owners and ISSOs had not ensured that required background checks had been performed for all contractors supporting the systems reviewed. Furthermore, for background checks that had been completed, there were a number of different types of checks that were performed, which were not always consistent with requirements stated in GSA's IT Security Policy. As such, GSA systems and sensitive Privacy Act data are at an increased risk of being compromised. Appendix D lists the status of background checks for contractors supporting the 10 systems we reviewed by type of check performed.

The GSA-CIO has implemented several controls to provide oversight and evaluation of contractor provided and supported systems. The Office of the GSA-CIO performs quarterly scanning of contractor supported systems and reviews contractors' internal system scanning results. NIST SP 800-26 self-assessments were also performed for all GSA systems including contractor provided/supported systems. However, for three contractor provided eGovernment solutions, the ISSO had not provided comprehensive oversight and evaluation of third party vendors that were receiving and processing Privacy Act Data for government employees since system interconnections had not been authorized as part of the C&A. While the risk assessment for one eGovernment solution identified lack of verification of security for third parties as a risk area, the system owner decided not to verify the security of third parties supporting the eGovernment solution system interconnections. As such, the risk of compromising Privacy Act data by the solution providers supporting the vendors was increased. OMB Circular A-130 Appendix III requires agencies to obtain written management authorization before connecting their IT systems to other systems. NIST guidance recommends that a written authorization be documented in the form of a Memorandum of Agreement or Interconnection Security Agreement. This written authorization should define the rules of behavior and controls that must be maintained for the system interconnection.

In addition, timely completion of background checks for contractor personnel with access to GSA systems and data remains a risk. The GSA-CIO recognized the need for background checks by reporting this security weakness on the agencywide POA&M, and subsequently indicated completion of that item in November 2004. Similar to findings in our 2003 and 2004 FISMA reviews, independent assessments of 10 systems in 2005 found that background checks were not completed for approximately half of the identified contractors allowed access to these systems or data, and the type of background check completed varied widely, as shown in Appendix D. ISSOs were unable to provide the status of background checks for contractors supporting one system.

Subsequent to a recommendation in our 2004 FISMA report, the GSA-CIO revised the background check requirement from a National Agency Check with Inquiries Credit (NACIC) to a Special Agreement Check (SAC) as follows: *"Contractors who design, operate, test, maintain, and/or monitor GSA systems must have at least a background investigation consisting of a Special Agreement Check (SAC) consisting of the following checks: FBI Fingerprint, Security/Suitability Investigations Index (SII), Defense Clearance and Investigations Index (DCII), Immigration and Naturalization Service Master Index (INSMI), and credit."* [1] With the revised policy, system security officials were reminded of their responsibilities to obtain the background checks.

Discussions with the Senior Agency Information Security Officer confirmed that GSA will be required to address background checks in FY 2006 with implementation of Homeland Security Presidential Directive-12 (HSPD-12) on common identification standards for Federal employees and contractors. Under HSPD-12 all Executive Departments and Agencies and independent establishments must issue credentials based on a "National Agency Check with Written Inquiries (NACI)." However, until HSPD-12 is implemented, system owners should be reminded that the lack of completed background checks remains a risk, and that compensating controls should be implemented in all cases where personnel without background checks have already been given access to GSA systems or data.

## RECOMMENDATIONS

To improve security over GSA's data and information technology assets, we recommend that the GSA-CIO take actions to:

1) Increase oversight of GSA's Information Technology Security Policy and procedure implementation related to certification and accreditation to ensure that:
   a) Security for third party interconnections is assessed and evaluated as part of system certification and accreditation.
   b) Certification and accreditation documentation, including risk assessments, security plans, security plan testing and evaluations, and plans of action and milestones are current and complete.

2) Develop and implement procedures to ensure completion and maintenance of system contingency plans as part of the certification and accreditation process, and clarify roles, responsibilities, and requirements for comprehensive system contingency plan testing.

3) Develop an enterprise-wide approach to patch management and vulnerability scanning to include identification of tools and processes to clarify roles and responsibilities for system owners in managing risks for their systems, including devices maintained by vendors.

4) Expand the quarterly technical vulnerability scanning program provided by the Office of the Senior Agency Information Security Officer to include oversight and evaluation of system owners' application of hardening guides for routers, switches, and devices maintained by vendors.

5) Identify and promote the adoption of compensating controls across GSA to minimize risks where persons were granted access to systems or data prior to the completion of required background checks.

## MANAGEMENT COMMENTS

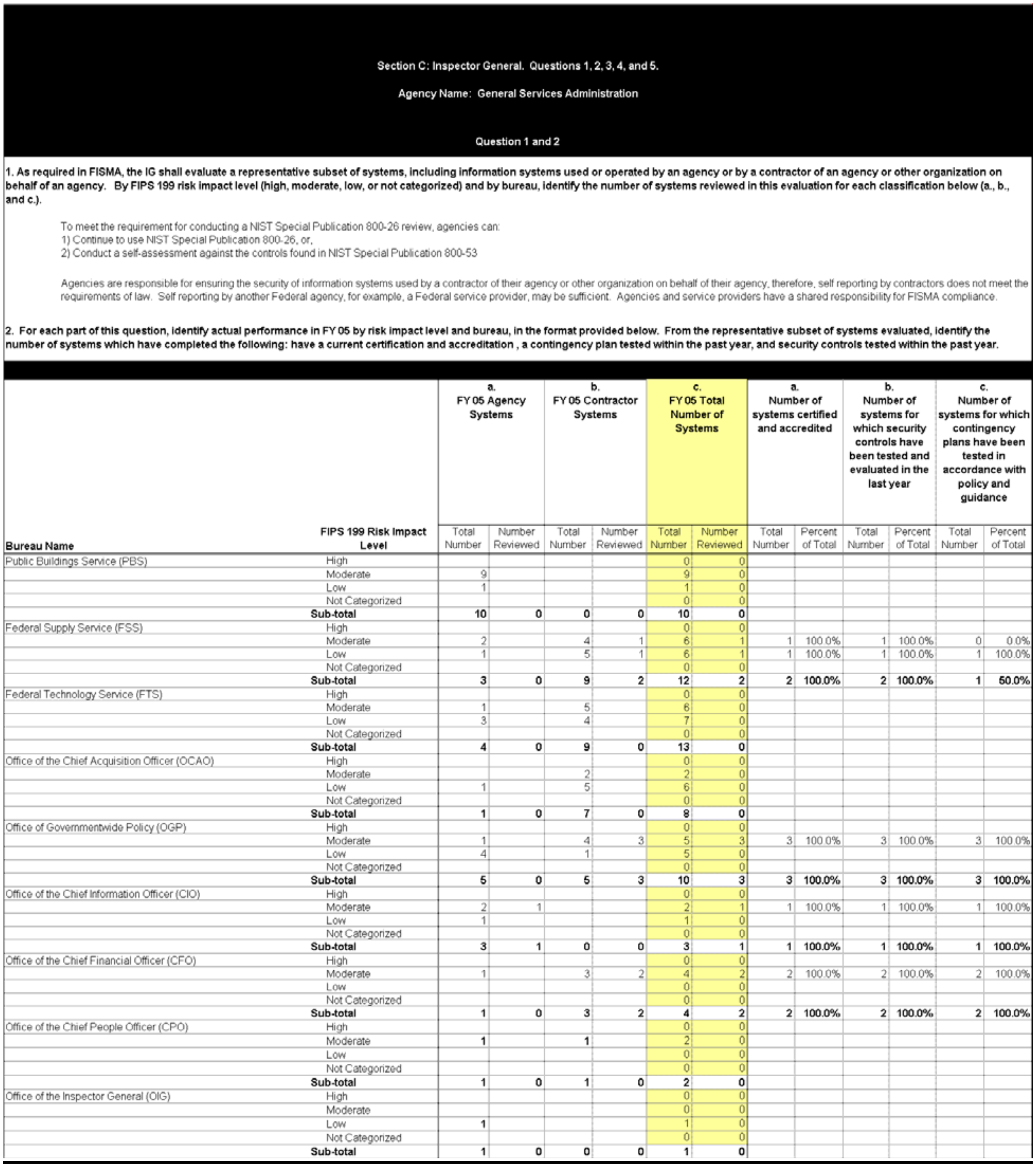
The GSA-CIO concurred with the findings and recommendations outlined in this report. A copy of the GSA-CIO's comments are included in their entirety as Appendix E.

## 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. While this audit included a review of management, operational, and technical controls for 10 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 managerial, operational, and technical controls with the IT Security Program.

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

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



Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: General Services Administration

Question 1 and 2

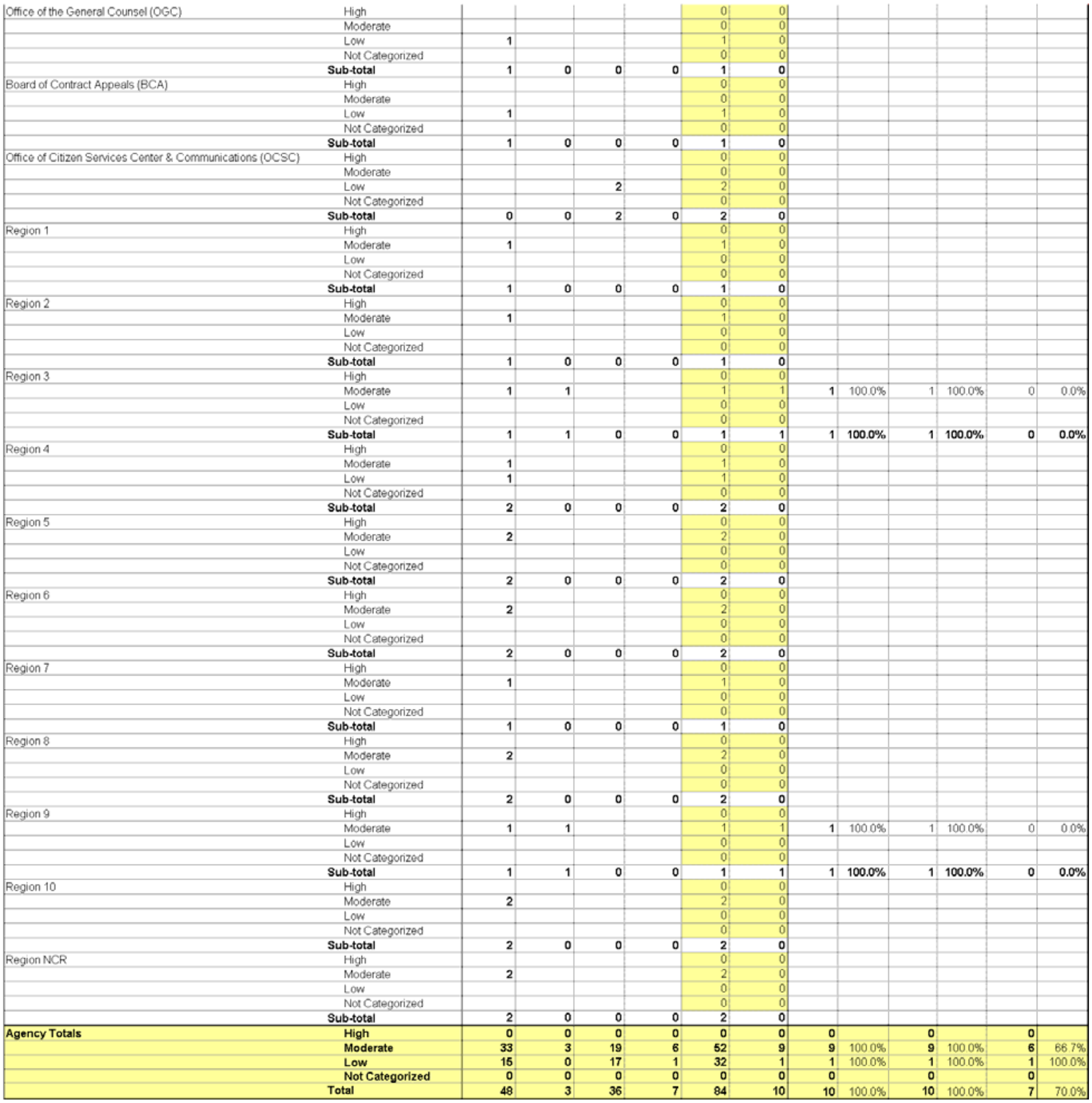
**1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).**

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

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.

**2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.**

| | | a. FY 05 Agency Systems | | b. FY 05 Contractor Systems | | c. FY 05 Total Number of Systems | | a. Number of systems certified and accredited | | b. Number of systems for which security controls have been tested and evaluated in the last year | | c. Number of systems for which contingency plans have been tested in accordance with policy and guidance | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Bureau Name** | **FIPS 199 Risk Impact Level** | Total Number | Number Reviewed | Total Number | Number Reviewed | Total Number | 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 | 9 | | | | 9 | 0 | | | | | | |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **10** | **0** | **0** | **0** | **10** | **0** | | | | | | |
| Federal Supply Service (FSS) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | 4 | 1 | 6 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | Low | 1 | | 5 | 1 | 6 | 1 | 1 | 100.0% | 1 | 100.0% | 1 | 100.0% |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **3** | **0** | **9** | **2** | **12** | **2** | **2** | **100.0%** | **2** | **100.0%** | **1** | **50.0%** |
| Federal Technology Service (FTS) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | 5 | | 6 | 0 | | | | | | |
| | Low | 3 | | 4 | | 7 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **4** | **0** | **9** | **0** | **13** | **0** | | | | | | |
| Office of the Chief Acquisition Officer (OCAO) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | 2 | | 2 | 0 | | | | | | |
| | Low | 1 | | 5 | | 6 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **1** | **0** | **7** | **0** | **8** | **0** | | | | | | |
| Office of Governmentwide Policy (OGP) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | 4 | 3 | 5 | 3 | 3 | 100.0% | 3 | 100.0% | 3 | 100.0% |
| | Low | 4 | | 1 | | 5 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **5** | **0** | **5** | **3** | **10** | **3** | **3** | **100.0%** | **3** | **100.0%** | **3** | **100.0%** |
| Office of the Chief Information Officer (CIO) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | 1 | | | 2 | 1 | 1 | 100.0% | 1 | 100.0% | 1 | 100.0% |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **3** | **1** | **0** | **0** | **3** | **1** | **1** | **100.0%** | **1** | **100.0%** | **1** | **100.0%** |
| Office of the Chief Financial Officer (CFO) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | 3 | 2 | 4 | 2 | 2 | 100.0% | 2 | 100.0% | 2 | 100.0% |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **1** | **0** | **3** | **2** | **4** | **2** | **2** | **100.0%** | **2** | **100.0%** | **2** | **100.0%** |
| Office of the Chief People Officer (CPO) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | **1** | | **1** | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **1** | **0** | **1** | **0** | **2** | **0** | | | | | | |
| Office of the Inspector General (OIG) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | **1** | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | **1** | **0** | **0** | **0** | **1** | **0** | | | | | | |



| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Office of the General Counsel (OGC) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 0 | 0 | 0 | 1 | 0 | | | | | | |
| 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 | | | | | | |
| Office of Citizen Services Center & Communications (OCSC) | High | | | | | 0 | 0 | | | | | | |
| | Moderate | | | | | 0 | 0 | | | | | | |
| | Low | | | 2 | | 2 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 0 | 0 | 2 | 0 | 2 | 0 | | | | | | |
| Region 1 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | | | 1 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 0 | 0 | 0 | 1 | 0 | | | | | | |
| Region 2 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | | | 1 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 0 | 0 | 0 | 1 | 0 | | | | | | |
| Region 3 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | 1 | | | 1 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 1 | 0 | 0 | 1 | 1 | 1 | **100.0%** | 1 | **100.0%** | 0 | **0.0%** |
| Region 4 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | | | 1 | 0 | | | | | | |
| | Low | 1 | | | | 1 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| Region 5 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| Region 6 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| Region 7 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | | | | 1 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 0 | 0 | 0 | 1 | 0 | | | | | | |
| Region 8 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| Region 9 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 1 | 1 | | | 1 | 1 | 1 | 100.0% | 1 | 100.0% | 0 | 0.0% |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 1 | 1 | 0 | 0 | 1 | 1 | 1 | **100.0%** | 1 | **100.0%** | 0 | **0.0%** |
| Region 10 | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| Region NCR | High | | | | | 0 | 0 | | | | | | |
| | Moderate | 2 | | | | 2 | 0 | | | | | | |
| | Low | | | | | 0 | 0 | | | | | | |
| | Not Categorized | | | | | 0 | 0 | | | | | | |
| | **Sub-total** | 2 | 0 | 0 | 0 | 2 | 0 | | | | | | |
| **Agency Totals** | **High** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | |
| | **Moderate** | 33 | 3 | 19 | 6 | 52 | 9 | 9 | 100.0% | 9 | 100.0% | 6 | 66.7% |
| | **Low** | 15 | 0 | 17 | 1 | 32 | 1 | 1 | 100.0% | 1 | 100.0% | 1 | 100.0% |
| | **Not Categorized** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | | 0 | | 0 | |
| | **Total** | 48 | 3 | 36 | 7 | 84 | 10 | 10 | 100.0% | 10 | 100.0% | 7 | 70.0% |

| Question 3 | | |
|---|---|---|
| In the format below, evaluate the agency's oversight of contractor systems, and 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. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.<br><br>Response Categories:<br>- Rarely, for example, approximately 0-50% of the time<br>- Sometimes, for example, approximately 51-70% of the time<br>- Frequently, for example, approximately 71-80% of the time<br>- Mostly, for example, approximately 81-95% of the time<br>- Almost Always, for example, approximately 96-100% of the time | - Almost Always, for example, approximately 96-100% of the time |
| **3.b.** | The agency has developed an 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.<br><br>Response Categories:<br>- Approximately 0-50% complete<br>- Approximately 51-70% complete<br>- Approximately 71-80% complete<br>- Approximately 81-95% complete<br>- Approximately 96-100% complete | - Approximately 96-100% complete |
| **3.c.** | The OIG **generally** agrees with the CIO on the number of agency owned systems. | Yes |
| **3.d.** | The OIG **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 |
| **3.e.** | The agency inventory is maintained and updated at least annually. | Yes |
| **3.f.** | The agency has completed system e-authentication risk assessments. | Yes |

## Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- 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, for example, approximately 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). | - Sometimes, for example, approximately 51-70% of the time |
| **4.c.** | Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress. | - Almost Always, for example, approximately 96-100% of the time |
| **4.d.** | CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis. | - Almost Always, for example, approximately 96-100% of the time |
| **4.e.** | OIG findings are incorporated into the POA&M process. | - Almost Always, for example, approximately 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, for example, approximately 96-100% of the time |

Comments: The General Services Administration - Chief Information Officer (GSA-CIO) has developed an agencywide POA&M process, all ten systems reviewed have a POA&M, and the majority of known IT security weaknesses were being managed in the POA&Ms. However, there was inconsistent implementation of the process. Three systems were not recording and managing all IT security weaknesses through the POA&M process. Two contractor provided major applications did not include weaknesses identified in the their risk assessments and contingency plan test results. Another general support system maintaining a subsidiary record of technical scanning weaknesses failed to record scan results as an overall weakness on the POA&M.

## Question 5

OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

| | | |
|---|---|---|
| | Assess the overall quality of the Department's certification and accreditation process.<br>Response Categories:<br>- Excellent<br>- Good<br>- Satisfactory<br>- Poor<br>- Failing | - Satisfactory |

Comments: The overall OIG assessment of "Satisfactory" resulted from system owners' inconsistent implementation of the GSA CIO's Certification and Accreditation (C&A) process developed in accordance with NIST SP 800-37 and FIPS 199. The GSA-CIO is reviewing system security documentation for consistency with GSA policy and NIST guidance and reports that 85% of agency systems have a current C&A. However, system owners for the ten systems we reviewed had not consistently implemented the process demonstrating the need for more monitoring of implementation. For three general support systems, one had not updated its C&A to reflect risks for Voice over Internet Protocol (VoIP) implementations, another had an outdated ST&E, and the third had an incomplete security plan and risk assessment. For three contractor provided major applications, the C&A did not include an assessment of security been formally authorized by the DAA as required by OMB Circular A-130, Appendix III. One major application did not prioritize and remediate high-risk vulnerabilities within six months as required by the certification letter. Another major application did not have a comprehensive risk assessment or address system interconnection controls in the security plan. ST&E results did not include recommended remediation actions for one system. For another system, the security plan did not include controls for all system components.

**Section B: Inspector General. Question 6, 7, 8, and 9.**

**Agency Name: General Services Administration**

**Question 6**

| | | |
|---|---|---|
| **6.a.** | Is there an agency wide security configuration policy?<br>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. | |
| **6.b.** | Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software. | |

| **Product** | **Addressed in agencywide policy?**<br>**Yes, No, or N/A.** | **Do any agency systems run this software?**<br>**Yes or No.** | **Approximate the extent of implementation of the security configuration policy on the systems running the software.**<br>**Response choices include:**<br>**- Rarely, or, on approximately 0-50% of the systems running this software**<br>**- Sometimes, or on approximately 51-70% of the systems running this software**<br>**- Frequently, or on approximately 71-80% of the systems running this software**<br>**- Mostly, or on approximately 81-95% of the systems running this software**<br>**- Almost Always, or on approximately 96-100% of the systems running this software** |
|---|---|---|---|
| Windows XP Professional | Yes | Yes | - Mostly, or on approximately 81-95% of the systems running this software |
| Windows NT | Yes | Yes | - Sometimes, or on approximately 51-70% of the systems running this software |
| Windows 2000 Professional | Yes | Yes | |
| Windows 2000 Server | Yes | Yes | - Sometimes, or on approximately 51-70% of the systems running this software |
| Windows 2003 Server | Yes | Yes | - Almost Always, or on approximately 96-100% of the systems running this software |
| Solaris | Yes | Yes | - Almost Always, or on approximately 96-100% of the systems running this software |
| HP-UX | No | Yes | |
| Linux | Yes | Yes | |
| Cisco Router IOS | Yes | Yes | - Almost Always, or on approximately 96-100% of the systems running this software |
| Oracle | Yes | Yes | |
| Other. Specify: IIS 4.0 and IIS 5.0 | Yes | Yes | - Almost Always, or on approximately 96-100% of the systems running this software |

Comments: We performed vulnerability scanning on ten select systems to determine the degree of implementation of hardening guides. Our scanning did not include devices that were running Windows 2000 Professional, Linux, or Oracle. For two general support systems, we identified contractor maintained devices operating on Windows NT and Windows 2000 Server that had not been hardened in accordance with GSA's IT Security Policy. These devices had several critical and major level vulnerabilities that could compromise the security of the systems. Further, there was no patch management process in place for these two general support systems to ensure that vulnerabilities were mitigated in a timely manner. We identified one contractor provided major application that was running HP-UX on one server, which had a number of critical and major vulnerabilities. The GSA-CIO has not developed a hardening guide for HP-UX because the one server scanned as part of our assessment is the only known device using HP-UX. Three routers running Cisco IOS included in our vulnerability scanning had been hardened.

| | | |
|---|---|---|
| | **Question 7** | |
| Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below. | | |
| **7.a.** | The agency follows documented policies and procedures for identifying and reporting incidents internally.<br>Yes or No. | Yes |
| **7.b.** | The agency follows documented policies and procedures for external reporting to law enforcement authorities.<br>Yes or No. | Yes |
| **7.c.** | The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov<br>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 ten systems we reviewed. | | |
| | **Question 8** | |
| **8** | Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?<br>Response Choices include:<br>- Rarely, or, approximately 0-50% of employees have sufficient training<br>- Sometimes, or approximately 51-70% of employees have sufficient training<br>- Frequently, or approximately 71-80% of employees have sufficient training<br>- Mostly, or approximately 81-95% of employees have sufficient training<br>- Almost Always, or approximately 96-100% of employees have sufficient training | - Almost Always, or approximately 96-100% of employees have sufficient training |
| | **Question 9** | |
| **9** | Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training?<br>Yes or No. | Yes |

# FY 2005 OFFICE OF INSPECTOR GENERAL
# FISMA REVIEW OF GSA'S INFORMATION
# TECHNOLOGY SECURITY PROGRAM
# REPORT NUMBER A050174/O/T/F05024

## TEN SYSTEMS REVIEWED BY THE OFFICE OF INSPECTOR GENERAL IN 2005

| System | Owner | Description |
|---|---|---|
| SASy<br>(Major Application) | Federal Supply Service<br>(FSS) | The Sales Automation System (SASy) is the FSS automated system to conduct sales of surplus government property in an efficient, expeditious manner and obtain maximum net returns with a minimum of inconvenience to holding agencies. SASy is a contractor supported Privacy Act system categorized as low risk. |
| eOffer<br>(Part of the FSS-19 Major Application) | Federal Supply Service<br>(FSS) | eOffer is an Internet accessible application designed to offer the vendor community an electronic means for submitting contract offers to the GSA FSS and is part of FSS-19. eOffer is a contractor supported system categorized as moderate risk. |
| eTravel EDS<br>(Major Application) | Federal Supply Service<br>(FSS) | Electronic Data Systems (EDS) eTravel provides one of three eGovernment travel solutions whose purpose is to realize operational efficiencies, cost-savings, and increased service to the Federal traveler through a common, automated, and integrated approach to managing Federal Government travel functions. eTravel EDS is a contractor provided hardware and software solution containing Privacy Act data categorized as moderate risk. |
| eTravel CWGT<br>(Major Application) | Federal Supply Service<br>(FSS) | Carlson Wagonlit (CWGT) eTravel provides one of three eGovernment travel solutions whose purpose is to realize operational efficiencies, cost-savings, and increased service to the Federal traveler through a common, automated, and integrated approach to managing Federal Government travel functions. eTravel CWGT is a contractor provided hardware and software solution containing Privacy Act data categorized as moderate risk. |
| eTravel NGMS<br>(Major Application) | Federal Supply Service<br>(FSS) | Northrup Grumman Mission Systems (NGMS) eTravel provides one of three eGovernment travel solutions whose purpose is to realize operational efficiencies, cost-savings, and increased service to the Federal traveler through a common, automated, and integrated approach to managing Federal Government travel functions. eTravel NGMS is a contractor provided hardware and software solution containing Privacy Act data categorized as moderate risk. |
| WABN<br>(General Support System) | Office of the Chief Information Officer (CIO) | Security risks for GSA's Wide Area Backbone Network (WABN) are managed as part of the CIO's Enterprise Infrastructure Operations system. WABN serves as the primary infrastructure for interconnecting GSA's geographic locations and network users. |
| PAR<br>(Major Application) | Office of the Chief Financial Officer<br>(CFO) | The Payroll Accounting and Reporting System (PAR) provides complete payroll functionality for GSA employees and maintains retirement records for submission to the Office of Personnel Management. PAR is a contractor supported system categorized as moderate risk. |
| NEAR<br>(Major Application) | Office of the Chief Financial Officer<br>(CFO) | The National Electronic Accounting and Reporting (NEAR) system is designed to control, record, classify, and summarize financial events to meet requirements of the Federal accounting for annual, multiple year, or no year appropriations and revolving funds. NEAR is a contractor supported system categorized as moderate risk. |
| Region 3<br>PBS LAN<br>(General Support System) | Mid Atlantic Region<br>(R-3) | The Region 3 Public Buildings Service (PBS) Local Area Network (LAN) provides the Information Technology (IT) communications and data processing infrastructure for GSA employees and contractors. This system is categorized as moderate risk. |
| Region 9<br>PBS/FTS LAN<br>(General Support System) | Pacific Rim Region<br>(R-9) | The Region 9 Public Buildings Service/Federal Technology Service (FTS) LAN provides the IT communications and data processing infrastructure for GSA employees and contractors. This system is categorized as moderate risk. |

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## RESULTS OF TECHNICAL VULNERABILITY SCANNING FOR TEN SYSTEMS

Results of technical scanning for known vulnerabilities are presented below. Categorizations of critical, major, and minor vulnerabilities are assigned by our automated scanning tool. All scans were non-intrusive and conducted behind system firewalls with the assistance of system administrators and Information System Security Officers. False positives and vulnerabilities previously identified by systems owners as an acceptable risk have been excluded.

| System | Devices Scanned | Critical Vulnerabilities | Major Vulnerabilities | Minor Vulnerabilities |
|---|---|---|---|---|
| SASy | 6 | 0 | 1 | 3 |
| eOffer | 7 | 0 | 0 | 1 |
| eTravel EDS | 40 | 1 | 1 | 4 |
| eTravel CWGT | 8 | 1 | 2 | 0 |
| eTravel NGMS | 5 | 13 | 4 | 14 |
| WABN | 20 | 10 | 10 | 10 |
| PAR | 21 | 0 | 4 | 3 |
| NEAR | 1 | 0 | 1 | 0 |
| Region 3<br>PBS LAN | 78 (LAN)<br>8 (VoIP) | 66<br>35 | 25<br>7 | 14<br>6 |
| Region 9<br>FTS/PBS LAN | 143 | 14 | 8 | 2 |

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## STATUS OF CONTRACTOR BACKGROUND CHECKS FOR TEN SYSTEMS

Independent assessments of 10 systems found that background checks were not completed for approximately half of the identified contractors allowed access to these systems or data. Background checks are the responsibilities of the System Owner, Information Systems Security Manager and Information System Security Officer.

| System | Number of Contractor Personnel | Background Checks Not Completed | Completed Background Checks By Type[4] | Percent With a Completed Background Check |
|---|---|---|---|---|
| SASy | 5 | 2 | 3 NACIC | 60% |
| eOffer[5] | | | | 0% |
| eTravel EDS | 143 | 82 | 61 Background Investigations[6] | 43% |
| eTravel CWGT | 78 | 0 | 78 Consisting of all or parts of the following: County Criminal Search, Statewide Criminal Search, Federal District Court Criminal Search, Government Watch List, Qualisys Drug Screen, 5 Panel Drug Test, Academic Check, Social Security Number Trace, Professional license, and/or Lexis-Nexis checks | 100% |
| eTravel NGMS | 65 | 50 | 15 DOD Secret Clearance | 23% |
| WABN | 14 | 4 | 10 NACIC | 71% |
| PAR and NEAR[7] | 30 | 21 | 9 NACIC | 30% |
| Region 3 PBS LAN | 17 | 1 | 9 NCIC<br>6 FBI Fingerprint<br>1 Contract Suitability | 94% |
| Region 9 PBS/FTS LAN | 13 | 4 | 9 DHS Limited Check | 69% |

[4] Documentation supporting the type of background checks conducted varied widely by system. NACIC is a National Agency Check with Inquiries Credit. DOD Secret Clearance is a security clearance for classified documents. NCIC is a National Crime Information Center check. FBI fingerprint is a basic criminal check. Contract Suitability check did not define the nature of the background checks. The Department of Homeland Security reported completing an unspecified limited check for one location.

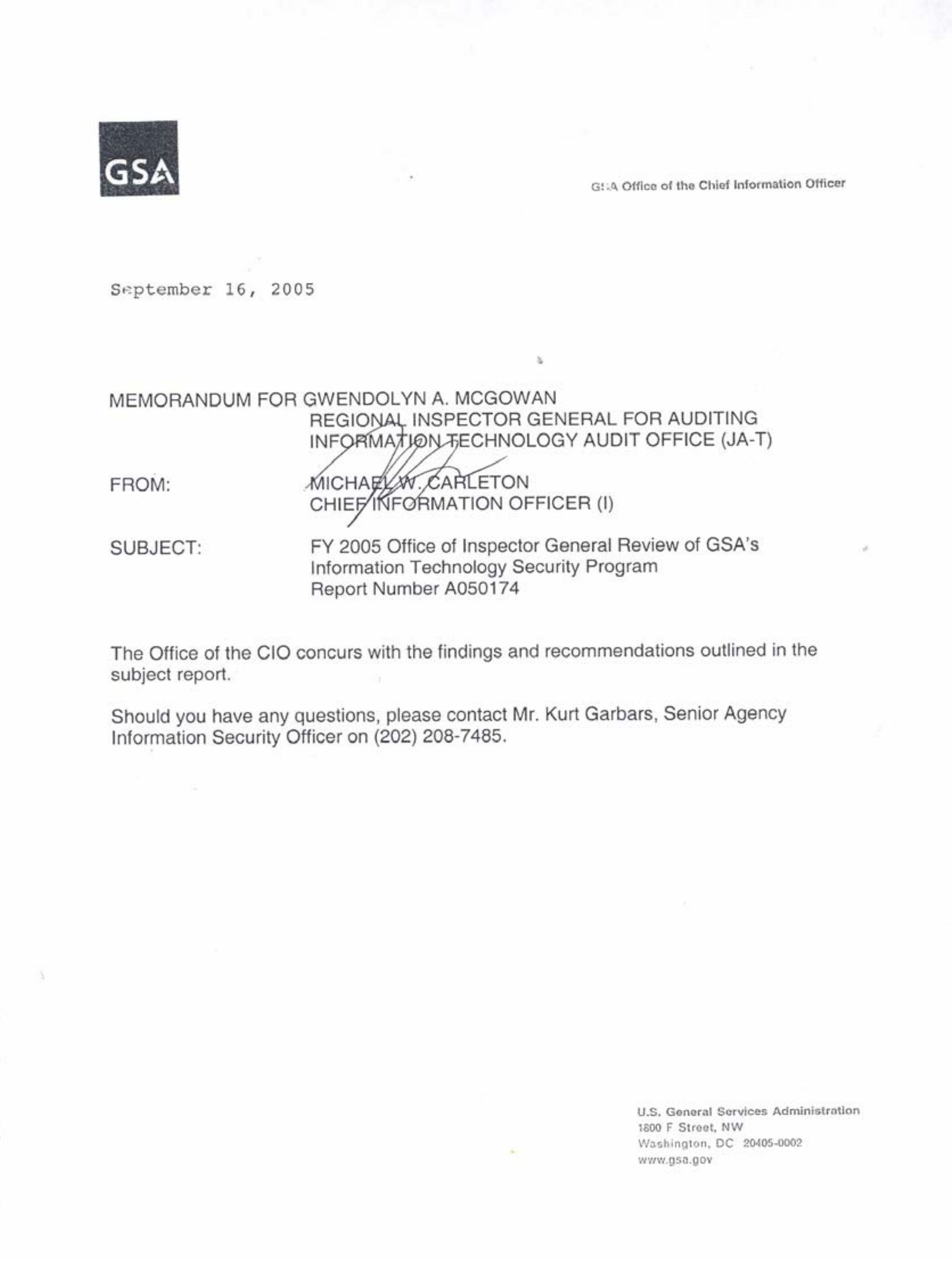
[5] Officials with significant security responsibilities for eOffer did not provide a list of contractor personnel and the status of their background checks.

[6] For the eTravel EDS system, no further information was provided as to the type of background investigations that were completed for contract staff.

[7] Both PAR and NEAR systems are hosted at the same contractor facility and supported by the same staff. Contractor background check numbers posted represent both systems.

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA’S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## GSA CIO’S RESPONSE TO DRAFT AUDIT REPORT



GSA

GSA Office of the Chief Information Officer

September 16, 2005

MEMORANDUM FOR GWENDOLYN A. MCGOWAN
REGIONAL INSPECTOR GENERAL FOR AUDITING
INFORMATION TECHNOLOGY AUDIT OFFICE (JA-T)

FROM: MICHAEL W. CARLETON
CHIEF INFORMATION OFFICER (I)

SUBJECT: FY 2005 Office of Inspector General Review of GSA’s
Information Technology Security Program
Report Number A050174

The Office of the CIO concurs with the findings and recommendations outlined in the subject report.

Should you have any questions, please contact Mr. Kurt Garbars, Senior Agency Information Security Officer on (202) 208-7485.

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405-0002
www.gsa.gov

FY 2005 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA’S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A050174/O/T/F05024

## REPORT DISTRIBUTION

| | Copies |
|---|---|
| Office of the Chief Information Officer (I) | 3 |
| Office of the FSS Chief Information Officer (FI) | 1 |
| Office of the Chief Financial Officer (B) | 2 |
| Office of the Chief People Officer (C) | 1 |
| Mid-Atlantic Region 3 (3A) | 1 |
| Pacific Rim Region 9 (9A) | 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 |
| Regional Inspector General for Auditing (JA-3 and JA-9) | 2 |
| Administration and Data Systems Staff (JAS) | 1 |
| Assistant Inspector General for Investigations (JI) | 1 |
| Regional Inspector General for Investigations (JI-3 and JI-9) | 2 |