Audit Report

FY 2006 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A060123/O/T/F06018

September 8, 2006

Office of Inspector General
General Services Administration

OFFICE OF INSPECTOR GENERAL
GSA

Office of Audits

FY 2006 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A060123/O/T/F06018

September 8, 2006

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 8, 2006

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 2006 Office of Inspector General FISMA Review of GSA's
Information Technology Security Program
Report Number A060123/O/T/F06018

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. Efforts to better secure GSA's systems continue, but system security officials do not consistently ensure effective implementation of GSA's IT Security Policy due, in part, to a lack of accountability and the need for program policies and procedures for measuring individual performance. While the Senior Agency Information Security Officer has taken steps over the last year to address previously reported weaknesses, we continue to find instances where system security officials did not ensure that systems were properly protected. We concluded that effective implementation of GSA's IT Security Program at the system level is dependent upon improved accountability for persons with key IT security responsibilities. 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 D.

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)

Attachments

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

TABLE OF CONTENTS

APPENDICES

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

EXECUTIVE SUMMARY

Purpose

The objective of this audit was to assess the effectiveness of the General Services Administration's (GSA's) Information Technology (IT) Security Program and practices for select systems in meeting Federal Information Security Management Act of 2002 (FISMA) requirements. Our response to specific questions outlined in the Office of Management and Budget (OMB) Fiscal Year (FY) 2006 reporting guidance for FISMA is included in Appendix A. This audit report is provided for inclusion as an appendix in GSA's FY 2006 FISMA report and FY 2008 budget submission to the OMB.

Background

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 FY 2006 independent evaluation of the GSA agency-wide IT Security Program and controls for select systems as required by FISMA. Results of prior audits of GSA's IT Security Program have been issued annually since 2001 and included recommendations to address program weaknesses in 2004 and 2005.

Results-in-Brief

Efforts to better secure GSA's systems continue, but system security officials do not consistently ensure effective implementation of GSA's IT Security Policy due, in part, to a lack of accountability and the need for program policies and procedures for measuring individual performance. In our vulnerability scanning of systems reviewed for FISMA, sample systems have shown improvements as evidenced by a decrease in the number of critical vulnerabilities we identified from 140 in 2005 to 19 in 2006. While the Senior Agency Information Security Officer (SAISO) has taken steps over the last year to address previously reported weaknesses, we continue to find instances where Information System Security Officers (ISSOs) and Information System Security Managers (ISSMs) did not ensure that systems were properly secured. We concluded that effective implementation of GSA's IT Security Program at the system level is dependent upon improved accountability for persons with key IT security responsibilities. Further, there is a need for improved policy and procedures to establish standardized performance goals and measures for associates and contractors performing ISSO and ISSM responsibilities, since these individuals do not typically report directly to the Office of the GSA Chief Information Officer (GSA-OCIO). Accountability in the IT Security Program also depends on periodic assessments of performance goal accomplishment for each ISSO and ISSM, and the results of those assessments being provided to the appropriate ISSO, ISSM, and Authorizing Official (AO). Finally, an analysis of technical security controls for web applications and Voice over Internet Protocol (VoIP) implementations found that GSA's IT

Security Program would also benefit from a more proactive approach to addressing emerging IT security risks. Appendix A contains our responses to specific FISMA questions, as requested by OMB.

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. Implement improved accountability for associates and contractors supporting GSA's IT Security Program by taking actions to:
    a. Engage the Administrator's support for developing standardized performance goals and measures for Information System Security Officers and Information System Security Managers across GSA Service, Staff, and Regional Offices, with periodic assessments of performance by the Senior Agency Information System Officer for use in performance evaluations.
    b. Require that contracts and task orders for Information System Security Officer and Information System Security Manager services, in support of GSA systems, include performance requirements similar to goals and measures being established for GSA associates in these roles.
    c. Collaborate with the GSA Personnel Security Requirements Division to identify and implement procedures and controls that effectively ensure prompt initiation of contractor background investigations for individuals accessing GSA systems and data.

2. Strengthen GSA's IT Security Policy and procedures in the following areas:
    a. Develop guidance and directives necessary to establish and monitor IT security performance goals and measures for Information System Security Officers and Information System Security Managers.
    b. Require Senior Agency Information Security Officer approval of Information System Security Officer and Information System Security Manager assignments.
    c. Add the roles of Contracting Officer and Contracting Officer's Technical Representative as persons with IT security responsibilities, and clarify the responsibilities of systems security officials in the background investigation process.
    d. Segregate IT security roles and responsibilities by requiring that one individual cannot be both the Information System Security Officer and Information System Security Manager for a single system.
    e. Clarify the *Contractor Operations* section of the policy to require that task orders, as well as contracts, include appropriate security requirements.

3. Ensure that the Information Technology Architecture Planning Committee, IT Security Subcommittee regularly takes actions to address risks with emerging technologies.

4. Develop and implement technical/hardening guides for securing web applications and Voice over Internet Protocol.

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) 2006 independent evaluation of the General Services Administration's (GSA) agency-wide Information Technology (IT) Security Program and controls for select systems, as required by FISMA. Results of prior audits of GSA's IT Security Program have been issued annually since 2001 and included recommendations to address program weaknesses in 2004 and 2005.

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 2006 reporting guidance for FISMA is included in Appendix A. This audit report is provided for inclusion as an appendix in GSA's FY 2006 FISMA report and FY 2008 budget submission to the OMB.

We met with Agency IT security officials in the GSA Office of the Chief Information Officer (GSA-OCIO) and in Services, Staff Offices, and Regions (S/SO/R), including the GSA Senior Agency Information Security Officer (SAISO), Information System Security Managers (ISSMs), and Information System Security Officers (ISSOs) for select systems. In 2006, we reviewed security controls for 10 systems across GSA, which included six components of larger systems, to assess the comprehensiveness of the implementation of the Agency IT Security Program. Appendix B lists the 10 systems reviewed as part of this audit. We reviewed GSA's agency-wide 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 2005, and the related management letter.

To assess the effectiveness of GSA's IT Security Program implementation, we examined risk assessments, system security plans, security assessment results, certification and accreditation (C&A) letters, contingency plans, and Plans of Action and Milestones (POA&M) for each system. In addition to reviewing the comprehensiveness of documentation, we evaluated additional managerial, technical and operational controls including: vulnerability scanning, database configuration testing, and reviews of environmental and physical security, background investigations, and training. During our FISMA review, we performed a detailed analysis of one web application, initiated a broader review of web application security to address input validation, and issued an Alert Report in May 2006. Office of Inspector General (OIG) Alert

[1] GSA Order CIO P 2100.1C - *GSA Information Technology Security Policy*, February 17, 2006.

Reports are issued when significant, immediate internal audit concerns need to be conveyed to agency management before the completion of an ongoing review.

In addition to FISMA, we reviewed 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 2100.1C - GSA Information Technology Security Policy, February 17, 2006; GSA's procedural guides on conducting risk assessments, C&A, incident handling, and related technical hardening guides and standards, available on the GSA-OCIO's IT Security Intranet site; NIST Federal Information Processing Standards Publications, and 800 series Special Publications (SP); and Homeland Security Presidential Directive (HSPD) 12 "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004.

Audit work was performed between March 2006 and August 2006 in accordance with generally accepted government auditing standards.

RESULTS OF AUDIT

Efforts to better secure GSA's systems continue, but system security officials do not consistently ensure effective implementation of GSA's IT Security Policy due, in part, to a lack of accountability and the need for program policies and procedures that measure individual performance. In our vulnerability scanning of systems reviewed for FISMA, sample systems have shown improvements as evidenced by a decrease in the number of critical vulnerabilities we identified from 140 in 2005 to 19 in 2006. While the Senior Agency Information Security Officer (SAISO) has taken steps over the last year to address previously reported weaknesses, we continue to find instances where Information System Security Officers (ISSOs) and Information System Security Managers (ISSMs) did not ensure that systems were properly secured. We concluded that effective implementation of GSA's IT Security Program at the system level is dependent upon improved accountability for persons with key IT security responsibilities. Further, there is a need for improved policy and procedures to establish standardized performance goals and measures for associates and contractors performing ISSO and ISSM responsibilities, since these individuals do not typically report directly to the GSA Office of the Chief Information Officer (GSA-OCIO). Accountability in the IT Security Program also depends on periodic assessments of performance goal accomplishment for each ISSO and ISSM, and the results of those assessments being provided to the appropriate ISSO, ISSM, and Authorizing Official (AO). Finally, an analysis of technical security controls for web applications and Voice over Internet Protocol (VoIP) implementations found that GSA's IT Security Program would also benefit from a more proactive approach to addressing emerging IT security risks.

Appendix A contains our responses to specific FISMA questions, as requested by OMB. Our responses include assessments of the security of contractor provided solutions and agency systems, including components of larger major applications and general support systems. Components of larger systems were selected, as noted in Appendix B, since it is important that system owners ensure that all applications within defined system boundaries are secured. While all systems reported having a current Certification and Accreditation (C&A), the process was not implemented consistently for systems reviewed, where we identified incomplete risk assessments, system security plans, and security assessments. Three systems did not have properly tested contingency plans. Two systems operated for GSA by contractors were not provided GSA's IT Security Policy and were not being effectively monitored to ensure information was being protected. Background investigations were not requested for one of the two systems.

Standardized IT System Security Performance Goals and Measures Are Not In Place To Establish Accountability in GSA's IT Security Program

Weaknesses in several areas continue in GSA's IT Security Program without standardized IT security performance goals and measures in place to establish accountability for system security officials, despite improving program controls in the areas of vulnerability scanning and continuous monitoring. Again this year, we identified weaknesses with implementation of the C&A process, contractor background investigations, and contractor provided solutions, when IT Security Program processes did not ensure that ISSOs and ISSMs fulfilled their defined roles.

When assessing why we repeatedly find the same weaknesses, we determined that there was little evidence of ISSOs and ISSMs, whether associates or contractors, being held accountable for the security of their systems by Authorizing Officials or the GSA-OCIO. While the GSA-CIO and the SAISO have IT security performance goals and measures, they have limited influence over ISSOs and ISSMs under the supervision of Authorizing Officials in Service, Staff, and Regional Offices responsible for carrying out system security directives.

Recurring findings in three risk areas demonstrate the effects of not having standardized IT security performance goals and measures in place for individuals assigned system security responsibilities in GSA's IT Security Program. For most of the systems we reviewed, the **C&A process** was not being implemented consistently, **background investigations** were not always being requested for contractors working with GSA systems, and security officials were not providing adequate **oversight of contractor provided solutions**.

Certification and Accreditation Process

As reported in previous FISMA audits, the C&A process has not been consistently implemented across the Agency. In 2004, we reported that for the systems we reviewed the C&A process was not implemented consistently, not updated after major system changes, or not completed. We recommended strengthening policy and procedures to better manage risks by incorporating controls to ensure that C&A documentation, including risk assessments, security plans, and security plan testing and evaluations are current and complete. In 2005, we reported that the C&A process was not consistently implemented and recommended that the GSA-OCIO improve security over GSA’s data and IT assets by taking actions to increase oversight of the implementation of GSA’s IT Security Policy and procedures related to C&A. The GSA’s C&A process was revised to include oversight by GSA’s Office of the SAISO. The requirement for an IT security office review of C&A documents should strengthen the process over the next few years, but does not appropriately focus on accountability for system security officials. In 2006, we again found inconsistent implementation of the C&A process where we identified incomplete risk assessments, system security plans, security assessments, and contingency plans for systems reviewed. C&A documentation for a general support system was not updated to address additional functionality of the reviewed component. A contractor provided system did not follow GSA procedural guides when developing C&A documentation. ISSOs and ISSMs should have detected and initiated correction of the deficiencies identified in C&A documentation.

Contractor Background Investigations

Risks resulting from the lack of background investigations on contractors supporting GSA systems have been consistently identified since 2003, when we reported this issue as a significant deficiency. In 2004, we again reported the issue, recognizing a significant backlog in completing required investigations. We recommended developing compensating controls to reduce risks. In 2005, we reported that GSA systems and sensitive Privacy Act Data were at risk of being compromised due to incomplete background investigations and again recommended the identification and adoption of compensating controls. A requirement was added for a completed FBI National Criminal History Check (Fingerprint Check) before initial access to systems is granted. GSA further reduced risks by completing over 1,600 Fingerprint Checks and 568 contractor background investigations of varying types between October 2005 and July 2006. Despite the Agency's efforts, we identified multiple systems where background investigations on contractors supporting GSA systems were not requested during our 2006 reviews. Independent assessments of ten systems found that background investigations were not completed for approximately two thirds of the identified contractors allowed access to these systems or data. The GSA IT Security Policy places responsibility on the ISSO to assist the Data Owner and Authorizing Official in ensuring users have required background investigations. Although the GSA-OCIO has taken action on our recommendations, there are no apparent consequences for non-compliance on the part of system security officials. Appendix C lists the status of background investigations for contractors supporting the ten systems reviewed and the types of checks performed. Data Owners and ISSOs for eight of the nine systems utilizing contractor support personnel had not ensured that all required background investigations were completed. OMB Circular A-130, Appendix III requires that individuals in roles with the ability to bypass significant technical and operational controls be screened prior to performing those roles. We identified systems where contractors were performing key system administrator duties before the completion of their background investigations. One ISSO, whose primary responsibility is not security, incorrectly believed that it was not necessary to conduct background investigations for personnel supporting a contractor provided system on behalf of a GSA program. Under another ISSO, whose primary function is system Team Leader, a less rigorous background investigation than required was requested for contractor support personnel.

Contractor Provided Solutions Not Secured

GSA's IT Security Program has not been effective in consistently enforcing policy and procedures for contractor owned and operated systems supporting GSA programs and maintaining GSA data. In 2004 and 2005, we reported on contractor provided solutions that were not compliant with the Agency IT Security Policy and procedures required by their contracts with GSA. In 2006, as in prior years, contractors providing solutions for GSA were not provided with GSA’s IT Security Policy and procedures by the ISSO, were not adequately monitored for compliance with the Agency IT Security Policy, and were unaware of several vulnerabilities detected during our review. These findings confirm that efforts to implement prior audit recommendations did not consistently improve security for contractor provided solutions. According to the GSA IT Security Policy, it is the responsibility of system security officials, including the ISSO, to ensure the system is operated, used, maintained, and disposed of in accordance with internal security policies and procedures. However, based on our reviews, there has been a consistent lack of accountability to ensure that ISSOs and other officials oversee contractor provided solutions.

The three identified risk areas demonstrate the need to modify the IT Security Program in a way that will help Authorizing Officials ensure the security of their systems, accomplish GSA's FISMA goals, and effectively implement GSA's IT Security Policy. Evaluating performance of ISSOs and ISSMs based on standardized IT security goals and measures, as part of individual performance assessments, would effectively promote implementation and improve accountability. We believe that the GSA-CIO should engage the Administrator’s support for developing standardized performance goals and measures for ISSOs and ISSMs across GSA Service, Staff, and Regional Offices, with periodic assessments of performance based on established measures. The GSA-OCIO should also collaborate with the Office of the Chief Acquisition Officer to develop contract and task order performance requirements when procuring ISSO and ISSM services for GSA systems, similar to the performance goals and measures used for GSA associates in these roles. Making IT security goals and measures a part of the individual performance appraisal process would be the most effective approach to providing accountability, reducing recurring risks, and improving the security of GSA's IT assets.

Additions and Modifications to GSA's IT Security Policy and Procedures Are Needed To Provide Program Accountability

In order to provide accountability and address recurring weaknesses with implementing GSA's IT Security Program, we identified opportunities for additions and modifications to GSA’s IT Security Policy and procedures in five areas to assist system security officials in comprehensively addressing system risk, fulfilling their responsibilities, and maintaining effective internal controls. Additions and modifications to policies and procedures would assist the SAISO and Authorizing Officials in evaluating the effectiveness of ISSOs and ISSMs supporting GSA's systems.

Guidance as the Basis for Performance Goals and Measures

The GSA IT Security Policy directs system security officials to a variety of procedural guides, NIST publications, and best practices, but the Agency has not developed an ISSO procedural guide or an ISSM procedural guide for implementing role-specific security responsibilities. This lack of specific guidance contributes to weaknesses identified with the C&A process, background investigations, and contractor provided solutions, in instances where ISSOs and ISSMs did not consistently fulfill their roles as defined in GSA's IT Security Policy. Procedural guidance should delineate the specific processes for completing assigned ISSO and ISSM responsibilities, establish clear performance goals and measures, and provide a basis for evaluations. When contractors are providing ISSO and ISSM services, the GSA-OCIO should also require that contract and task order performance requirements are included, similar to the performance goals and measures to be used for GSA associates in these roles.

Persons with Security Responsibilities

Contracting Officers (COs) and Contracting Officer's Technical Representatives (COTRs) are not identified in Chapter 2 of the GSA IT Security Policy as individuals with security roles and responsibilities. The policy does state in Chapter 1 that *"GSA system program managers and contracting officers shall ensure that the appropriate security requirements of this order are put on contract for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the government."* NIST SP 800-35, *Guide To Information Technology Security Services,*[2] which provides guidance for contracting officials, includes COs and COTRs as persons with roles and responsibilities when contracting for security services. With current Personnel Security Requirements Division procedures, COTRs initiate contractor background investigations, and take action in the case of an unfavorable adjudication on contractors supporting GSA systems. Contractor services were employed for nine of the ten systems we reviewed this year and we identified multiple instances where COTRs had not requested all required background investigations. Adding COs and COTRs to the IT Security Policy, *Chapter 2 Roles and Responsibilities*, would clarify IT security responsibilities. In addition, the

[2] NIST SP 800-35 - *Guide To Information Technology Security Services*, October 2003.

Contractor Operations section of GSA's IT Security Policy should be clarified to require that task orders, as well as contracts, include appropriate security requirements.

Background Investigation Roles and Responsibilities

GSA's IT Security Policy is not consistent with other Agency directives for ensuring that background investigations are completed on persons supporting GSA systems. The policy directs that background investigations be conducted in accordance with Standard Operating Procedures for HSPD-12 and the GSA Suitability and Personnel Security Handbook.[3] However, the Agency IT Security Policy is not consistent with processes in place for contractor background investigations. GSA's IT Security Policy states that ISSOs are to assist the Authorizing Official and Data Owner in ensuring that required background investigations are completed. In contrast, the GSA Personnel Security Requirements Division staff, responsible for adjudicating background investigations, informed us that responsibility for requesting contractor background investigations is with the COTR, not the officials identified in the IT Security Policy. Clarification of the Agency IT Security Policy would facilitate improved implementation of contractor background investigations where COTRs are responsible for requests.

Information System Security Officer and Information System Security Manager Assignments

An additional factor contributing to security weaknesses was the assignment of an ISSO with a lack of IT knowledge and experience commensurate with duties of an ISSO. For a contractor provided E-Government call center system that processes, stores, and transmits private citizen's names, addresses, and credit card numbers, the ISSO did not ensure that contractor personnel were following GSA IT Security Policy and procedures. Specifically, the ISSO did not provide the contractor with the Agency's IT Security Policy and guidance, and when we inquired about IT security for the system, the ISSO directed us to contact the contractor's security manager. Under the current Agency IT Security Program, ISSOs and ISSMs are assigned without defined minimum qualifications or approval by the SAISO.

Segregation of Security Responsibilities

In some instances, security roles are not properly segregated, as required by OMB, and as intended by the IT Security Policy. Out of 79 GSA systems, six systems had one individual performing both the ISSO and ISSM roles. Of the six systems, two Regional general support systems had the same individual acting as ISSM, ISSO, and System Program/Project Manager. Security responsibilities are routinely "other duties as assigned," secondary to the individual's primary job responsibilities. For a system in our sample where security documentation was not comprehensive and the POA&M was missing identified security weaknesses, a contributing factor was a lack of segregation of ISSO, ISSM, and System Program/Project Manager responsibilities.

OMB Circular A-123[4] has specifically directed that within the Agency's structure, management should clearly: "*define areas of authority and responsibility; appropriately delegate the authority and responsibility throughout the agency; establish a suitable hierarchy for reporting; support appropriate human capital policies for hiring, training,*

[3] GSA Order ADM P 9732.1C, *Suitability and Personnel Security*, January 15, 1998.

[4] OMB Circular A-123, *Management's Responsibility for Internal Control*, December 21, 2004.

> *evaluating, counseling, advancing, compensating and disciplining personnel; and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization*." Control activities include policies, procedures and mechanisms in place to help ensure that agency objectives are met, such as proper segregation of duties. Internal control also needs to be in place over information systems, and due to the rapid changes in information technology, controls must also adjust to remain effective. As such, an individual should not be assigned to the roles of ISSO and ISSM for a single GSA system.

To strengthen and clarify GSA's IT Security Policy, the GSA-OCIO should develop procedural guidance necessary to set and monitor IT security performance goals and measures for system security officials. COs and COTRs should be added to the list of persons with IT security responsibilities, and roles and responsibilities for the background investigation process should be clarified. Further, the GSA-OCIO should collaborate with the GSA Personnel Security Requirements Division to identify and implement controls that effectively ensure all requisite contractor background investigations are initiated. The *Contractor Operations* section of GSA IT Security Policy should be clarified to require that task orders, as well as contracts, include appropriate security requirements. Additionally, the GSA-OCIO should require the SAISO to review and approve ISSO and ISSM assignments and require that one individual cannot act as both the ISSO and ISSM for a single system.

GSA Would Benefit From A More Proactive Approach for Addressing Emerging Risks

During this year's audit fieldwork, we identified emerging risks that have not yet been addressed in specific GSA IT security procedural and technical/hardening guides. A more proactive approach would benefit system owners in securing web applications and Voice over Internet Protocol (VoIP) implementations by addressing risks associated with these technologies. While the IT Security Subcommittee of the Information Technology Architecture Planning Committee (ITAPC) meets regularly, the subcommittee has not been proactive in addressing emerging risks such as those identified in this year's FISMA security reviews.

Web Application Security

The importance of web application security is increasing as applications move to this expanded form of connectivity. Over 70 percent of attacks against web sites or web applications come at the application layer, not the network or system layer. The Open Web Application Security Project (OWASP) reports that, *"Insecure software has its consequences, but insecure web applications, exposed to millions of users through the Internet are a growing concern."*[5] Attacks on web applications, both internal and external, bypass traditional network firewall and password access controls and may not be monitored. Attackers are increasingly targeting web applications, which have traditionally not been secured as well as network perimeters. Web based phishing attacks attempting to trick users into disclosing personal and proprietary information are also exploiting the inherent public trust in *.gov* web sites.

In May 2006, we issued an Alert Report to address two significant areas of risk with web applications that needed to be more comprehensively addressed in GSA's IT Security

[5] OWASP, *The Ten Most Critical Web Application Security Vulnerabilities*, 2004 Update.

Policy, C&A guidance, and monitoring practices. Vulnerabilities were found with web application security due to insufficient input validation and unsecured web servers running outdated and unsupported operating system software. Unmanaged vulnerabilities have the potential to harm the public's trust and increase resistance to sharing information with GSA and other government agencies. The Agency updated C&A procedural guidance to include testing for web application vulnerabilities, performed an assessment of 18 Internet-facing web applications, and trained ten GSA personnel on web application security. The GSA-OCIO also awarded a web application security scanning contract in July 2006 and implemented a requirement that all new GSA web applications must be tested for vulnerabilities before being published on the Internet.

Voice over Internet Protocol Security

VoIP, the transmission of voice over packet-switched IP networks, is one of the most important emerging trends in telecommunications. As with many new technologies, VoIP introduces both security risks and opportunities. VoIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues. Lower cost and greater flexibility are among the promises of VoIP for the enterprise, but VoIP should not be installed without careful consideration of the security problems introduced.[6]

In 2005 and 2006, we found Regional deployments of VoIP susceptible to multiple critical system and architectural vulnerabilities that would have benefited from guidance on implementing these VoIP deployments. The Agency IT Security Policy directs GSA employees and contractors to use NIST SP 800-58 as a guide, but does not provide vendor-specific implementation configuration settings and guidance necessary to properly secure these deployments. Additionally, several risks identified in NIST SP 800-58 were not addressed as part of the implementation process for either system.

GSA systems have shown improvements, as evidenced by a decrease in the number of critical vulnerabilities we identified from 140 in the ten systems sampled in 2005 to 19 in ten different systems sampled in 2006. However, the GSA-OCIO should develop technical/hardening guides for newly identified emerging risk areas to benefit system developers and system owners. Additionally, the ITAPC IT Security Subcommittee should regularly take actions to address risks with emerging technologies.

[6] National Institute of Standards and Technology. NIST Special Publication 800-58, *Security Considerations for Voice over IP Systems,* January 2005.

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. Implement improved accountability for associates and contractors supporting GSA's IT Security Program by taking actions to:
    a. Engage the Administrator’s support for developing standardized performance goals and measures for Information System Security Officers and Information System Security Managers across GSA Service, Staff, and Regional Offices, with periodic assessments of performance by the Senior Agency Information System Officer for use in performance evaluations.
    b. Require that contracts and task orders for Information System Security Officer and Information System Security Manager services, in support of GSA systems, include performance requirements similar to goals and measures being established for GSA associates in these roles.
    c. Collaborate with the GSA Personnel Security Requirements Division to identify and implement procedures and controls that effectively ensure prompt initiation of contractor background investigations for individuals accessing GSA systems and data.

2. Strengthen GSA's IT Security Policy and procedures in the following areas:
    a. Develop guidance and directives necessary to establish and monitor IT security performance goals and measures for Information System Security Officers and Information System Security Managers.
    b. Require Senior Agency Information Security Officer approval of Information System Security Officer and Information System Security Manager assignments.
    c. Add the roles of Contracting Officer and Contracting Officer’s Technical Representative as persons with IT security responsibilities, and clarify the responsibilities of systems security officials in the background investigation process.
    d. Segregate IT security roles and responsibilities by requiring that one individual cannot be both the Information System Security Officer and Information System Security Manager for a single system.
    e. Clarify the *Contractor Operations* section of the policy to require that task orders, as well as contracts, include appropriate security requirements.

3. Ensure that the Information Technology Architecture Planning Committee, IT Security Subcommittee regularly takes actions to address risks with emerging technologies.

4. Develop and implement technical/hardening guides for securing web applications and Voice over Internet Protocol.

MANAGEMENT COMMENTS

A copy of the GSA-CIO’s comments will be included in their entirety as Appendix D.

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 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

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

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

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

Agency Name:

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 over the past fiscal year 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.

		Question 1						**Question 2**					
		a. **Agency Systems**		**b.** **Contractor Systems**		**c.** **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		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	10	2			10	2	2	100.0%	2	100.0%	2	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**10**	**2**	**0**	**0**	**10**	**2**	**2**	**100.0%**	**2**	**100.0%**	**2**	**100.0%**
Federal Supply Service (FSS)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2		9	1	11	1	1	100.0%	1	100.0%	0	0.0%
	Low	1		3		4	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**3**	**0**	**12**	**1**	**15**	**1**	**1**	**100.0%**	**1**	**100.0%**	**0**	**0.0%**
Federal Technology Service (FTS)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2		6	1	8	1	1	100.0%	1	100.0%	1	100.0%
	Low	2		2		4	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**4**	**0**	**8**	**1**	**12**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
Office of the Chief Acquisition Officer (OCAO)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate			4		4	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low	1		3		4	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**7**	**0**	**8**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Office of Governmentwide Policy (OGP)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low	3		2		5	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**4**	**0**	**2**	**0**	**6**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Office of Chief Information Officer (CIO)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2	1			2	1	1	100.0%	1	100.0%	1	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**2**	**1**	**0**	**0**	**2**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
Office of Chief Finance Officer (CFO)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1		3	1	4	1	1	100.0%	1	100.0%	1	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**3**	**1**	**4**	**1**	**1**	**100.0%**	**1**	**100.0%**	**1**	**100.0%**
Office of Chief People Officer (CPO)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1		1		2	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**1**	**0**	**2**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Office of the Inspector General (OIG)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Office of General Counsel (OGC)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Board of Contract Appeals (BCA)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Office of Citizen Services and Communications (OCSC)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low			2	1	2	1	1	100.0%	1	100.0%	0	0.0%
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**0**	**0**	**2**	**1**	**2**	**1**	**1**	**100.0%**	**1**	**100.0%**	**0**	**0.0%**
Region 1	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!

	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 2	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 3	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 4	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2				2	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 5	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2	2			2	2	2	100.0%	2	100.0%	2	100.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**2**	**2**	**0**	**0**	**2**	**2**	**2**	**100.0%**	**2**	**100.0%**	**2**	**100.0%**
Region 6	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2	1			2	1	1	100.0%	1	100.0%	0	0.0%
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**2**	**1**	**0**	**0**	**2**	**1**	**1**	**100.0%**	**1**	**100.0%**	**0**	**0.0%**
Region 7	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 8	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	2				2	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**2**	**0**	**0**	**0**	**2**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 9	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Region 10	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
National Capitol Region (NCR)	High					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Moderate	1				1	0		#DIV/0!		#DIV/0!		#DIV/0!
	Low					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Not Categorized					0	0		#DIV/0!		#DIV/0!		#DIV/0!
	Sub-total	**1**	**0**	**0**	**0**	**1**	**0**	**0**	**#DIV/0!**	**0**	**#DIV/0!**	**0**	**#DIV/0!**
Agency Totals	**High**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Moderate	**35**	**6**	**23**	**3**	**58**	**9**	**9**	100.0%	**9**	100.0%	**7**	77.8%
	Low	**9**	**0**	**12**	**1**	**21**	**1**	**1**	100.0%	**1**	100.0%	**0**	0.0%
	Not Categorized	**0**	**0**	**0**	**0**	**0**	**0**	**0**	#DIV/0!	**0**	#DIV/0!	**0**	#DIV/0!
	Total	**44**	**6**	**35**	**4**	**79**	**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 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. 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	- Almost Always, for example, approximately 96-100% of the time
3.b.1.	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. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems:

		Missing Contractor Systems:
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).	- Frequently, for example, approximately 71-80% 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 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. The POA&M for one Regional general support system did not include multiple weaknesses identified during the C&A process. The POA&M for a component of a larger major application did not include weaknesses identified for the component during vulnerability scanning.

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. Response Categories: - Excellent - Good - Satisfactory - Poor - 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. One contractor system was not given GSA procedural guides when developing C&A documentation and therefore the C&A documentation did not conform to GSA requirements. Security documentation for one general support system was not updated to address the reviewed component.

Section B: Inspector General. Question 6, 7, 8, and 9. **Agency Name:** **Question 6**			
6.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.		
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?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Mostly, or on approximately 81-95% 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	- Mostly, or on approximately 81-95% of the systems running this software
HP-UX	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Linux	Yes	Yes	- Sometimes, or on approximately 51-70% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Rarely, or, on approximately 0-50% of the systems running this software
Other. Specify:			

Comments: We performed vulnerability scanning on ten select systems including four contractor systems and six components of larger systems to determine the degree of implementation of hardening guides. Audit determinations regarding the extent of hardening guide implementations are based on a sample of ten select systems and may differ from agency responses due to different sample sizes. One contractor system had a Linux device with critical-level vulnerabilities indicating that it had not been appropriately hardened. Review of Oracle database settings for two contractor systems showed numerous inconsistencies with the Agency's recommended settings, indicating that the Oracle devices had not been hardened in accordance with GSA's IT security policy.

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. Yes or No.	Yes

7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. 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 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? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - 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? Yes or No.	Yes

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA’S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

TEN SYSTEMS REVIEWED BY THE OFFICE OF INSPECTOR GENERAL IN 2006

System	Owner	Description
e-Buy (Component of the GSA Advantage! Major Application)	Federal Supply Service (FSS)	e-Buy is GSA's latest acquisition tool and is designed primarily for the acquisition of services and/or large purchases. e-Buy is a system that allows agency buyers to post Requests For Quotes for a specified period of time for a wide range of products and services offered from Multiple Award Schedule contract vendors. e-Buy is a component of a contractor supported system categorized as moderate risk.
USA Services/NCC (Major Application)	Office of Citizen Services and Communications (OCSC)	USA Services/National Contact Center (NCC) responds to public inquiries seeking information on a wide range of government programs. The Government contracted out the operations of the NCC in 1990. In FY2003, the NCC responded to over 1.5 million inquiries and took over 246,000 orders for consumer publications. USA Services/NCC is a contractor supported system categorized as low risk.
Data Gateway (Component of Realty Services Enclave Major Application)	Public Buildings Service (PBS)	Data Gateway establishes standard tools and allows for consistency and accuracy in data by enabling the electronic transfer of key business information among a number of disparate systems. Data Gateway is a component of an Agency system categorized as moderate risk.
FEDdesk (Component of PAR Major Application)	Office of Chief Financial Officer (CFO)	Under the FEDdesk suite of services, GSA offers Federal agencies fully automated and paperless transactions for time and attendance. FEDdesk is a component of a contractor supported system categorized as moderate risk.
Region 6 VoIP (Component of Region 6 PBS LAN General Support System)	Heartland Region (R6)	The Region 6 VoIP system resides on the Region 6 PBS LAN in Kansas City, MO and provides voice service and voice mail. Region 6 VoIP is a component of an Agency system categorized as moderate risk.
Region 5 PBS LAN (General Support System)	Great Lakes Region (R5)	The Region 5 PBS LAN system provides both onsite and remote network access to the users of the Great Lakes Region Organizational Unit of the GSA Active Domain that enables them to perform their business line missions and support their customers by accessing, viewing, creating and modifying Regional and National non-classified data through local and Nationally maintained applications. Region 5 PBS LAN is an Agency system categorized as moderate risk.
Region 5 FTS LAN (General Support System)	Great Lakes Region (R5)	The purpose of the Region 5 FTS LAN system is to provide both onsite and remote network access to the users of the Great Lakes Region Domain that enables them to perform their business line missions and support their customers by accessing, viewing, creating and modifying Regional and National non-classified data through local and Nationally maintained applications. Region 5 FTS LAN is an Agency system categorized as moderate risk.
RAS (Component of Enterprise Infrastructure Operations General Support System)	Office of the Chief Information Officer (CIO)	The RAS is GSA’s private remote access network infrastructure offering remote network connectivity to all GSA associates and partners nationwide. The RAS Infrastructure supports several remote access technologies including: 56kbps Dial-up, Integrated Services Digital Network (ISDN) at 128kbps, High Speed Access using Virtual Private Network (VPN), and GSA private Enterprise Digital Service Link (eDSL). RAS is a component of an Agency system categorized as moderate risk.

System	Owner	Description
NSOBS/TOPS (Major Application)	Federal Technology Service (FTS)	NSOBS/TOPS automates the local service and long distance business processes including ordering, billing and reconciliation of telecommunications services. The benefits of this project include minimization of paperwork, processing speed, and ensuring customer satisfaction. It supports all Government agency customers with telecommunications inventory management, on-line ordering, and on-line access to account information. NSOBS/TOPS is a contractor supported system categorized as moderate risk.
OA Tool (Component of Realty Services Enclave Major Application)	Public Buildings Services (PBS)	The Occupancy Agreement Tool (OA Tool) is used by Realty Specialists responsible for obtaining space for PBS customers. The OA Tool interacts with STAR to provide readiness, occupancy agreement, and billing information. OA Tool is a component of an Agency system categorized as moderate risk.

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

STATUS OF CONTRACTOR BACKGROUND INVESTIGATIONS FOR TEN SYSTEMS

System	Number Of Contractor Personnel	GSA Required NACIC Background Investigations Completed[7]	GSA Required NACIC Background Investigations Requested But Not Completed	GSA Required NACIC Background Investigations Not Requested
e-Buy[8]	94	12	82	0
USA Services/NCC	5	0	0	5
Data Gateway	5	1	2	2
FEDdesk	7	6	1	0
Region 6 VoIP[9]	0	0	0	0
Region 5 PBS LAN	22	7	15	0
Region 5 FTS LAN	4	0	3	1
RAS	10	4	6	0
NSOBS/TOPS	7	7	0	0
OA Tool	23	9	6	8

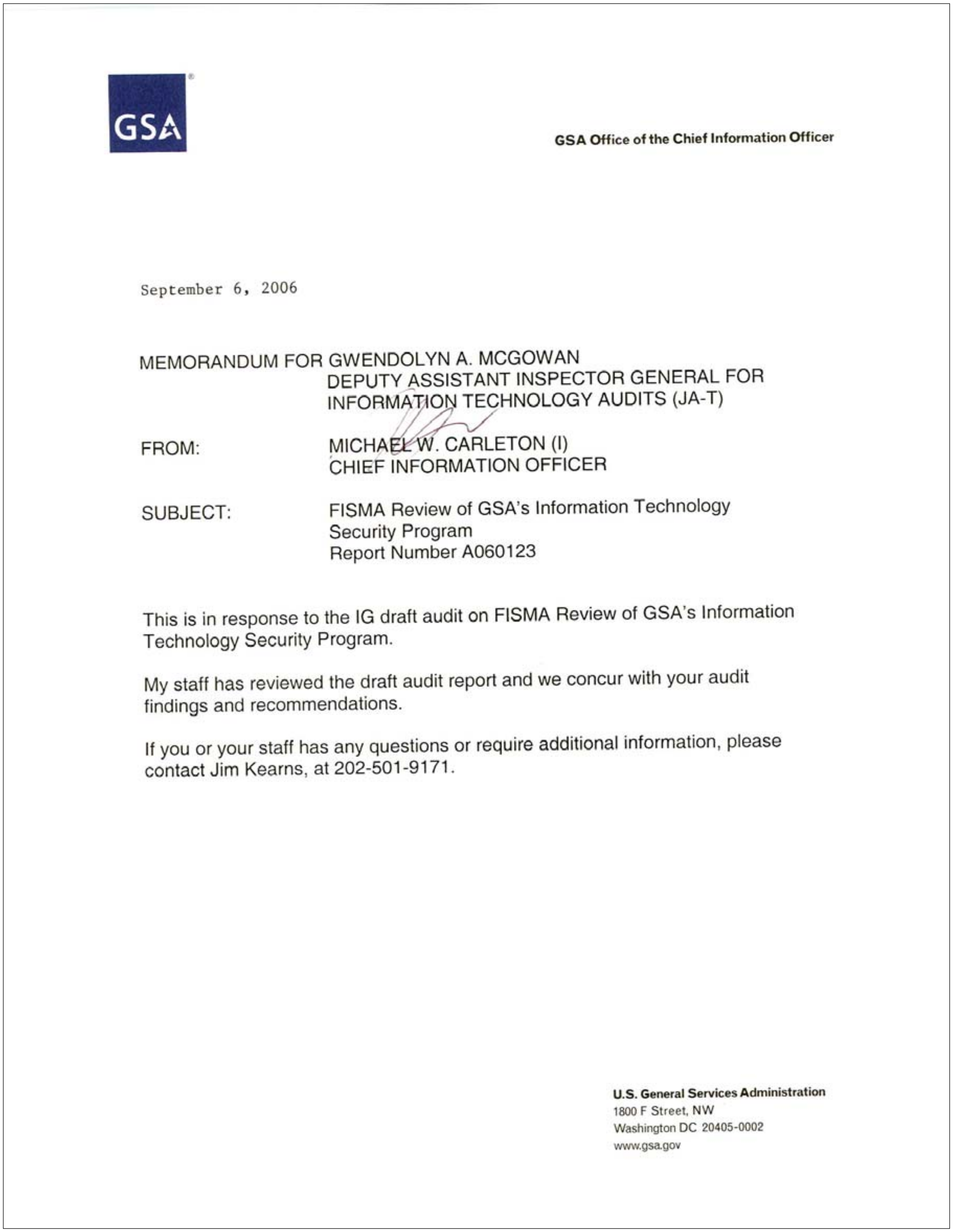
[7] Column includes completed NACIC (National Agency Check with Inquiries Credit), DOD Top Secret Clearance, MBI, and LBI investigations.

[8] The ISSO for e-Buy did not identify contractor support personnel for one company supporting the system, and did not confirm whether NACIC background investigations had been requested.

[9] Region 6 VoIP was the only system in our sample not supported by contractor personnel.

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

GSA-CIO'S RESPONSE TO DRAFT AUDIT REPORT



GSA

GSA Office of the Chief Information Officer

September 6, 2006

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

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

SUBJECT: FISMA Review of GSA's Information Technology
Security Program
Report Number A060123

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 Jim Kearns, at 202-501-9171.

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

FY 2006 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A060123/O/T/F06018

REPORT DISTRIBUTION

	Copies
Office of the Chief Information Officer (I)	3
Office of the Chief Financial Officer (B)	2

	Electronic Copies
Office of the CFO Chief Information Officer (BD)	1
Office of the FAS Chief Information Officer (TH)	1
Office of the PBS Chief Information Officer (PGA)	1
Office of the CSC Chief Information Officer (XCI)	1
Great Lakes Region 5 (5A)	1
Heartland Region 6 (6A)	1
Audit Follow-up and Evaluation Branch (BECA)	1
Assistant Inspector General for Auditing (JA)	2
Audit Operations Staff (JAO)	1
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
Regional Inspector General for Auditing (JA-5 and JA-6)	2
Administration and Data Systems Staff (JAS)	1
Assistant Inspector General for Investigations (JI)	1
Regional Inspector General for Investigations (JI-5 and JI-6)	2