Audit Report

FY 2009 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

September 30, 2009

Office of Inspector General
General Services Administration

Office of Audits

FY 2009 OFFICE OF INSPECTOR GENERAL FISMA REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM REPORT NUMBER A090126/O/T/F09011

September 30, 2009

U.S. GENERAL SERVICES ADMINISTRATION
Office of Inspector General

Date: September 30, 2009

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

To: Casey Coleman
Chief Information Officer (I)

Subject: FY 2009 Office of Inspector General FISMA Review of GSA's Information Technology Security Program
Report Number A090126/O/T/F09011

The Federal Information Security Management Act of 2002 (FISMA) requires Inspectors General to perform an independent evaluation to determine the effectiveness of their respective agency's information security program, including testing a subset of the agency's information systems. This audit report presents the results of the Inspector General's Fiscal Year (FY) 2009 independent evaluation of the General Services Administration's (GSA's) agency-wide Information Technology (IT) Security Program, as required by FISMA, and reflects results from our system security audits conducted during the year. While important steps have been taken to develop, document, and implement an agency-wide IT security program in GSA, we found the need to improve risk management practices to better protect GSA systems and sensitive information in four main areas: (1) certification and accreditation (C&A) of system controls, (2) internal application security, (3) security of social media technologies, and (4) oversight of systems provided by contractors.

Risk management practices for GSA systems can be improved by strengthening the Agency's C&A process to ensure that sufficient information is provided to support testing results on the status of management, operational, and technical system controls. This could provide GSA management and the Agency's customer base with additional information needed to support risk-based decision making. While GSA has taken several steps to prevent and detect malicious external activity, a more proactive approach is needed to strengthen security controls for several internal agency applications that process, store, and/or transmit sensitive information across Agency Services/Staff Offices/Regions. GSA is also implementing important social media technologies to facilitate collaboration and sharing of information within the Agency and with the public. We found the need to enhance oversight of these technologies to ensure that GSA security requirements are met. Finally, increased security and privacy program oversight of contractor supported systems could provide additional assurance to GSA and customer agencies that required security controls have been implemented and sensitive information protected.

Under the Recovery Act, GSA has been given approximately $5.8 billion for construction and renovation of Federal buildings and improving the fuel efficiency of government vehicles. GSA will rely on its information systems to track, report, and manage Recovery Act funds. Working with system security officials across GSA to address the risk areas highlighted in this report can better enable GSA to meet its security objectives and the requirements of the Recovery Act with speed and transparency.

I wish to express my appreciation to you, your staff, and individuals with system security responsibilities for their assistance with this audit. If you have any questions regarding our review of GSA's IT Security Program, please contact me or Gwendolyn McGowan, Deputy Assistant Inspector General for Information Technology Audits, on 703-308-1223.

Khalid Hasan
Audit Manager
Information Technology Audit Office (JA-T)

FY 2009 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

TABLE OF CONTENTS

Appendices

FY 2009 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

EXECUTIVE SUMMARY

Purpose

The Federal Information Security Management Act of 2002 (FISMA)[1] provides: (1) a framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets; (2) for the development and maintenance of minimum controls required to protect Federal information and information systems; and (3) a mechanism for improved oversight of Federal agency information security programs. Inspectors General (IGs) are required by FISMA to perform an annual independent evaluation to determine the effectiveness of their respective agency's information security program, including testing a subset of the agency's information systems. The objective of this audit was to determine if the General Services Administration (GSA) had developed, documented, and implemented an agency-wide information security program to provide information security for the data and systems that support the operations and assets of the Agency. If not, what additional actions are needed to strengthen information security risk management practices for GSA? Appendix A contains our objective, scope, and methodology for the audit.

Background

Information security is a critical consideration for GSA as it carries out its mission and responds to the requirements of the American Recovery and Reinvestment Act of 2009 (Recovery Act).[2] Information security is also important as GSA works to implement transparency and open government initiatives to make Agency operations more transparent, participatory, and collaborative. To meet its mission, GSA relies on a portfolio of 94 information systems with a total enacted budget in FY 2009 of approximately $540 million.[3] GSA has established an agency-wide IT security program, which is managed by the Office of the Chief Information Officer, to provide for the confidentiality, integrity, and availability of Agency information systems.

An agency-wide IT security program provides a management framework for ensuring that risks are understood and that effective controls are selected and properly implemented for Agency information systems. FISMA is the primary legislation governing Federal information security programs, and it builds upon earlier legislation through added emphasis on the management of information security. FISMA directs agencies to develop, document, and implement an agency-wide information security program to provide information security for the operations and assets of the agency. Table I below provides the components that must be included in agency information security programs, as required by FISMA. FISMA also directs IGs to perform an annual independent evaluation to determine the effectiveness of information security programs and

[1] Title III of the Electronic Government Act of 2002 (Public Law 107-347).
[2] American Recovery and Reinvestment Act of 2009, Public Law 111-5, February 17, 2009.
[3] As reported on the IT Dashboard.

practices of their respective agency. These evaluations are to include: (1) testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems; and (2) an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.

Table I: FISMA Information Security Program Areas

Program Area	FISMA Requirement
Risk Assessment	Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.
Policies and Procedures	Policies and procedures that (1) are based on risk assessments; (2) cost-effectively reduce information security risks to an acceptable level; and (3) ensure that information security is addressed throughout the life cycle of each agency information system.
Planning	Subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate.
Security Awareness Training	Security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of: (1) information security risks associated with their activities; and (2) their responsibilities in complying with agency policies and procedures designed to reduce these risks.
Periodic Testing and Evaluation	Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually.
Remediation Process	A process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
Incident Management	Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines.
Continuity of Operations	Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

This audit report presents the results of the GSA Inspector General's FY 2009 independent evaluation of GSA's IT Security Program, as required by FISMA, and reflects results from system security audits conducted during the year. Appendix B provides a description of the select GSA systems considered in our annual FISMA review.

Results in Brief

GSA has taken steps to develop, document, and implement an agency-wide information technology (IT) security program and also provide information security for the operations and assets managed by the Agency. The GSA Chief Information Officer recently revised agency-wide IT security policy and has published several new guides to support risk management activities for IT systems and to address prior years' audit findings. We also noted improvements in the implementation of GSA's IT Security Program for select agency systems. However, we found areas where additional improvements are needed in GSA's IT Security Program and instances

where system security officials' practices did not mitigate risks and protect sensitive Agency data and systems, as required. IT security findings for our annual FISMA review fall into four main areas: (1) certification and accreditation of system controls, (2) internal application security, (3) security of social media technologies (e.g., blogs, wikis), and (4) oversight of systems provided by contractors. Further, Appendix C summarizes security control areas where we found improvements were needed to better manage risks for specific GSA systems, including for access control, audit logging and monitoring, and secure configuration of system devices.

Improvements in these areas could provide management with additional information to make risk-based decisions on the security of GSA's IT systems, including those provided by contractors. Further, focusing IT security program efforts to address risks in these key areas could result in better protection of sensitive Agency information and transactions, including personally identifiable and Federal buildings information. Under the Recovery Act, GSA has been given approximately $5.8 billion for construction and renovation of Federal buildings and improving the fuel efficiency of government vehicles. This money must be spent with increased speed and transparency, and GSA will rely on its information systems to track, report, and manage Recovery Act funds and information. Working with system security officials across GSA to address the risk areas highlighted in this report can better enable GSA to meet its security objectives and the requirements of the Recovery Act with speed and transparency.

Recommendations

To improve GSA's IT Security Program and better ensure the security of Agency systems, data, and operations, we recommend that the GSA Chief Information Officer take actions to:

1. Strengthen system certification and accreditation (C&A) processes by:

    a. Developing language to be included in C&A contracts for the provision of adequate details on methods used to conclude on the effectiveness of system security controls and updating Agency security guidance accordingly.
    b. Enhancing oversight processes to ensure that detailed information on testing procedures and methodologies is provided in system C&A packages.
    c. Collaborating with system security officials to ensure that system boundaries and controls for minor applications are adequately considered with C&A activities.

2. Enhance the security of internal applications by working with GSA Services/Staff Offices/Regions to:

    a. Develop and maintain an inventory of internal applications, including the data maintained and functions performed by these applications.
    b. Ensure that these applications, including those we have identified in Appendix D, meet GSA security requirements.
    c. Strengthen change management procedures to better ensure that applications are put in operation with appropriate security controls.

3. Improve security of GSA's social media technologies, such as blogs and wikis, by:

    a. Reviewing all Agency-operated social media sites to ensure that appropriate access controls are established for creation and maintenance of such sites.
    b. Incorporating the Agency's social media policy into security awareness training and rules of behavior.
    c. Ensuring that periodic security reviews of social media sites are performed.

4. Work with the Chief Human Capital Officer, Chief Acquisition Officer, and other Agency officials, as appropriate, to enhance the security of systems supported by contractors by:

    a. Developing an inventory of contractors supporting GSA IT systems that have significant privacy information responsibilities.
    b. Ensuring that appropriate security awareness and privacy training is provided to contractors supporting GSA systems, including role-based training for contractors with significant privacy information responsibilities.
    c. Prioritizing ongoing efforts to analyze and mitigate the use of non-government domains for GSA systems by focusing on systems provided by contractors as managed service offerings.
    d. Ensuring that appropriate privacy clauses are included in contracts, statements of work, and task orders for Privacy Act systems.

Management Comments

The GSA Chief Information Officer concurred with the audit findings and recommendations outlined in this report. A copy of the Chief Information Officer's comments is included in its entirety in Appendix E.

FY 2009 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

INTRODUCTION

Information security threats to Federal agencies, including the General Services Administration (GSA), are growing and evolving. For example, the number of security related incidents reported by Federal agencies to the United States Computer Emergency Readiness Team (US-CERT) has increased significantly over the last three years. Information security is a critical consideration for GSA as it carries out its mission, responds to the requirements of the American Recovery and Reinvestment Act of 2009 (Recovery Act), and works to implement transparency and open government initiatives to make Agency operations more transparent, participatory, and collaborative. To meet its mission, GSA relies on a portfolio of 94 information systems with a total enacted budget in Fiscal Year (FY) 2009 of approximately $540 million.[4] GSA has established an agency-wide Information Technology (IT) security program, which is managed by the Office of the Chief Information Officer (OCIO), to provide for the confidentiality, integrity, and availability of Agency information systems.

An agency-wide IT security program provides a management framework for ensuring that risks are understood and that effective controls are selected and properly implemented for Agency information systems. The Federal Information Security Management Act of 2002 (FISMA) is the primary legislation governing Federal information security programs, and it builds upon earlier legislation through added emphasis on the management of information security. FISMA directs agencies to develop, document, and implement an agency-wide information security program to provide information security for the operations and assets of the agency. FISMA also directs Inspectors General (IGs) to perform an annual independent evaluation to determine the effectiveness of information security programs and practices of their respective agency. These evaluations are to include: (1) testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems; and (2) an assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines.

This audit report presents the results of the GSA Office of Inspector General's (OIG) FY 2009 annual review of GSA's IT Security Program, and reflects results from system security audits conducted during the year in response to FISMA requirements. Appendix B provides a description of the select systems considered in our independent evaluation and Appendix C summarizes key security control areas where we found that additional steps need to be taken to better manage risks for these specific GSA systems.

[4] As reported on the IT Dashboard.

RESULTS OF AUDIT

GSA has taken steps to develop, document, and implement an agency-wide IT security program and also provide information security for the operations and assets managed by the Agency. The GSA Chief Information Officer (GSA-CIO) recently revised agency-wide IT security policy and has published several new guides to support risk management activities for IT systems and to address prior years' audit findings. We also noted improvements in the implementation of GSA's IT Security Program for select agency systems. However, we found areas where additional improvements are needed in GSA's IT Security Program and instances where system security officials' practices did not mitigate risks and protect sensitive Agency data and systems, as required. IT security findings for our annual FISMA review fall into four main areas: (1) certification and accreditation of system controls, (2) internal application security, (3) security of social media technologies (e.g., blogs, wikis), and (4) oversight of systems provided by contractors. Further, Appendix C summarizes key control areas where we found improvements were needed to better manage risks for specific GSA systems, including for access control, audit logging and monitoring, and secure configuration of system devices.

While GSA has established a certification and accreditation (C&A) process that is based on Federal policy and guidance, implementation of this process by system owners has not ensured that risks are managed or key information provided to support risk-based decisions. Specifically, we identified applications processing sensitive information that were not covered under existing C&A's, and detailed information on the assessment procedures and methodologies employed to determine the adequacy of controls in place were not available for select systems. This resulted in security vulnerabilities that were not being addressed and impacted the ability of management and GSA's customer base to rely on approved controls to make informed decisions about system security. Our audit work also identified several internal GSA applications with security control weaknesses, including with access controls, which provided anyone in the Agency the ability to view sensitive transactions and information, including personally identifiable and secure buildings information. GSA is also implementing emerging social media technologies, such as blogs, to facilitate collaboration and sharing of information within the Agency and with the public. We found a need to enhance oversight of these technologies to ensure that they meet GSA security requirements and that appropriate access controls are implemented for creating and posting Agency information. Finally, increased security and privacy program oversight of contractor supported systems could provide additional assurance to GSA and customer agencies that required security controls have been implemented and sensitive information is protected.

Under the Recovery Act, GSA has been given approximately $5.8 billion for construction and renovation of Federal buildings and courthouses and improving the fuel efficiency of government vehicles. This money must be spent with increased speed and transparency, and GSA will rely on its information systems to track, report, and manage Recovery Act funds and information. Working with system security officials across GSA to address the risk areas highlighted in this report can better enable GSA to meet its security objectives and the requirements of the Recovery Act with speed and transparency.

Improvements to Agency-wide Certification and Accreditation Processes Would Better Assist Management and Provide Additional Information for Making Risk-based Decisions

While GSA has established an agency-wide certification and accreditation (C&A) process based on Federal policy and guidance, and all five of the select systems we reviewed had been certified and accredited, improvements in implementation of this process are needed in two main areas to ensure that sensitive information and risks are being managed. First, as reported by the OIG last year,[5] system C&As are not consistently ensuring that risks with minor applications[6] in GSA are being mitigated as needed. Specifically, we found that several internal Agency applications that stored or transmitted sensitive information were not covered by existing system security plans. Further, for two of the five systems we reviewed, including the only "high" risk system in GSA, details on the methods and procedures utilized to conclude on the effectiveness of security controls in place were not identified or documented as part of C&A activities. While improvements have been made with implementation of GSA's C&A process, taking steps to address these areas could provide vital information, support risk-based decisions, and protect sensitive information and electronic transactions.

Through a search of GSA's Intranet site, we identified several internal applications storing sensitive information that had not been included in existing system security plans. These applications were operating with security control weaknesses that permitted anyone with access to GSA's Intranet, including contractors, to view sensitive information. This access spanned Personally Identifiable Information (PII), Sensitive but Unclassified (SBU) buildings information, and financial information (refer to the next section and Appendix D for additional information). Primary causes for these weaknesses were that GSA does not have a comprehensive inventory of its internal applications and system security officials were unaware that these applications had been developed and implemented. GSA's IT Security Policy requires all information systems, including minor applications, to be covered by a system security plan. Further, FISMA requires agency information security programs to include subordinate plans for providing adequate information security for networks, facilities, and systems, or groups of systems, as appropriate.

For two of five systems we reviewed, including GSA's only "high" risk system, assurances were not provided in the C&A package regarding the methodologies and procedures utilized to conclude on the effectiveness of system controls. A primary cause for this was that contract documents for C&A services did not require this information. A lack of such information limits the ability of GSA management and the Agency's customer base to rely on the C&A to make risk-based decisions. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37[7] notes that agency officials should have the most complete, accurate, and

[5] FY 2008 Office of Inspector General FISMA Review of GSA's Information Technology Security Program, Report Number A080081/O/T/F08016, September 11, 2008.

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

[7] NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.

trustworthy information possible on the security status of their information systems in order to make timely, credible risk-based decisions.

Security certification and accreditation encompass activities that are an integral part of GSA's IT risk management process. Improving results for GSA's C&A process can provide additional security for sensitive Agency information and systems. Specifically, we recommend that the GSA-CIO take actions to strengthen C&As for GSA systems by: (1) developing language to be included in C&A contracts for the provision of adequate details on methods used to conclude on the effectiveness of system security controls and updating Agency security guidance accordingly; (2) enhancing oversight processes to ensure that detailed information on testing procedures and methodologies is provided in system C&A packages; and (3) collaborating with system security officials to ensure that system boundaries and controls for minor applications are adequately considered with C&A activities.

Security Controls for Internal GSA Applications Should Be Strengthened to Reduce Risks with Sensitive Agency Information and Transactions

GSA's Services/Staff Offices/Regions (S/SO/Rs) rely on internal applications to support Agency operations, and we found weaknesses in security controls for several of these applications. We found applications that were available to anyone with access to GSA's Intranet site, which potentially includes several thousand employees and contractors. Further, these applications were not always encrypting sensitive information that was being transmitted and stored inside of GSA. Appendix D provides a summary of the internal applications we identified where appropriate security controls were not in place and information that was placed at risk due to control weaknesses.

Specifically, we found an internal Regional application providing access to shared SBU drawings and other sensitive files for Federal buildings to anyone with access to GSA's Intranet. For this same Region, another application used to input data to GSA's financial management system of record lacked appropriate access controls, enabling access to PII and the ability to submit transactions. System officials informed us that compensating controls were in place to address these weaknesses. However, system controls to detect potential fictitious transactions submitted through this application were not documented or available for testing. In addition, we identified several other internal applications supporting GSA Services and Staff Offices that were not securely configured. For example, an application being used by the Federal Acquisition Service (FAS) for management and tracking of system problem tickets, such as for user requests for password resets or for problems with usability, permitted unauthorized access to anyone in GSA.

Along with weaknesses in access controls for internal applications, we identified sensitive information including PII, financial information, and SBU buildings information that was available to those without a need to know. We found sensitive usernames and passwords and program code for specific GSA systems that was not adequately protected. If this information were to be obtained by a malicious user, it could lead to identity theft, financial fraud, or harm to GSA's reputation. Further, while GSA has several protections in place to prevent a malicious individual from gaining access to the Agency's internal network, if an outsider was able to circumvent these protections, this information is not stored or restricted properly to prevent

unauthorized access that could disrupt GSA operations. Appropriate encryption and access controls would limit the ability of malicious internal or external users to gain access to this information.

There are three primary causes for these application security control weaknesses. First, system security officials were not always aware that these applications were developed and put into operation on GSA's internal network. Second, a comprehensive inventory of internal applications, including the data maintained and functions performed by these applications, has not been developed. Third, C&A's, particularly for general support systems, have not ensured that risks with these types of applications are effectively managed. While GSA's IT Security Policy requires that system access be granted on a need to know basis and that all information systems incorporate proper user identification and authentication methodologies, these applications fell through the cracks. Further, data owners are required by the policy to ensure that system access is restricted to authorized users in order to enforce job function alignment, segregation of duties, and need to know. In addition, web application security guidance provided by the GSA-CIO notes that sensitive information should be encrypted and applications should use secure transmission protocols.

With implementation of the Recovery Act, GSA has been provided approximately $5.8 billion to construct and renovate Federal buildings, as well as improve the fuel efficiency of the Federal fleet. Undertaking Recovery Act projects will require GSA to utilize internal applications to track and manage funds and other information. As such, ensuring that appropriate controls are implemented to enforce segregation of duties and need to know for access to agency applications is critical to prevent fraud, waste, and abuse. We recommend that to enhance the security of internal applications, the GSA-CIO work closely with Agency S/SO/Rs to: (1) develop and maintain an inventory of internal applications, including the data maintained and functions performed by these applications; (2) ensure that these applications, including those we have identified in Appendix D, meet GSA security requirements; and (3) strengthen change management procedures to better ensure that applications are put in operation with appropriate security controls.

Enhancing Oversight of Emerging Social Media Technologies Could Facilitate Secure Collaboration and Information Sharing Within GSA and With the Public

To meet goals for government that is more citizen-centered, transparent, participatory, and collaborative and to facilitate collaboration and information sharing internally and with the public, GSA has been implementing important social media technologies. Increased oversight and monitoring of these technologies is needed to ensure that only authorized individuals are able to create social media web sites in GSA and that sensitive Agency information is protected. While GSA has established a process to request, review, and approve the creation of internal and public facing social media related sites, we found that anyone in GSA with a Lotus Notes e-mail account, including contractors, was able to bypass this process and create sites on the internal GSA network. We also identified internal social media sites that lacked appropriate access

controls, and a public facing wiki owned by GSA that had been the target of spam postings.[8] Promptly after we informed system security officials of these vulnerabilities, steps were taken to fix the security weaknesses. While GSA recently developed detailed policy for the use of social media technologies,[9] these weaknesses demonstrate a need to take a more proactive approach to ensure that this technology promotes secure collaboration and sharing of information within GSA and with the public.

Social media encompasses various activities that integrate technology, social interaction, and content creation. Examples of social media technologies include blogs, wikis, and social networking sites. Table II below provides a description of these technologies. GSA encourages the use of social media technologies to enhance communication, collaboration, and information exchange in support of GSA's mission and the Agency has developed a number of internal and external blogs. For example, the Chief Financial Officer has developed an internal blog to provide a forum for expanding communications on performance management, planning, budgeting, and financial management.

Table II. Select Social Media Technologies[10]

Social Media Technology	Description
Blog	A web based forum with regular entries of commentary, descriptions of events, or other materials where the blog host posts material on the website and others may provide comments.
Wiki	A collection of web pages that encourages users to contribute or modify content.
Social networking services	Tools used to connect people who share the same interests or activities.
Podcast	A way of publishing audio files on the web so they can be downloaded to portable listening devices.

There were three primary causes for security weakness with GSA's use of social media technology. First, C&A for the component of GSA's Lotus Notes infrastructure that provides the capability to create and manage social media related sites is still in the process of being completed. As such, security controls assessment for these sites had not yet been completed. Secondly, at the time of our testing, GSA had not finalized detailed policy and procedures for the creation, use, and maintenance of social media sites. As previously noted, GSA has since distributed policies and procedures for the use of social media technologies. A general condition that contributed to these weaknesses was that agency officials were not performing comprehensive oversight of internally generated social media sites.

[8] Spam postings are unsolicited bulk messages that often contain malware. Malware refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.
[9] GSA Order CIO 2106.1, *GSA Social Media Policy,* July 17, 2009; GSA Order CIO P 2106.2, *GSA Social Media Handbook,* July 17, 2009.
[10] GSA Order CIO P 2106.2, *GSA Social Media Handbook,* July 17, 2009.

As a result of the weaknesses that we identified with GSA's use of social media technologies, there was increased risk that users could create sites for malicious purposes. Further, weak access controls for internal blogs can lead to users posting misleading information and impersonating authorized GSA officials. This could harm GSA's reputation and provide an avenue for phishing[11] attacks. GSA's IT Security Policy requires all information systems to be certified and accredited and have access controls implemented to authorize or restrict the activities of users and system personnel to authorized transactions and functions. In addition, GSA's Social Media Handbook notes that requests to create blogs must be approved by the Regional Administrator or Head of a Service or Staff Office.

Social media technologies are important tools to enhance communication, collaboration, and information exchange in support of GSA's mission. These technologies are also important to make Agency operations more transparent, participatory, and collaborative. To facilitate secure collaboration and information sharing within GSA and with the public, we recommend that the GSA-CIO take actions to: (1) review all Agency-operated social media sites to ensure that appropriate access controls are established for creation and maintenance of such sites; (2) incorporate the Agency's social media policy into security awareness training and rules of behavior; and (3) ensure that periodic security reviews of social media sites are performed.

Strengthening Oversight Processes is Needed to Ensure the Security of Contractor Supported Systems

While GSA's IT Security Program has established processes to provide oversight of systems supported by contractors, improvements are needed to ensure that sensitive Agency and customer information is protected. For two of the five systems we reviewed, we found that system security officials had not ensured that all contractors supporting GSA systems had been provided with security awareness and privacy training. We also found that required privacy clauses were not included in contract documents for Privacy Act systems and that management attention was needed to prioritize ongoing efforts to analyze and mitigate the use of non-government domains for GSA systems provided by contractors. GSA, like other Federal agencies, relies on contractors for systems development, maintenance, and operation for select systems managed by the Agency. Over half of the systems listed on GSA's FISMA inventory are classified as "contractor" systems, including those offered as managed services that support other Federal agencies. Ensuring that these systems meet GSA security requirements is important to achieving GSA's mission and for protecting sensitive Agency and customer information.

GSA provides security awareness and privacy training through GSA Online University to Agency associates and contractors that have Lotus Notes GSA e-mail addresses. However, not all contractors directly supporting Agency systems have these e-mail addresses. While contractors are oftentimes provided with security awareness and privacy training from their employer, system officials have not ensured that this training meets GSA requirements. Further, GSA does not yet have a complete inventory of contractors with significant privacy information

[11] Phishing refers to tricking individuals into disclosing sensitive personal information through deceptive computer-based means. To perform a phishing attack, an attacker creates a web site or e-mail that looks as if it is from a well-known organization.

responsibilities, which makes it difficult to identify those individuals who should take requisite training. In addition, for two Privacy Act systems we reviewed, security officials did not perform adequate oversight to ensure that appropriate privacy clauses were included in associated contracts. As a result, GSA may be unable to hold contractors accountable for any deviations from security or privacy policies. Further, contractors may be unaware of their responsibilities to secure GSA systems and data. GSA's IT Security Policy requires all GSA employees and contractors to complete annual security awareness and privacy training and that all Agency contracts involving Privacy Act information include appropriate privacy clauses.

For two of the five systems we reviewed that were provided by contractors as managed service offerings to GSA and several other Federal organizations, we found that these systems were not hosted on official government approved domains. Specifically these two systems were hosted on commercial domains (.com) versus official government domains (e.g., .gov, Fed.us, or .mil). A primary cause for this is that GSA has not yet made a determination if Agency systems that are hosted on commercial domains should be migrated to approved government domains. As a result, there is a greater risk that users of these systems would be susceptible to phishing attacks, and GSA may not be able to take advantage of security improvements with the Federal government's Domain Name System Security (DNSSEC) initiative.[12] OMB Memorandum M-05-04[13] states that agencies must use only .gov, .mil, or Fed.us domains unless the agency head explicitly determines another domain is necessary for the proper performance of an agency function.

With the many systems in GSA that are supported by contractors for the Agency, it is important for GSA's IT Security Program to ensure that oversight mechanisms are strengthened to ensure that these systems meet security requirements. This is of increased importance as contractor supported systems in GSA are provided to several other Federal organizations. To strengthen oversight of contractor supported systems, we recommend that the GSA-CIO work with the Chief Human Capital Officer, Chief Acquisition Officer and other Agency officials, as appropriate, to: (1) develop an inventory of contractors supporting GSA IT systems that have significant privacy information responsibilities; (2) ensure that appropriate security awareness and privacy training is provided to contractors supporting GSA systems, including role-based training for contractors with significant privacy information responsibilities; (3) prioritize ongoing efforts to analyze and mitigate the use of non-government domains for GSA systems by focusing on systems provided by contractors as managed service offerings; and (4) ensure that appropriate privacy clauses are included in contracts, statements of work, and task orders for Privacy Act systems.

[12] For more information, see OMB Memorandum M-08-23, *Securing the Federal Government's Domain Name System Infrastructure*, August 22, 2008.
[13] OMB Memorandum M-05-04, *Policies for Federal Agency Websites*, December 17, 2004.

CONCLUSIONS

Information security is a critical consideration for GSA as it carries out its mission and responds to the requirements of the Recovery Act. Information security is also important as GSA works to implement transparency and open government initiatives to make Agency operations more transparent, participatory, and collaborative. GSA has taken steps to develop, document, and implement an agency-wide IT security program and provide information security for the operations and assets of the Agency. Further, we noted improvements in system officials implementation of GSA's IT Security Program. However, additional improvements are needed with GSA's IT Security Program and systems officials' implementation practices to protect sensitive Agency and customer information and manage risks in four main areas: (1) certification and accreditation of system controls, (2) internal application security (3) security of social media technologies (e.g., blogs, wikis), and (4) oversight of systems provided by contractors. Addressing these four areas could better enable GSA to meet its security objectives and the requirements of the Recovery Act with speed and transparency.

RECOMMENDATIONS

To improve GSA's IT Security Program and better ensure the security of Agency systems, data, and operations, we recommend that the GSA Chief Information Officer take actions to:

1. Strengthen system certification and accreditation (C&A) processes by:

    a. Developing language to be included in C&A contracts for the provision of adequate details on methods used to conclude on the effectiveness of system security controls and updating Agency security guidance accordingly.
    b. Enhancing oversight processes to ensure that detailed information on testing procedures and methodologies is provided in system C&A packages.
    c. Collaborating with system security officials to ensure that system boundaries and controls for minor applications are adequately considered with C&A activities.

2. Enhance the security of internal applications by working with GSA Services/Staff Offices/Regions to:

    a. Develop and maintain an inventory of internal applications, including the data maintained and functions performed by these applications.
    b. Ensure that these applications, including those we have identified in Appendix D, meet GSA security requirements.
    c. Strengthen change management procedures to better ensure that applications are put in operation with appropriate security controls.

3. Improve security of GSA's social media technologies, such as blogs and wikis, by:

    a. Reviewing all Agency-operated social media sites to ensure that appropriate access controls are established for creation and maintenance of such sites.
    b. Incorporating the Agency's social media policy into security awareness training and rules of behavior.
    c. Ensuring that periodic security reviews of social media sites are performed.

4. Work with the Chief Human Capital Officer, Chief Acquisition Officer, and other Agency officials, as appropriate, to enhance the security of systems supported by contractors by:

    a. Developing an inventory of contractors supporting GSA IT systems that have significant privacy information responsibilities.
    b. Ensuring that appropriate security awareness and privacy training is provided to contractors supporting GSA systems, including role-based training for contractors with significant privacy information responsibilities.
    c. Prioritizing ongoing efforts to analyze and mitigate the use of non-government domains for GSA systems by focusing on systems provided by contractors as managed service offerings.
    d. Ensuring that appropriate privacy clauses are included in contracts, statements of work, and task orders for Privacy Act systems.

MANAGEMENT COMMENTS

The GSA-Chief Information Officer concurred with the audit findings and recommendations outlined in this report. A copy of the Chief Information Officer's comments is included in its entirety in Appendix E.

INTERNAL CONTROLS

As discussed in the Objective, Scope, and Methodology section of our report (see Appendix A), the objective of our audit was to determine if the General Services Administration (GSA) has developed, documented, and implemented an agency-wide information security program to provide information security for the data and systems that support the operations and assets of the Agency. If not, what additional actions are needed to strengthen information security risk management practices for GSA? While this audit included a review of elements of GSA's IT Security program including select management, operational, and technical controls for five GSA systems, we did not test all controls across the Agency. The Results of Audit and Recommendations sections of this report state, in detail, the need to strengthen specific processes and controls established with GSA IT Security Program through collaboration with officials across the Agency.

APPENDIX A - OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine if the General Services Administration (GSA) has developed, documented, and implemented an agency-wide information security program to provide information security for the data and systems that support the operations and assets of the Agency. If not, what additional actions are needed to strengthen information security risk management practices for GSA? We focused our review on the implementation of processes established with GSA's Information Technology (IT) Security Program to manage risks for select Agency IT systems. As such, we reviewed policies, procedures, technical guides, and standards established with GSA's IT Security Program to provide information security for the Agency's information resources and assets[14]. We also reviewed policies established for GSA's Privacy Program and for protection of Sensitive but Unclassified (SBU) buildings information[15]. We assessed the implementation of GSA's IT Security Program for five select Agency systems. Appendix B provides additional information on the systems reviewed. For these select systems, we conducted security audits to determine whether management, operational, and technical controls had been implemented to effectively manage risks in accordance with the Federal Information Security Management Act and GSA's IT Security Program.

To gain an understanding of GSA's IT Security Program and the implementation of controls for select Agency systems, we met with GSA IT security officials in the Office of the GSA Chief Information Officer and in Services, Staff Offices, and Regions (S/SO/R), including the Federal Acquisition Service, Public Buildings Service, Office of the Chief Human Capital Officer, and Office of the Chief Financial Officer. We also met with the GSA Chief Information Officer, Senior Agency Information Security Officer, and security officials for the select systems we reviewed. We also met with GSA's external auditor, KPMG, and considered results of information systems controls testing performed for the financial statement audit with our FISMA reviews.

In our review of GSA's IT Security Program, in addition to Agency policies and procedures, we evaluated the implementation of information security program elements from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers*, October 2006. To assess security controls, we applied the

---

[14] GSA Order CIO P. 2100.1D, *GSA Information Technology Security Policy*, June 21, 2007; GSA Order CIO 2106.1, *GSA Social Media Policy*, July 17, 2009; GSA Order CIO P 2106.2, *GSA Social Media Handbook*, July 17, 2009; GSA Directive CIO 2100.3A, *IT Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities*, June 26, 2008; GSA Order CIO 2104.1, *GSA Information Technology (IT) Rules of Behavior*, July 3, 2003; and various procedural and technical guides and standards established by the GSA-CIO.

[15] GSA Order CPO 1878.1, *GSA Privacy Act Program*, October 27, 2003; GSA Order CPO 1878.2, *Conducting Privacy Impact Assessments (PIAs) in GSA*, May 28, 2004; GSA Order HCO 9297.2A, *GSA Information Breach Notification Policy*, February 26, 2009; and PBS Order 3490.1A , *Document Security for Sensitive but Unclassified Building Information*, June 1, 2009.

NIST Federal Information Processing Standards (FIPS) Publication[16] and SP 800 series security guidelines. We also utilized other applicable regulations, policies, and guidance, including OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, November 2000; and the following OMB memoranda: M-05-04, *Policies for Federal Agency Public Websites*, December 17, 2004; M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; M-07-11, *Implementation of Commonly Accepted Security Configurations for Windows Operating Systems*, March 22, 2007; and M-08-05, *Implementation of Trusted Internet Connections (TIC)*, November 20, 2007.

To assess the effectiveness of GSA's IT Security Program implementation, we examined system certification and accreditation packages, including system risk assessments, security plans, security assessment results, contingency plans, and system-and program-level plans of action and milestones. We conducted vulnerability scanning and database and web application configuration testing for the select systems we reviewed. We manually tested specific security controls for social media websites, such as blogs and wikis, and various internal applications.

We conducted this performance audit in accordance with generally accepted government auditing standards between February and August of 2009. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[16] FIPS Publication 199, S*tandards for Security Categorization of Federal Information and Information Systems*, February 2004; FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

FY 2009 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

APPENDIX B – SELECT GSA SYSTEMS CONSIDERED IN THE OIG'S FY 2009 REVIEW OF GSA'S INFORMATION TECHNOLOGY SECURITY PROGRAM

APPENDIX C – SUMMARY OF NIST SP 800-53 CONTROL AREAS WHERE ADDITIONAL STEPS ARE NEEDED TO BETTER MANAGE RISKS FOR THE SELECT SYSTEMS REVIEWED BY THE OIG IN FY 2009

APPENDIX D – SUMMARY OF SECURITY CONTROL WEAKNESSES IDENTIFIED IN INTERNAL GSA APPLICATIONS

Due to the sensitive nature of information contained appendices B-D, only reports provided to system security officials and the GSA Office of the Chief Information Officer contain the details of the appendices. Requests for the details of the appendices should be referred to the Deputy Assistant Inspector General for Information Technology Audits.

APPENDIX E – GSA-CIO'S RESPONSE TO DRAFT REPORT

GSA

GSA Office of the Chief Information Officer

September 24, 2009

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

FROM: CASEY COLEMAN
CHIEF INFORMATION OFFICER (I)

SUBJECT: Draft FY 2009 Office of Inspector General FISMA Review of GSA'S Information Technology Security Program
Report Number A000126-1

This is in response to the IG draft audit on FY 2009 Office of Inspector General FISMA Review of GSA's Information Technology Security Program.

My staff has reviewed the draft audit report and we concur with your audit findings and recommendations.

If you or your staff have any questions or require additional information, please contact Kurt Garbars on 202-208-7485.

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

FY 2009 OFFICE OF INSPECTOR GENERAL
FISMA REVIEW OF GSA'S INFORMATION
TECHNOLOGY SECURITY PROGRAM
REPORT NUMBER A090126/O/T/F09011

APPENDIX F – REPORT DISTRIBUTION

Copies

WITH APPENDICES B-D

Chief Information Officer (I) 3

Office of the Senior Agency Information Security Officer (IS) 1

Commissioner, Public Buildings Service (P) 1

Commissioner, Federal Acquisition Service (Q) 1

Chief Financial Officer (B) 1

Chief Human Capital Officer (C) 1

Chief Acquisition Officer (V) 1

Regional Administrator, Great Lakes Region (5A) 1

WITHOUT APPENDICES B-D

Internal Control and Audit Division (BEI) 1

Assistant Inspector General for Auditing (JA and JAO) 2

Deputy Assistant Inspector General for Finance and Administrative Audits (JA-F) 1

Deputy Assistant Inspector General for Real Property Audits (JA-R) 1

Deputy Assistant Inspector General for Acquisition Audits (JA-A) 1

Regional Inspector General for Auditing (JA-5) 1

Administration and Data Systems Staff (JAS) 1

Assistant Inspector General for Investigations (JI) 1