WEAKNESSES IDENTIFIED DURING THE FY 2010 FEDERAL INFORMATION SECURITY MANAGEMENT ACT REVIEW

Report Number: 11-06

Date Issued: January 28, 2011

U.S. Small Business Administration
Office Inspector General

Memorandum

To: Paul T. Christy
Chief Information Officer

Date: January 28, 2011

/S/ original signed

From: Peter L. McClintock
Deputy Inspector General

Subject: Report on the Audit of SBA's Compliance with the Federal Information Security Management Act for FY 2010
Report No. 11-06

The Federal Information Security Management Act (FISMA) of 2002 provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. The Act requires (1) agencies to implement a set of minimum controls to protect Federal information and information systems; and (2) the agencies' Office of Inspector General (OIG) annually perform independent evaluations of the information security program and practices of that agency to determine its effectiveness. Finally, the Act directs the National Institute of Standards and Technology (NIST) to develop standards and guidelines for implementing its requirements in coordination with the Office of Management and Budget (OMB).

On April 21, 2010 OMB issued Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information System Management Act and Agency Privacy Management*; providing instructions for agency's to meet their FY 2010 reporting requirements under FISMA. This memorandum requires IGs to evaluate agency compliance in ten information security program areas: (1) Certification and Accreditation (C&A); (2) Configuration Management; (3) Security Incident Management; (4) Security Training; (5) Remediation/Plan of Actions and Milestones (POA&M); (6) Remote Access; (7) Identity Management; (8) Continuous Monitoring; (9) Contractor Oversight; and (10) Contingency Plans. The objective of our FY 2010 review was to evaluate the effectiveness of SBA's computer security program and practices in these areas in accordance with applicable Federal requirements[1].

To assess SBA's compliance in the OMB information security program areas, we reviewed agency documentation, interviewed program management officials, and performed reliability tests on agency-provided reports. Additionally, we selected judgmental samples of agency systems to conduct detailed analysis of their compliance with C&A, POA&M, and contingency planning requirements.

During the course of our FISMA review, we received an anonymous complaint alleging that contractors located in the IT security division were performing work on behalf of the agency without having obtained the necessary security clearances. The complaint also stated that these contractors had access to sensitive SBA information. In response to this allegation, we requested and reviewed SBA security clearance documentation for IT security contractors and interviewed Agency officials responsible for clearing contractors and granting network access.

We performed the audit work between August 2010 and November 2010 in accordance with *Government Auditing Standards* prescribed by the Comptroller General of the United States.

BACKGROUND

FISMA requires OIGs to perform annual independent evaluations of their agency's information security program and practices to determine its effectiveness. Since 2003, we have performed annual reviews of SBA's compliance with FISMA standards and guidelines established by NIST and reported our results to OMB. Previous OIG reviews identified and reported weaknesses in SBA compliance with requirements over information system configuration management, the development and management of ISAs, certification and accreditation of major information systems, and the identification and management of system vulnerabilities (i.e. POA&M). Additionally, during the course of our FY 2008 FISMA review, we determined that SBA did not consistently ensure that contractors were properly vetted prior to granting them access to sensitive SBA systems and data.

In 2004, we conducted an audit of SBA's Continuity of Operations Planning (COOP) Program. This audit identified significant deficiencies with SBA's continuity of operation and disaster response capabilities. Specifically, the audit

[1] Applicable Federal guidance include those provided in NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) as well as OMB Circulars and Memoranda.

found that SBA IT system disaster recovery plans were not adequate to ensure the recovery of its mission critical systems. As a result, SBA stated that it would develop and test recovery plans for its mission critical systems and revise the plans accordingly.

In FY 2009, SBA changed its IT security contractor and awarded a contract to Glacier Technologies, LLC to provide IT security support and information assurance measures and controls in accordance with FISMA, OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, and relevant SBA Standard Operating Procedures (SOPs).

RESULTS IN BRIEF

Our audit identified that significant improvements are needed in critical computer security areas in order for SBA to fully meet the requirements set forth in FISMA and OMB Circular A-130. We found that SBA did not maintain a complete and accurate inventory of system interfaces as required by FISMA. SBA also had not obtained interconnection security agreements (ISAs) for all systems that connect to other systems, as required by OMB Circular A-130. Only 5 of 26 systems with external interconnections currently had an ISA. ISAs are necessary to document the controls the system receiving SBA data must provide in order to protect its confidentiality, integrity and availability. Without interface inventories and ISAs, SBA cannot specify what data is transmitted from system to system and whether appropriate controls and adequate security are afforded to SBA data residing in external systems.

SBA did not have comprehensive and integrated configuration management policies and procedures, hardware and software inventories, and baseline configurations for all its systems, as required by FISMA and NIST guidance. As a result, systems may not be appropriately configured to provide adequate security over SBA information.

We also found that SBA did not properly identify, implement and assess baseline security controls as part of its system C&A process. Federal guidance requires that information systems be categorized according to risk and baseline controls selected and implemented based on their risk categorization. We found a system with baseline controls that were insufficient for its risk category; a high-risk system with its controls assessed as if it were a moderate-risk system; and a system certified and accredited using baseline controls from outdated and less stringent NIST guidance. As a result, SBA mission critical information systems may have inadequate and ineffective security controls, and control failures may not be appropriately identified for corrective action.

SBA did not track all the POA&M vulnerability information that OMB requires, adhere to planned remediation dates, and update the plan in a timely manner. As a result, the agency is unable to link security costs to security performance, cannot ensure that all weaknesses are included in the POA&M, and may remove un-remediated weaknesses from the POA&M, exposing the agency's systems to significant risk.

Our audit also disclosed that SBA did not develop or could not provide evidence it had developed system disaster recovery plans for [FOIA ex. 2] Additionally, during FY 2010, SBA did not test the disaster recovery plans for [FOIA ex. 2] As a result, SBA may be unable to restore its mission critical and major information systems within acceptable timeframes after a disaster.

During the course of our FISMA review, we received an anonymous complaint alleging that contractors located in the IT security division had access to sensitive information and were performing work on behalf of the agency without having obtained the necessary security clearances. We found that 17 of the 32 contractors we reviewed began working for SBA prior to the completion of their preliminary security clearance. As a result, SBA exposed itself to increased risk of unauthorized use and/or disclosure of sensitive and personally identifiable information.

Finally, several of our findings relating to FISMA noncompliance fall within the responsibilities of SBA's IT security contractor. An agency analysis of its contract with Glacier Technologies, LLC determined that many of the contract requirements were not being satisfied. While SBA has initiated corrective actions to ensure that its IT security contractor meets the provisions of its contract, continued oversight is needed to improve SBA's compliance with FISMA and other federal IT security requirements.

In order to address the deficiencies identified, we recommended that SBA: (1) update its major systems list to include all interfaces and obtain written ISAs for every system interconnection; (2) establish a program at SBA to manage, control and monitor system interconnections throughout their lifecycle; (3) develop configuration management policies and procedures; (4) develop and maintain a centralized inventory of all agency hardware and software; (5) develop and document baseline configurations for each information system; (6) revise the SBA C&A procedures to reflect the risk management framework approach established in NIST SP 800-37, Rev.1 and current POA&M guidance; (7) re-evaluate [FOIA ex. 2] and[FOIA ex. 2]security controls at the appropriate risk category using current NIST guidance; (8) modify the POA&M reporting tool to comply with OMB requirements; (9) develop and test system disaster recovery plans annually for major systems and implement corrective actions based on test results;

(10) enforce the agency SOP for contractor background investigations and perform periodic reviews to ensure compliance; and (11) conduct quality reviews of deliverables and quarterly reviews of IT security contractor performance. SBA management expressed concurrence with our recommendations.

RESULTS

SBA Has Not Developed a Complete Inventory of System Interconnections and Interconnection Security Agreements Have Not Been Established

SBA did not maintain a complete inventory of system interfaces to its major systems as required by FISMA. We reviewed seven SBA information systems and determined that interconnections identified in the C&A documentation were not included in SBA's interconnection inventory. Further, 13 of the interconnections not included in the interconnection inventory were to systems that are outside of the agency's control.

SBA could not provide evidence that it has established ISAs with all interconnected systems as required in OMB Circular A-130. We requested copies of ISAs for all SBA systems. In response, SBA only provided the audit team with four ISAs covering two major systems. However, SBA's interconnection inventory indicates that there are 24 systems with interconnections that require ISAs.

FISMA requires that an agencies major system inventory "shall include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency." Additionally, OMB Circular A-130 Appendix III requires prior written management authorization for system interconnections. For major applications, the Circular requires that shared information be given a level of protection that is comparable to the protection provided while residing within the source application. The Circular also requires that for authorized interconnections, controls be established consistent with NIST guidance.

Without a centralized management program for system interconnections, SBA cannot ensure that all interconnections will be documented in an ISA and necessary controls implemented, as required by Federal regulation. Additionally, without an inventory of interconnections and corresponding ISAs, SBA is not in a position to know which data is transmitted among its systems and to external systems; whether appropriate risk-based controls are applied to the data in the external systems; and whether external entities agree to adhere to SBA's rules of behavior.

SBA Had Not Developed Comprehensive Configuration Management Policies and Procedures and Had Not Inventoried or Established Baseline Configurations for All Systems.

FISMA requires every agency to develop an information security program that includes policies and procedures that ensure compliance with agency-determined minimally acceptable system configuration requirements. NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems* requires agencies to develop configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This guidance also requires agencies to develop procedures to facilitate the implementation of the configuration management policy. While SBA has established some configuration policies and procedures that relate to specific systems or networks, the agency had not developed an integrated agency-wide configuration management policy and associated procedures.

We found that SBA had not established baseline configurations for all hardware and software systems. SBA could not provide baseline configurations for many of SBA's major information systems, including financial systems such as the [FOIA ex. 2] and [FOIA ex. 2] The Office of Chief Information Officer (OCIO) was also unable to provide auditors with baseline configurations for all hardware (i.e. switches, printers).

SBA did not maintain complete inventories of its software and hardware. The software inventory provided during our review included only client-side software derived from Systems Management Server (SMS) scans. SMS scans only detect software on devices that have an active connection to the agency network. Other software applications, including major systems [FOIA ex. 2] were not included in the software inventory provided by SBA. The hardware inventory provided to the auditors was also not complete. It included only hardware with Microsoft operating systems installed that were directly attached to the SBA network.

NIST Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information System*s, specifies minimum security requirements for Federal information and information systems in seventeen security-related areas. In the configuration management security area, FIPS 200 states: "Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems."

Security configuration management provides an important function for establishing and maintaining secure information system configurations and provides important support for managing risks in information systems. Without an agency-wide configuration management policy, individual systems may adopt configurations that are not risk-appropriate. Without complete hardware and software inventories, systems or system components may escape the configuration management process altogether. Systems without configuration baselines may not implement critical controls and therefore lack the security that is commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized modification of the information they contain.

SBA Needs to Improve its Certification and Accreditation Process

During our FISMA review of SBA's C&A process, we identified weaknesses in SBA's procedures and the identification, application, and assessment of system baseline security controls. We found that while SBA has developed procedures to manage its C&A process, these procedures were outdated and were not reflective of the current NIST guidance over system security authorization and system control assessment. Additionally, these procedures had not been revised to correctly describe the agency-wide POA&M process. Finally, our review of system C&A packages found that three systems either did not adequately assess system security controls in accordance with NIST SP 800-53A guidance or the minimum baseline security controls were not appropriately selected up-front for assessment.

For two major systems [FOIA ex. 2] we noted the following:

- SBA’s [FOIA ex. 2] is rated as a “High” priority system under FIPS 199, “*Standards for Security Categorization of Federal Information and Information System,”* due to the level of confidentiality, integrity and availability of the information it supports. While it appeared that the appropriate baseline system security controls were selected for this system, these baseline controls were only tested at the “Moderate” level during the security control assessment phase.

- SBA's [FOIA ex. 2] was re-certified and accredited in April 2010 after a significant change in its control environment due to the migration to a new hosting provider. During the C&A process, however, SBA did not utilize current guidance in NIST SP 800-53 Revision 3, published in August 2009, which introduced additional controls and control enhancements for application to Federal information systems.

NIST SP 800-53A provides guidelines for assessing the effectiveness of security controls defined in NIST SP 800-53 based on the system FIPS 199 security categorization. Systems with higher impact levels require more comprehensive security control baselines and assessments of these security control baselines at this higher level.

Additionally, FIPS 200 requires federal agencies to comply with revisions in NIST Special Publications within one year. The guidance specifically states, "Federal agencies will have up to one year from the date of final publication to fully comply with the changes but are encouraged to initiate compliance activities immediately." Further, OMB Memorandum 10-15 states that for legacy systems undergoing significant changes, agencies are expected to be in compliance with the most recent NIST publications immediately upon deployment of the information system.

As a result of the weaknesses identified in SBA's C&A program, system controls in SBA [FOIA ex. 2] information systems may not be implemented or operating effectively and control failures may not be appropriately identified for corrective action.

SBA's POA&M Program Reporting Tool Did Not Adequately Track Weaknesses, Provide Accurate Estimated Dates for Remediation, and Was Not Updated Timely

SBA's POA&M reporting tool did not include or sufficiently track all required fields. OMB M-04-25, *"FY 2004 Reporting Instructions for the Federal Information Security Management Act"*, identifies eight fields to be tracked by an agency's POA&M process. In FY 2010, SBA migrated its centralized POA&M database to its [FOIA ex. 2] in order to provide transparency and accountability over information system vulnerabilities. We commend SBA's effort to increase visibility of its POA&M and responsibility for the mitigation of system vulnerabilities. However, the current SBA reporting tool did not adequately track the following risk mitigation fields: funding resources, changes to milestones, how the weakness was identified (i.e. source), and the status.

During our FISMA review of SBA's POA&M process, we found that weaknesses were not adequately managed and that SBA did not sufficiently mitigate vulnerabilities by the estimated remediation date. For two major SBA systems, vulnerabilities either detected through internal system scans or IG reports were not placed into the system's POA&M for remediation. Additionally, SBA closed two "Medium" risk vulnerabilities for its [FOIA ex. 2] without completing the proposed actions to remediate the vulnerabilities. Finally, for three major SBA systems, initial estimated remediation dates for system vulnerabilities were missed. For example, [FOIA ex. 2] had four "High" risk vulnerabilities still unresolved from its C&A in 2006. These vulnerabilities were initially scheduled to be completed by March 2007.

We also found that SBA's POA&M reporting tool was not updated on a timely basis. System owners were often non-responsive to OCIO requests for quarterly system vulnerability status updates. For example, system owners for four major SBA systems did not respond to OCIO information requests for over six months.

OMB Memorandum 04-25 provides guidance to agencies to implement their agency-wide POA&M process. It requires that POA&Ms be established for all agency information systems with identified vulnerabilities and that security costs for a system be linked to its security performance. POA&Ms should include all known security weaknesses, including weaknesses identified in audits and critical infrastructure vulnerability assessments. The memorandum also establishes mandatory fields and information agency POA&Ms must include and requires program officials to update the agency Chief Information Officer (CIO) on their progress on a quarterly basis.

The purpose of a POA&M program is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. Without a comprehensive, documented, and functioning POA&M process, the agency will be unable to link security costs to security performance and weaknesses may be accidently omitted or closed without satisfactory remediation exposing the SBA's systems to significant risk.

SBA's Continuity of Operations Planning and Testing Program for Mission Critical Information Systems Needed Significant Improvement

During our FISMA review of SBA's COOP Program, we found that system disaster recovery plans had not been developed or tested. SBA was unable to provide evidence that it had developed system contingency plans for[ex. 2]of its [ex. 2] major systems. Additionally, SBA documentation supported that only[ex. 2]major systems received recovery tests during the year.

SBA SOP 90-47-2 *"Automated Information System Security Program"* states that a disaster recovery plan must be prepared and tested semi-annually for each major application system, each regional and district accounting information system, the Office of Financial Operations, and SBA's mainframe computer center. Additionally, NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems,* states that information system contingency plan testing is a critical element of a viable contingency capability. Testing enables plan deficiencies to be identified and addressed by validating one or more of the system components and the operability of the plan.

Without documented system recovery plans that have been tested to ensure their effectiveness, SBA may be unable to restore its [FOIA ex. 2] major information systems within established timeframes.

SBA IT Security Contractors Were Permitted Access to Sensitive Information and Secured Areas Without Required Clearances

While performing our FISMA review, we received an anonymous complaint alleging that contractors located in the IT security division were performing work on behalf of the agency without having obtained the necessary security clearances. In response to this allegation, we compared OCIO IT Security contractor start dates with background clearance forms provided by OCIO and found that 17 of 32 contractors performed work on behalf of the agency prior to being cleared. Some of these contractors were operating in SBA's security operations center which allowed physical access to sensitive information and systems.

Additionally, our review of system POA&Ms identified two ongoing vulnerabilities related to contractor background investigations. Specifically, the POA&M for SBA's [FOIA ex. 2] identified that contractors had not undergone SBA background investigations and their company-sponsored background investigations did not meet Federal criteria. Additionally, the POA&M for SBA's [FOIA ex. 2] identified that background investigations were not performed for contractor personnel responsible for daily system operations.

OMB Circular A-130 requires Federal agencies to screen individuals applying for access to government data and systems based on the level of risk presented by their access. SBA SOP 90-47-2 classifies all SBA data as sensitive and requires all contractor personnel to undergo background investigations. In addition, contractor personnel occupying positions designated as critical-sensitive cannot be given access to sensitive data until an appropriate security clearance has been granted. SBA requires that SBA Form 1228, *Computer Access*

Clearance/Security, be used to request all network account access for new contractor employees.

Despite SBA's requirement that contractors occupying positions sensitive in nature must receive prior clearance, this requirement was not adhered to for many of the contractors performing IT security functions for the agency. Without ensuring that contractors meet the agency standards for character and integrity, SBA is exposing itself to increased risk for unauthorized use and/or disclosure of sensitive and personally identifiable information.

SBA Needs to Improve Oversight of the IT Security Contract

We noted that several of our findings relating to FISMA noncompliance fell within the existing performance work statement between SBA and its IT security contractor. These areas included maintaining system inventories, coordinating ISAs, configuration management and control, performing certification and accreditations of SBA systems, managing SBA's POA&M process, and providing support to SBA in the development of continuity of operation plans. Under the contract, Glacier Technologies, LLC is also responsible for incident response, security awareness training and the continuous monitoring of security controls.

In September 2010, the Acting Chief Information Security Officer performed an analysis of SBA's contract with Glacier Technologies, LLC and found that many of the contract requirements were not being satisfied. As a result, SBA issued recommendations to the contractor and established milestones for compliance.

We commend SBA on taking actions to ensure that its IT security contractor meet the provisions of its contract. However, the contract provides for SBA to conduct continuous quality assurance reviews and quarterly performance reviews of the above activities. We believe that ongoing oversight is needed to ensure all work products meet established Federal quality standards.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Update the list of Major Systems to include all the interfaces between each system and all other systems and networks, including those not operated by, or under the control of the agency and obtain written Interconnection Security Agreements for every SBA system that has an interconnection to another system.

2. Establish a program at SBA to manage, control and monitor system interconnections throughout their lifecycle. The program should

encompass planning, establishing, maintaining and terminating system interconnections, including enforcement of security requirements.

3. Develop configuration management policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

4. Develop and maintain a centralized inventory of all agency hardware and software.

5. Develop and document baseline configurations for each information system and maintain the baseline under configuration control.

6. Revise the SBA Certification and Accreditation Program Description procedural document to reflect the risk management framework approach established in NIST SP 800-37, Rev.1 and the current POA&M process.

7. Re-evaluate the technical, operational and management controls of [FOIA ex. 2] and[FOIA ex. 2]at the appropriate FIPS 199 level using guidance provided by NIST SP 800-53 and NIST SP 800-53A.

8. Modify the POA&M reporting tool to comply with the requirements set forth in OMB Memorandum 04-25.

9. Develop and test system disaster recovery plans for all of SBA's major systems at least annually and initiate any necessary corrective actions based on test results.

10. Enforce SOP 90-47 2 requirements for contractor background investigations and perform periodic reviews to ensure that SBA contractors have completed the clearance process prior to accessing sensitive information.

11. Perform continuous quality assurance reviews of deliverables and quarterly reviews of IT security contractor performance to ensure all applicable areas of OMB and NIST compliance criteria are met.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On December 23, 2010, we provided the Chief Information Officer with the draft report for comment. On January 21, 2011, the Chief Information Officer submitted a formal response, which is contained in its entirety in Appendix I. The response expressed concurrence with all of the recommendations presented in this report.

ACTIONS REQUIRED

Please provide your management decision for each recommendation on the attached SBA forms 1824, Recommendation Action Sheet, within 30 days from the date of this report. Your decision should identify the specific action(s) taken or planned for each recommendation and the target date(s) for completion.

We appreciate the courtesies and cooperation of the OCIO during this audit. If you have any questions concerning this report, please call me at (202) 205-[ex. 2] or Jeffrey Brindle, the Director, Information Technology and Financial Management Group at (202) 205- [ex. 2]

APPENDIX I. MANAGEMENT COMMENTS

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

Date: January 21, 2011

To: Peter L. McClintock
Deputy Inspector General

From: Paul T. Christy
Chief Information Officer

Subject: Draft Report on the Audit of SBA's Compliance with the Federal Information Security Management Act for FY 2010

The Office of Chief Information Officer has reviewed and concurs with the findings posted in the draft report. Further explanation of corrective action will be provided in the Management Decision.

If you require additional information, please contact Ja'Nelle DeVore on 202-205-[ex. 2]