U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

ADVISORY MEMORANDUM
REPORT NO. 12-15

DATE: July 16, 2012

TO: Eric Won
Chief Information Officer

SUBJECT: Weaknesses Identified During the FY 2011 Federal Information Security Management Act Review

The purpose of this memorandum is to report risk areas requiring management follow-up as a result of our most recent Federal Information System Management Act (FISMA) review. The act requires Office of Inspectors General (OIG) to perform annual independent evaluations of their agency's information security program and practices to determine their effectiveness.

To determine SBA's compliance in these areas, the OIG contracted with Independent Public Accountant (IPA), KPMG, to perform the audit procedures relating to FISMA. The IPA interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's Information Technology (IT) security controls. The OIG monitored the IPA's work and reported the SBA's compliance with FISMA with the Agency FISMA filings on November 4, 2011.

The OIG's Fiscal Year 2011 review found that significant improvements were needed in critical computer security areas in order for the SBA to fully meet the requirements set forth in FISMA and Office of Management and Budget (OMB) Circular A-130.[1] We performed additional fieldwork between November 2011 and March 2012 to further clarify issues and recommend corrective actions. This work was performed in accordance with Generally Accepted Government Auditing Standards, prescribed by the Comptroller General of the United States. 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.

The results of our review showed that the Office of Chief Information Officer (OCIO) needs to prioritize remediation of IT security vulnerabilities identified in prior audits. Furthermore, the OCIO also needs to perform recertification reviews of its general support system's end users and monitor remote access logs for unauthorized activity. We are re-issuing a prior year recommendation relating to the OCIO's oversight of its IT Security Contractor.

[1] Management of Federal Information Resources

To prevent future degradation of its security environment, the SBA needs to immediately undertake remediation actions to establish practices which will ensure effective oversight of potential security risks and resolve outstanding audit recommendations.

We request that you provide your management decision for each recommendation on the attached SBA Form 1824, Recommendation Action Sheet, 8/15/2012 (30 days after final report date). Your decision should identify the specific actions taken or planned for each recommendation and the target dates for completion.

***

Background

The Federal Information Security Management Act (FISMA) requires federal agencies to develop, implement, and report on the effectiveness of the agency's information security program. For Fiscal Year(FY) 2012, the OIG was required to report on the following 11 areas: 1) risk management; 2) configuration management; 3) incident response and reporting; 4) security training; 5) plan of actions and milestones; 6) remote access management; 7) identity and access management; 8) continuous monitoring management; 9) contingency planning; 10) contractor systems; and 11) security capital planning.

Results

The SBA Continues to Subject Itself to Risks through Unresolved IT Recommendations

Unresolved audit recommendations left SBA's IT security posture vulnerable to external and internal threats. Our review of outstanding recommendations in the FISMA controls areas showed that 30 OIG audit recommendations remained open as of January 2012. [2]

The OMB Circular A-50, on audit follow-up, states that agencies' audit follow-up system must require prompt resolution and corrective actions on audit recommendations. Further, resolutions shall be made within six months and corrective actions should be implemented as soon as possible. The SBA's Standard Operating Procedures (SOP), Audit Follow-up System, requires program offices to complete the implementation of recommendations within a year of management and the OIG's agreement on the plan.

As of January 2012, there were 30 open OIG audit recommendations in the FISMA controls areas. One of these recommendations dated back to the OIG's audit of SBA's FY 2006 financial statements. This occurred mainly due to the lack of timely implementation of the recommendations directly relating to FISMA reporting areas. As a result, these unresolved IT recommendations left SBA's systems vulnerable to external and internal threats. The underlying conditions that require correction in the open audit recommendations are integral to the SBA complying with FISMA guidance.

[2] This number does not include four open recommendations that were repeated over multiple fiscal years.

A complete listing of each outstanding recommendation and its particular status can be found in Appendix 1. A summary of the recommendations by reporting area and date the corrective action was first recommended is included below:

Risk Management

The oldest outstanding OIG recommendation in this category was issued on January 28, 2011. There are three outstanding recommendations pertaining to:

- SBA Certification and Accreditation
- System interconnections

Configuration Management

The oldest outstanding OIG recommendation in this category was issued on November 12, 2010. There are five outstanding recommendations from two audits pertaining to:

- Configuration management policies and procedures
- Baseline configurations
- Inventory

Incident Response and Reporting

The oldest outstanding OIG recommendation in this category was issued on November 14, 2011. There are two outstanding recommendations pertaining to:

- *Vulnerability assessment*
- *Incident management*

Security Training

The oldest outstanding OIG recommendation in this category was issued on November 12, 2010. There is one outstanding recommendations pertaining to:

- *Training and monitoring*

Plan of Action and Milestones (POA&M)

The oldest outstanding OIG recommendation in this category was issued on January 28, 2011. There is one outstanding recommendations pertaining to:

- *POA&M reporting tool compliance*

Remote Access Management

The oldest outstanding OIG recommendation in this category was issued in this report. There is one outstanding recommendations pertaining to:

- *Log monitoring*

Identity and Access Management

The oldest outstanding OIG recommendation in this category was issued on November 15, 2006. There are ten outstanding recommendations issued in four previous audit reports and one outstanding recommendation issued in this report pertaining to:

- *Segregation of duties*
- *End user authentication*
- *Account management*
- *Least privilege*

Continuous Monitoring Management

The oldest outstanding OIG recommendation in this category was issued on November 12, 2010. There are three outstanding recommendations from two audit reports pertaining to:

- Log monitoring
- Vulnerability tracking and monitoring
- Vulnerability management processes

Contingency Planning

The oldest outstanding OIG recommendation in this category was issued on January 28, 2011. There are three outstanding recommendations from two audit reports pertaining to:

- *Planning and testing*
- *Alternate storage site*

Contractor Systems

The oldest outstanding OIG recommendation in this category was issued on January 28, 2011. There is one outstanding recommendations pertaining to:

- *Background investigations*

Security Capital Planning

There are currently no outstanding recommendations for Security Capital Planning

Recommendation

We recommend that the Chief Information Officer:

1. Develop an overall strategy to timely implement audit recommendations issued by the OIG relating to FISMA security requirements.

The SBA Has Not Fully Implemented Security Practices Outlined in Its IT Security Assistance Contract

The SBA has a number of tasks in its IT security assistance contract with Glacier Technologies which are not being performed. This finding was identified during our last review of FISMA and is being re-issued due to incomplete implementation.

The SBA entered into an IT security assistance contract with Glacier Technologies to provide: 1) project management; 2) general information security support; 3) certification and accreditation; 4) audits; 5) FISMA reviews and analyses; 6) disaster recovery and contingency planning; 7) security operations and vulnerability assessment; 8) information privacy support; 9) incident response management; and 10) risk management.

We found that the SBA has not required the IT security assistance contractor to perform four specific tasks outlined in the contract:

- **Configuration Management –** The contractor is to conduct configuration management and maintain configuration control of all SBA IT resources to include operating system and application system updates, revisions and patches.

  According to OCIO officials, configuration management was outside of the responsibility of the security assistance contractor since these services were provided by a different vendor. However, the establishment and monitoring of baseline configurations are FISMA reporting requirements and the contractor is responsible for maintaining configuration control according to their contract.

- **Threat Analysis of Engineering Change Requests –** The contractor is to perform threat analyses of SBA Engineering Change Requests.

  The OCIO stated that SBA’s Enterprise Change Control Board performed the threat analysis of SBA engineering change requests. Further, the security assistance contractor did not perform threat assessments. However, threat analysis is needed on change requests as part of documenting and testing. The testing of change requests which affect system baseline configurations is a FISMA reporting requirement under Configuration Management.

- **Software Application Security –** The contractor is to ensure software application security.

  The OCIO stated that the security assistance contractor performed vulnerability scans of only internal applications. However, an application security program should also include continuous monitoring of baseline configurations for all internal and external major applications.

  The monitoring of contractor baselines is a FISMA reporting requirement under Configuration Management and Continuous Monitoring Management.

- **Review and prepare responses to Interagency Security Agreements** – The contractor is to review and prepare responses to Interagency Security Agreements (ISA), Memoranda of Agreement (MOA), and Memoranda of Understanding (MOU).

  The OCIO stated that it has the responsibility to finalize ISAs, MOAs, and MOUs. These documents specify security controls used to protect SBA systems and data, documents the terms and conditions for sharing data, and defines the purpose of the interconnection. The security assistance contractor can perform the preliminary documentation relating to the ISA, MOA, and MOU. The lack of fully utilizing a contract whereby the contractor receives full remittance for services, which should be performed under the terms of the contract, prevents SBA from receiving the full value of its contract capabilities.

Recommendation

We recommend that the Chief Information Officer:

2. Perform continuous quality assurance reviews of deliverables and quarterly reviews of IT security contractor performance to ensure all applicable areas of OMB and National Institute of Standards and Technology (NIST) compliance criteria are met.

The SBA has Not Recertified Its Network Users in Compliance with NIST Guidance

The IPA determined that SBA's Local Area Network/Wide Area network (LAN/WAN) general support system had not had its user population reviewed or recertified for appropriate levels of access to the network within the past year. The timely recertification of network users is necessary to ensure that individuals have the appropriate level of access to the network.

The NIST's Recommended Security Controls for Federal Information Systems requires that, for access control and account management purposes, accounts should be reviewed at an organization-defined frequency. This review should update the accounts of authorized users to ensure that individuals have the appropriate level of access to the network. Further, it ensures that personnel with high-level privileges still have a need for the elevated level of access to perform their duties.

The SBA did not review and recertify its user population, including highly privileged users, to its general support systems for appropriate access within the past year. As a result, SBA systems were vulnerable to personnel having a greater level of access than needed and possibly performing duties for which they were not authorized to perform.

Recommendation

We recommend that the Chief Information Officer:

3. Perform periodic recertification reviews of end-users in agency general support systems to ensure that users are authorized and have current access privileges. Alternatively, design compensating controls for recertification for end-users of general support systems.

Remote Access Audit Logs Were Not Reviewed for Unauthorized Activity

The SBA remains at risk of not timely detecting unauthorized access to computer networks. The SBA's SOP, Automated Information System Security Program, requires system administrators and database administrators to review and analyze audit logs at least weekly to identify unauthorized user activity and system errors. According to OCIO officials, the SBA did not review its Virtual Private Network (VPN) audit logs for unauthorized activity within the past year. This leaves the systems vulnerable to individuals trying to penetrate the network through the SBA's current remote access protocols and gaining unauthorized access to SBA's network and financial systems.

Recommendation

We recommend that the Chief Information Officer:

4. Continuously monitor remote access audit logs for potential unauthorized activity.

AGENCY COMMENTS AND OIG RESPONSE

On June 5, 2012, we provided a draft of this report to the Chief Information Officer. On June 22, 2012, the Office of Inspector General received SBA's comments. A summary of management's comments and our response follows.

Agency Comments

The CIO agreed to the accuracy of the current and prior year recommendations, provided updates on statuses, and adjusted closure dates. The OCIO closed one recommendation since the completion of the OIG's fieldwork and stated that they were working hard to remediate the remaining open findings.

Additionally, the CIO stated that configuration management is being performed by the Office of Communications and Technology Services and they are in the process of having the item removed from their security assistance contract.

OIG Response

We found that the OCIO concurred with our findings and recommendations. Included in the OCIO's response were revised completion dates of outstanding audit recommendations referenced in Appendix I.

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 Small Business Administration during this audit.

If you have any questions concerning this report, please call me at (202) 205-7390 or Jeff Brindle, Director, IT and Financial Management Group at (202) 205-7490.

***

/S/ original signed.
John K. Needham
Assistant Inspector General for Auditing

Appendix I: Open Current and Prior Year FISMA Recommendations

FISMA Open Recommendations Relating to our Department of Homeland Security Cyber-Scope Evaluation (All recommendations are to the Chief Information Officer unless otherwise noted)

Risk Management – The organization develops and implements a comprehensive strategy to manage risk to IT organizational operations and assets.

- 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. *Recommendation Closure was due 9/30/2011.*

- 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. *Recommendation Closure was due 9/30/2011.*

- 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. *Recommendation Closure was due 6/30/2011.*

Configuration Management – The organization develops minimally acceptable system configuration requirements to ensure a baseline level of security for its IT operations and assets.

- Develop configuration management policies and procedures that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. *Recommendation Closure was due 9/30/2011.*

- Develop and maintain a centralized inventory of all agency hardware and software. *Recommendation Closure was due 9/30/2011.*

- Develop and document baseline configurations for each information system and maintain the baseline under configuration control. *Recommendation Closure was due 9/30/2011.*

- Implement configuration management policies and procedures for document retention (to include supporting evidence) to validate the authorization of operating system changes. *Recommendation closure is due 9/28/2012.*

- Enforce an organization-wide configuration management process, to include policies and procedures for maintaining documentation that supports testing and approvals of software changes. This recommendation was reported in audits of SBA's financial statement for FY 2010 and FY 2011. The original *recommendation closure was due 4/30/2011.*

Incident Response and Reporting –The organization establishes an incident handling capability as well as tracking, documenting and reporting incidents to appropriate authorities.

- Update the vulnerability assessment team (VAT) procedures, to include: (a) updating the VAT policies and procedures in accordance with NIST, (b) performing technical reviews of the results for critical issues that need immediate action and take timely corrective action, (c) executing procedures to monitor the completion of the patch management deployment across the SBA enterprise, and (d) prioritizing vulnerabilities as part of the ongoing continuous monitoring process. *Recommendation closure was due 3/31/2012.*

- Coordinate with SBA program offices to fully implement the SBA entity wide incident management and response program and ensure that procedures are enforced. *Recommendation closure was due 2/29/2012.*

Security Training – The organization ensures that users of information systems are aware of IT security risks, compliance with applicable laws and regulations, and that personnel are trained in their security-related responsibilities.

- Develop a comprehensive security education and training program for all IT security personnel and a method for monitoring the training program. This recommendation was reported in audits of SBA's financial statement for FY 2010 and FY 2011. The original *recommendation closure was due 6/1/2011.*

Plan of Actions and Milestones (POA&M) – The organization implements plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in information systems.

- Modify the POA&M reporting tool to comply with the requirements set forth in OMB Memorandum 04-25. *Recommendation closure was due 4/30/2011.*

Remote Access Management – The organization documents allowed methods of remote access, establish usage restrictions, and monitor for unauthorized remote access.

- Continuously monitor remote access audit logs for potential unauthorized activity. *(Current Year FISMA Review Recommendation)*

Identity and Access Management – The organization identifies and authenticates system users, and limits system users to the information, functions, and information systems those users are authorized to operate.

- Prevent users from anonymously connecting unauthorized devices by developing and implementing procedures to ensure mandatory domain authentication for IP address issuance. This recommendation was reported in audits of SBA's financial statement for FY 2010 and FY 2011. The original r*ecommendation closure was due 4/15/2011.*

- Coordinate with SBA program offices to ensure users access rights are authorized prior to gaining access to financial systems. *Recommendation closure was due 3/30/2012.*

- Coordinate with SBA program offices to develop and implement procedures for user access reviews to ensure that the proper access rights are set for financial subsystems. This recommendation was reported in audits of SBA's financial statement for FY 2010 and FY 2011. *The original recommendation closure was due 4/29/2011.*

- Oversee the review and validation of financial system accounts on a quarterly basis. *Recommendation closure is due 4/30/2012.*

- Enforce financial system password controls for System Administrators and Database Administrators and physical access controls in accordance with SBA SOP 90.47.2. *Recommendation closure was due 3/18/2011.*

- The Chief Operating Officer in conjunction with program offices, document and implement segregation of duty policies and procedures for LAS. *Recommendation closure was due 12/15/2010.*

- The Chief Operating Officer in conjunction with appropriate program officials should ensure that policies are implemented regarding segregation of duties for FRIS, JAAMS, DCMS, and LAS. *Recommendation closure was due 6/30/2011.*

- Perform periodic recertification reviews of end-users in agency general support systems to ensure that users are authorized and have current access privileges. Alternatively, design compensating controls for recertification for end-users of general support systems. *(Current Year FISMA Review Recommendation)*

- Restrict access to software program libraries based on the principle of least privilege, and implement compensating controls over actions where limited resources cause individuals to perform conflicting job functions. *Recommendation closure is due 6/30/2012.*

- Ensure that database administrators and system administrator access is restricted through role-based segregation of duties and managed through an effective audit log review process. *Recommendation closure is due 6/30/2012.*

Continuous Monitoring Management – The organization establishes a continuous monitoring capability for configuration control as well as performing ongoing security assessments of the information system.

- Implement a process to review the audit logs of all financial applications on a regular basis. Oversee the review and validation of financial system accounts on a quarterly basis. *Recommendation closure was due 3/30/2012.*

- Improve the vulnerability tracking and monitoring process to fully address high and medium risk vulnerabilities for key financial systems. Ensure that the vulnerability reports are reviewed and analyzed on a regular basis. Periodically monitor the existence of necessary services and protocols running on servers and network devices. Develop a more thorough approach to track and mitigate patch management and configuration management vulnerabilities identified during monthly scans. *Recommendation closure was due 4/30/2011.*

- Enhance security vulnerability management processes. Specifically, SBA should: (a) redistribute procedures and train employees on the process for reviewing and mitigating security vulnerabilities, (b) periodically monitor the existence of unnecessary services and protocols running on their servers and network devices, (c) perform vulnerability assessments with administrative credentials and penetration tests on all SBA offices from a centrally managed location with a standardized reporting mechanism that allows for trending, on a regularly scheduled basis in accordance with National Institute of Standards and Technology (NIST) guidance, (d) develop a more thorough approach to track and mitigate configuration management vulnerabilities identified during monthly scans, and (e) monitor security vulnerability reports for necessary or required configuration changes to their environment. *Recommendation closure was due 3/31/2012.*

Contingency Planning – The organization implements plans for emergency response, backup operations, and post-disaster recovery for organizational information systems.

- 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. *Recommendation closure was due 7/30/2011.*

- Enforce existing SBA policies to rotate backups off-site. *Recommendation closure is due 4/30/2012.*

- Coordinate with the Chief Financial Officer to create, implement, and test system specific and the Headquarter Continuity of Operations Plan. *Recommendation closure is due 7/30/2012.*

Contractor Systems – The organization ensures that its contractors abide by FISMA requirements.

- 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. *Recommendation closure was due 5/30/2011.*

Security Capital Planning – The organization ensures that the resources needed to implement the IT security program are available for expenditure as planned.

No current recommendations exist for Security Capital Planning.

Prior Coverage

Multiple audits and reviews have been conducted between 2003 and 2011 related to FISMA.
The OIG reports used in this audit, which can be accessed at http://www.sba.gov/office-of-inspector-general include:

- Audit of SBA's FY 2011 Financial Statements – Management Letter, November 14, 2011, Report Number 12-02
- OIG FISMA Report 11-06—Weakness Identified During the FY 2010 Federal Information Security Management Act Review, Report Number 11-06.
- Audit of SBA's FY 2010 Financial Statements – Management Letter, December 15, 2010, Report Number 11-03.
- Audit of SBA's FY 2008 Financial Statements – Report Number 09-03.
- Audit of SBA's FY 2006 Financial Statements – Report Number 07-03.

Appendix II: Agency Comments

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF THE CHIEF INFORMATION OFFICER

DATE: June 21, 2012

TO: John K. Needham
Assistant Inspector General for Auditing

SUBJECT: Response – Weaknesses Identified During the FY2011 Federal Information Security Management Act (FISMA) Review

The purpose of this memorandum is to provide a response to the Office of Inspector General's memorandum regarding FY 2011 FISMA weaknesses.

The following written comments are submitted for your review and acceptance.

Page 5, bullet 1 and Page 4, Recommendation 1
The Glacier contract is in the process of being modified to remove the Configuration Management task that the contractor is not required to perform. This task is covered under the Office of Communications and Technology Services.

Pages 8-11, Appendix I: Open Current and Prior Year FISMA Recommendations
The Open Current and Prior Year FISMA recommendations are still accurate. However, OCIO is diligently working to remediate the open findings. The following response includes proposed adjusted closure dates for your review and acceptance.

We appreciate the opportunity to comment and look forward to reviewing the final action memorandum.

/s/ Original Signed
Eric Won
SBA Chief Information Officer