Evaluation Report

Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review

April 30, 2014 Report Number 14-12

U.S. Small Business Administration
Office of Inspector General
Washington, D.C. 20416

FINAL REPORT TRANSMITTAL
REPORT NUMBER 14-12

DATE: April 30, 2014

TO: Renee Macklin, Chief Information Officer

SUBJECT: Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review

This report presents 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.

We conducted this evaluation in accordance with the Council of Inspectors General on Integrity and Efficiency (CIGIE) Standards for Inspection and Evaluations. Those standards require that we plan and perform the evaluation to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our objectives.

The SBA continues to need to prioritize remediation of IT security vulnerabilities identified in prior audits. 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 appreciate the courtesies and cooperation of the SBA extended to the staff during this review. Please direct any questions to me at (202) 205-7100 or Jeff Brindle, Director, IT and Financial Management Group at (202) 205-7490.

***

/s/
Robert A. Westbrooks
Deputy Inspector General

Executive Summary

Report Number 14-12

Weaknesses Identified During the FY 2013 Federal Information Security Management Act Review

What the OIG Reviewed

The Federal Information Security Management Act (FISMA) requires that the OIG review the SBA's Information Technology (IT) Security Program. To determine SBA's compliance with FISMA, the OIG contracted with Independent Public Accountant (IPA), KPMG, to perform review 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 in the Agency FISMA filings in December 2013. We also assessed progress in remediating open recommendations and compared our current year assessment with our FY 2012 FISMA evaluation.

What the OIG Found

In the annual FISMA report to the Department of Homeland Security, the OIG found SBA had sufficiently established its plan of actions and milestones, remote access management, security training, computer security incidents, contingency planning, contractor systems, and security capital planning. However, the SBA needs to further establish its configuration management, identity and access management, risk management, and continuous monitoring controls. In addition to weaknesses identified in FY 2013, the SBA needs to continue to remediate outstanding and overdue recommendations.

In the area of configuration management, the SBA continued to have challenges remediating vulnerabilities and implementing baseline configurations. Prior recommendations in these areas remained open.

Similarly, prior recommendations and actions addressing weaknesses in identity and access management remained open. The SBA needs to complete the implementation of its network access control tools and personal identification verification for logical access.

During our FY 2013 assessment, we also found that SBA's system authorization packages and continuous monitoring need improvement. Documentation for some sampled systems were either incomplete or were not updated as required.

Summary of FISMA Results by Category for FY 2013[1]

Configuration Management	Limited Progress
Identity and Access Management	Progress
Risk Management	Limited Progress
Continuous Monitoring	Limited Progress
Plan of action and Milestones	Substantial Progress
Remote Access Management	Limited Progress
Security Training	Substantial Progress
Incident Response and Reporting	Limited Progress
Contingency Planning	Substantial Progress
Contractor Systems	Progress
Security Capital Planning	Limited Progress

OIG Recommendations

In addition to already open FISMA relevant recommendations in Appendix II, the OIG made seven new recommendations to address weaknesses in the areas of: Identity and Access Management, Risk Management, POA&Ms, and Security Training.

Agency Comments

On April 22, 2014; management submitted comments and was in full agreement with our findings and recommendations.

[1] Our assessment compared affirmative responses in the OIG's FY 2013 versus FY 2012 Cyberscope results:

- Substantial Progress > 15% improvement
- Progress 5-15% improvement
- Limited Progress <5% improvement

Table of Contents

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) 2013, the OIG was required to report on the following 11 areas: (1) configuration management; (2) identity and access management; (3) risk management; (4) continuous monitoring controls; (5) plan of actions and milestones; (6) remote access management; (7) security training; (8) computer security incidents; (9) contingency planning; (10) contractor systems; and (11) security capital planning.

Results

In FY 2013, the SBA continued to show limited progress in meeting FISMA requirements. To demonstrate measurable progress, the SBA needs to remediate the 17 prior-year open recommendations relating to FISMA reporting areas identified in Appendix II of this report.

1) Configuration Management

The SBA received an overall assessment that it had not established a Configuration Management program that is consistent with FISMA reporting areas in the Cyberscope evaluation. In that regard, the SBA continues to have severe and long-standing configuration management vulnerabilities which affect the secure operation of the SBA's general support systems and major applications. These long-standing vulnerabilities contributed to SBA receiving a "red" for system software controls in the OIG's Management Challenge #2 on computer security.

2) Identity and Access Management

The SBA received an overall assessment that it had not established an Identity and Access Management program that is consistent with FISMA reporting areas in the Cyberscope evaluation. The SBA has identity and access management weaknesses which could potentially affect the security and authenticity of connections to SBA's general support systems and major applications.

Personal Identification Verification for Logical Access has Not Been Timely Implemented

As part of the OIG's FY 2012 FISMA evaluation, SBA identified that it would implement Personal Identification Verification (PIV) for logical access to SBA systems by September 30, 2013. As of October 1, 2013, the SBA reports that it will implement PIV for logical access by September 30, 2014.

According to OMB Memorandum Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors (Memorandum 11-11), requires that each agency is to develop and issue an implementation policy, by March 31, 2011, through which the agency will require the use of the PIV credentials as the common means of authentication for access to that agency's facilities, networks, and information systems.

Recommendation 1

We recommend that the Chief Information Officer implement Personal Identification Verification (PIV) for logical access to all SBA systems.

3) Risk Management

The SBA received an overall assessment that it had not established a Risk Management program that is consistent with FISMA reporting areas in the Cyberscope evaluation.

Security Authorization Packages were Not Complete

Security Authorization Packages for the ten systems sampled contained the following problems, issues or non-compliances:

- Five of ten systems sampled did not have adequate and up-to-date System Security Plans,
- Eight of ten systems sampled did not have Risk Assessments updated annually as required,
- Seven of ten systems sampled did not have Security Control Assessments completed during the year as required, and
- Four of six systems sampled did not have Plans of Actions and Milestones (POA&M) developed and entered into SBA's Cyber Security Asset Management tool.

The SBA SOP 90-47.3, Chapter 4, Section 5 – Security Authorization requires that agencies periodically review the security controls in their system and authorize system processing prior to operations and periodically thereafter. SOP 90-47.3, Appendix K, requires complete System Security Plans, Risk Assessments, Security Control Assessments, and POA&Ms.

System Security Plans were Not Updated

Five of ten systems sampled during the FISMA review did not have adequate and up-to-date System Security Plans. This included describing how baseline security controls were implemented and for four systems adequately and completely describing system boundaries. The SBA SOP 90-47.3, Chapter 12, Section 2 requires that System Security Plans be reviewed annually and updated to address changes to the information system.

Annual Risk Assessments were Not Updated

Eight of ten systems sampled during the FISMA review did not have annual risk assessments updated as required. The SBA SOP 90-47.3, Chapter 14, Section 3 – Risk Assessment requires that Risk Assessments are updated annually or more often if major changes occur to the system.

Recommendation 2

We recommend that the Chief Information Officer in conjunction with other program offices improve the quality of Security Authorization Packages for SBA systems and ensure that all required documentation is included in all authorization packages. This includes:

a. Require that Risk Assessments are updated yearly for all general support systems and major applications.
b. Ensure that Systems Security Plans are timely and accurately completed for all relevant general support systems and major applications.
c. Ensure that Security Assessment Reports are timely and accurately completed for all relevant general support systems and major applications.
d. Create Plans of Actions and Milestones (POA&M) for all general support systems and major applications when vulnerabilities are identified during Security Control Assessments or other evaluations. Additionally, enter the vulnerabilities identified during review into the Cyber Security Assessment and Management Tool (CSAM).

4) Continuous Monitoring Controls

The SBA received an overall assessment that it had not established a Continuous Monitoring Controls program that is consistent with FISMA reporting areas in the Cyberscope evaluation. The SBA did not update Security Assessments as part of continuous monitoring controls for seven of ten sampled systems in the FISMA evaluation for FY 2013. This indicates that the SBA has not fully implemented ongoing Security Control Assessments as part of Continuous Monitoring.

SBA SOP 90-47.3, Chapter 4, Section 2 – Security Assessment requires an annual assessment for all systems not undergoing the authorization process. SBA system owners are required to test a third of all controls and enhancements using a NIST 800-53 based assessment process.

5) Plans of Actions and Milestones

The SBA received an overall assessment that it had established a Plan of Actions and Milestones (POA&M) program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted two areas of improvement which needs to be implemented to be consistent with FISMA reporting areas in the Cyberscope evaluation.

Plans of Actions and Milestones Not Always Developed

The SBA had four of six systems sampled with POA&Ms which had not been developed and entered into the SBA Cyber Security Assessment and Management (CSAM) tool. The SBA SOP 90-47.3, Chapter 4, Section 4, POA&M requires that all SBA FISMA information systems must develop, update, and maintain a POA&M using an SBA provided tracking tool. The POA&M must document the planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

POAM Remediation Costs were Not Adequately Estimated for Vulnerabilities

The SBA had 180 of 236 weaknesses identified in the CSAM tool with either $0 or $1 as the remediation cost to correct the weaknesses. We conclude that this lack of adequate cost estimation prevents the SBA from adequately ensuring that resources and ownership are aware of the severity of IT weaknesses. The SBA SOP 90-47.3, Appendix J requires in the Procedures section (d) that the cost of remediation activities must be determined and included in POA&Ms.

Recommendation 3

We recommend that the Chief Information Officer in conjunction with other program offices identify estimated costs to correct POA&M vulnerabilities entered into CSAM so that SBA has an understanding of the price of mediation of its security vulnerabilities.

6) Remote Access Management

The SBA received an overall assessment that it had established a Remote Access Management program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted two areas of improvement which need to be implemented to be consistent with FISMA reporting areas in the Cyberscope evaluation.

Remote Access does Not Meet Encryption Standards

The SBA's remote access solution is not set to meet existing Federal encryption standards. The SBA SOP 90-47.3, Chapter 16, Section 11, Use of Cryptography requires that information systems in use at SBA shall use FIPS-approved security functions and NIST FIPS validated implementations for all cryptographic functions.

Remote Access does not automatically time-out after inactivity

The SBA's remote access solution does not automatically time-out after 30 minutes of inactivity. The SBA SOP 90-47.3, Chapter 1, Section 12, Remote Access requires that remote access sessions will be automatically disconnected upon logout or session inactivity lasting longer than 30 minutes.

Recommendations 4 & 5

We recommend that the Chief Information Officer upgrade SBA's remote access solution to:

- Fully incorporate required encryption standards.
- Time-out after 30 minutes of inactivity.

7) Security Training

The SBA received an overall assessment that it had established a Security Training program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted one area of improvement which needs to be implemented to be consistent with FISMA reporting areas in the Cyberscope evaluation.

Specialized Security Training

The SBA's specialized security training program was not fully effective. We identified that 58 of 372 personnel with specialized security positions had not taken specialized security training. This amounted to a non-compliance rate of 15.6%. The SBA SOP 90-47.3, Chapter 2, Section 3, Security Training requires that personnel with significant IT security duties be provided security training before authorizing access to the system or performing assigned duties, when required by system changes, and annually.

Recommendation 6

We recommend that the Chief Information Officer require that personnel with specialized security positions within the Agency take the enhanced security training to ensure that those personnel are adequately trained to perform their duties.

8) Computer Security Incidents

The SBA received an overall assessment that it had established a Computer Security Incidents program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted the SBA has an open audit recommendation from a prior year financial statement audit to implement a Security Incident SOP. A Security Incident SOP is needed to formalize incident response procedures for the Agency.

9) Contingency Planning

The SBA received an overall assessment that it had established a Contingency Planning program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted that the SBA does not have an alternate recovery site for one general support system and two major applications reviewed. The SBA general support system supports major applications which are critical to the continued successful operation of the SBA. This includes applications which support the 7a, and 504 loan programs.

10) Contractor Systems

The SBA received an overall assessment that it had established a Contractor Systems program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, the SBA still needs to successfully perform Security Control Assessments for all contractor-operated systems, and complete establishing of Interconnection Security Agreements for all interconnections.

11) Security Capital Planning

The SBA received an overall assessment that it had established a Security Capital Planning program that is consistent with FISMA reporting areas in the Cyberscope evaluation. However, we noted two areas of improvement which needs to be implemented to be consistent with FISMA reporting areas in the Cyberscope evaluation.

Assigning Security Responsibilities and Reporting Security Costs

The SBA needs to fully identify staffing responsible for IT security and fully allocate security costs for remediating vulnerabilities. The SBA Exhibit 53[2] for FY 2014 only identified security costs for OCIO IT-Security. The SBA's offices which oversee and operate its mission critical systems do not designate or assign personnel for IT security for their major applications. At a minimum, the Office of Capital Access, the Office of Chief Financial Officer, and the Office of Disaster Assistance; should have personnel specifically assigned to security duties within their respective offices due to the importance of the systems to the SBA.

Moreover, as previously identified in the POA&M section, the SBA had 180 of 236 weaknesses identified in the CSAM tool with either $0 or $1 as the remediation cost to correct the weaknesses. This lack of identifying the cost of IT security weaknesses understates the amount actually spent on IT security.

The SBA SOP 90-47.3 Chapter 15, Section 2 – Allocation of resources requires that the SBA define security requirements in information system mission/business planning; establish a discrete budget line item for information system security; and integrate information security into the capital planning and investment control process.

Recommendation 7

We recommend the Chief Information Officer to work with other SBA Offices to assign personnel with significant security duties as IT-Security resource expenditures.

Agency Comments and OIG Response

On March 18, 2014, we provided a DRAFT copy of this report to the Chief Information Officer for comment. On April 22, 2014, the Agency submitted formal comments, which are included in their entirety in Appendix III.

The Chief Information Officer carefully reviewed the draft and agreed with all findings and recommendations. The Chief Information Officer provided a specific action plan with target dates for final actions for each recommendation identified in this report. The specific action plan and target dates were specified in the *Recommendation Action Sheet SBA/OIG Follow-up System* (SBA Form 1824). Management's comments were responsive to our seven recommendations listed in this report. We consider these seven recommendations resolved but open pending completion of final actions.

[2] The Exhibit 53 is composed of two parts: Exhibit 53A, "Agency IT Investment Portfolio," which includes IT investment budget and architecture information, and Exhibit 53B, "Agency IT Security Portfolio," which includes a summary of agency and bureau IT security information, including IT security costs.

Appendix I: Scope and Methodology

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' 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 to develop standards and guidelines for implementing its requirements in coordination with the OMB.

On November 18, 2013, OMB issued Memorandum 14-04, *Fiscal Year 2013 Reporting Instruction for the Federal Information Security Management Act and Agency Privacy Management;* providing instructions for agencies to meet their FY 2013 reporting requirements under FISMA. This memorandum requires IGs to answer a set of information security questions in Cyberscope that evaluates agency implementation of security capabilities and measures their effectiveness.

To determine SBA's compliance in these areas, the OIG contracted with Independent Public Accountant (IPA), KPMG, to perform review procedures relating to FISMA. The IPA interviewed SBA personnel, inspected documentation, and tested the effectiveness of SBA's IT security controls. The OIG monitored the IPA's work and reported the SBA's compliance with FISMA with the Agency FISMA filings in December, 2013.

Prior Coverage

Small Business Administration-Office of Inspector General Reports

Report 13-15, *Briefing Report for the FY 2012 Federal Information Security Management Act* Review, issued March 29, 2013.

Report 14-01, *Report on the Most Serious Management and Performance Challenges Facing the Small Business Administration in Fiscal Year 2014,* issued October 31, 2013.

Appendix II: Open Current and Prior Year IT Security Recommendations Relating to FISMA

Appendix II identifies the open FISMA related recommendations. There are 17 open prior-year audit recommendations which directly affect SBA's Cyberscope evaluation as it relates to FISMA compliance. The seven recommendations listed above along with the 17 prior-year open audit recommendations represent SBA's current FISMA condition.

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.

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

- Develop and document baseline configurations for each information system and maintain the baseline under configuration control. OIG Report 11-06, Recommendation 5, Closure was due 9/30/2011.

- Develop and maintain a centralized inventory of all agency hardware and software. OIG Report 11-06, Recommendation 4, 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. OIG Report 12-02, Recommendation 14, Closure was 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. OIG Report 12-02, Recommendation 13, Closure was due 4/30/2011.

- Enhance security vulnerability management process. Specifically, (a) ensure that servers, operating systems, and databases are properly configured and updated on a routine basis; (b) monitor SBA vulnerability reports for required patches; (c) update systems based upon risk determination and threats. OIG Report 13-04, Recommendation 1, Closure was due 3/31/2014.

- 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. OIG Report 12-02, Recommendation 1, Closure was due 3/31/2012.

- Enforce a network access security baseline(s) across the network consistent with SBA security policy, Office of Management and Budget directives, and United States Government Configuration Baseline requirements. OIG Report 14-04, Recommendation 7, implementation date not established.

- Address the vulnerabilities noted during the FY 2013 audit consistent with SBA policy and SBA Vulnerability Assessment Team (VAT), Internal Operating Procedures, Version 1.4 and implement procedures to ensure the consistent identification, tracking, and resolution of security vulnerabilities across SBA's workstations, servers, databases, network devices, and other security relevant appliances. OIG Report 14-04, Recommendation 12, implementation date not established.

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. OIG Report 12-02, Recommendation 3, recommendation was closed after issuance of Cyberscope Report.

- Implement port-based network access controls across the SBA network. OIG Report 14-04, Recommendation 11, recommendation was closed after issuance of Cyberscope Report.

- 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. OIG Report 13-04, Recommendation 12, Closure was due 3/1/2014.

- Develop and implement procedures for user access termination to ensure access for terminated or transferred personnel is removed from systems in a timely manner. OIG Report 13-04, Recommendation 7, Closure was due 2/20/2013.

- Improve SBA's administration of logical system access by taking the following actions: (1) Implement an effective off-boarding process and verify periodically that controls to remove logical access for separated employees from SBA systems are implemented and operating as designed; (2) Establish a process for the identification and removal of separated contractors in order to help ensure that access is timely removed upon contractor separation; (3) Remove access to the general support systems and major applications (including development and test environments) timely when terminated employees and contractors are identified. OIG Report 14-04, Recommendation 4, implementation date not established.

- Grant elevated network privileges per business needs only and enforce the concept of least privilege or implement mitigating controls to ensure that activities performed using privileged network accounts (including service accounts) are properly monitored. OIG Report 14-04, Recommendation 13, implementation date not established.

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

- Coordinate with SBA program offices to fully implement the SBA entity wide incident management and response program and ensure that procedures are enforced. OIG Report 12-02, Recommendation 5, Closure was due 2/29/2012.

- Finalize, implement and monitor its entity-wide Incident Response Policy or Standard Operating Procedure. OIG Report 14-04, Recommendation 9, implementation date not established.

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. OIG Report 11-06, Recommendation 9, recommendation was closed after issuance of Cyberscope Report.

- Enforce existing SBA policies to rotate backups off-site. OIG Report 12-02, Recommendation 15, Closure was due 4/30/12.

- Coordinate with the CFO to create, implement, and test system specific and the HQ COOP. OIG Report 12-02, Recommendation 16, recommendation was closed after issuance of Cyberscope Report.

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

- The Office of Human Resource Solutions in conjunction with the Office of Chief Information Officer issue a new Telework SOP. OIG Report 13-15, Recommendation 1, recommendation was closed after issuance of Cyberscope Report.

- Continuously monitor remote access audit logs for potential unauthorized activity. OIG Report 12-15, Recommendation 4, Closure was due 12/30/2012.

- Improve SBA's remote access program by taking the following actions: (1) Incorporate security requirements into the Teleworking SOP consistent with NIST 800-46 Rev.; (2) Ensure employees acknowledge compliance with security requirements prior to establishing a remote connection to the SBA network when Teleworking or otherwise connecting remotely to a SBA system; and (3) Monitor compliance with the revised SOP 90.47.3 and the updated Teleworking SOP. OIG Report 14-04, Recommendation 14, implementation date not established.

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

- 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. OIG Report 11-06, Recommendation 1, 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. OIG Report 11-06, Recommendation 2, Closure was due 9/30/2011.

Appendix III: Agency Comments

U.S. SMALL BUSINESS ADMINISTRATION

WASHINGTON, D.C. 20416

Date: April 22, 2014

To: Robert A. Westbrooks
Deputy Inspector General

From: /s/ Renee A. Macklin
SBA Chief Information Officer

Subject: Response: Fiscal Year 2013 Federal Information Security Management Act (FISMA) Report

Thank You for the opportunity to respond on the draft report entitled, "Weaknesses Identified during the FY 2013 Federal Information Security Management Act Review." We have carefully reviewed the draft and agree with all findings and recommendations. Please refer to the attachments for further details on our planned corrective actions.

The Office of Chief Information Officer remains committed to improving its cyber security program. We appreciate your audit recommendations because they will help improve our security posture. If you have any questions, please contact Ja'Nelle L. Devore, Chief Information Security Officer, at (202) 205-7103.

Attachment

Cc: Ja'Nelle L. DeVore