Office of Inspector General

Small Business Administration

FY 2012 FISMA Review

Briefing Report

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

REPORT TRANSMITTAL
REPORT NO. 13-15

DATE: March 29, 2013

TO: Chase Garwood
Acting Chief Information Officer

Bridget Bean
Acting Chief Human Capital Officer

SUBJECT: Briefing Report for the FY 2012 Federal Information Security Management Act Review

This report presents the results of the SBA Federal Information Security Management Act (FISMA) review. This review assessed SBA's compliance with FISMA and was previously reported to the Department of Homeland Security through the Cyberscope reporting process. We have incorporated the comments from the Chief Information Officer and Chief Human Capital Officer into this report.

Please provide your response to this report for the recommendation on the attached SBA Form 1824, Recommendation Action Sheet, by April 28, 2013.

Consistent with OMB Circular A-50, your response should include the corrective action taken or planned for the recommendation and the target date for completion. If you disagree with the recommendation, please fully explain the reasons for disagreement. Please include the legal basis for disagreement based on interpretation of law, regulations, or the authority of officials to take or not take action. You may also propose alternative actions to those recommended that you believe would better address the issues presented in this report.

In order to fulfill our responsibilities under the Inspector General Act, we are providing copies of our report to the appropriate congressional committees responsible for oversight of the Small Business Administration. We will also post this report on the Office of Inspector General website for public dissemination.

We appreciate the courtesies and cooperation of the Office of Chief Information Officer and Office of Human Capital during this review. If you have any questions concerning this report, please call me at (202) 205-7390 or Jeffrey Brindle, Director, Information Technology and Financial Management at (202) 205-7490.

***

/s/

John K. Needham
Assistant Inspector General for Auditing

FY 2012 FISMA Review

Highlights

Why the OIG Performed this Review

The Federal Information Security Management Act (FISMA) requires that the OIG review the SBA's Information Technology (IT) Security Program.

The OIG is required to provide the results of the IT Security review to the Department of Homeland Security through the CyberScope reporting process.

What the OIG Found

The SBA made progress in meeting FISMA requirements, as outlined in OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for FISMA and Agency Privacy Management*. Some of the specific FISMA results included:

- Improvements in the Incident Response, and Risk Management areas.
- Performance in security capital planning continues to comply.

The OIG also determined that the SBA:

- Needs to make significant improvement to meet FISMA criteria in Configuration Management.
- Telework Standard Operating Procedure is more than ten years old and does not reflect current technically guidance.
- Has 36 open IT recommendations that directly impacts the security of SBA IT systems.

Note: This represents a net increase of six recommendations over last year's FISMA report.

Status of FISMA Compliance Areas at the End of FY 2012

Continuous Monitoring	⊡
Configuration Management	■
Identity Management	◘
Incident Response	☑↑
Risk Management	☑↑
Security Training	⊡
POA&M	◘
Remote Access	⊡
Contingency Planning	◘
Contractor Systems	⊡
Security Capital Planning	☑

☑ *Fully Met* ⊡ *Mostly met* ◘ *Partially met* ■ *Not met*

Recommendations

The OIG found that the SBA continues to show improvement in its IT Security Program. The OIG recommended the SBA needs to update its Telework Standard Operations Procedural manual.

The SBA concurred with this recommendation in its formal comments to the OIG.

Table of Contents

FY 2012 FISMA Review

Background

The Federal Information Security Management Act (FISMA) of 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.

The Office of Management and Budget (OMB) issued Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management,* for agencies to assess compliance with FISMA reporting requirements. Further, Inspectors General are required by FISMA to perform an annual evaluation to determine the effectiveness of the agency's information security program and practices, which includes:

- An assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines to include applicable National Institute for Standards and Technology (NIST) guidelines.
- Testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency's information systems.
- Vetting of the OIG's results through the Office of the Chief Information Officer (OCIO), and reporting them to the Office of Management and Budget and the Department of Homeland Security. This information is used in OMB's report to Congress, its preparation of the President's Budget, and in support of DHS's oversight of government information systems.

Approach

Objective

The objective of this review was to evaluate the SBA's progress during FY 2012 in adhering to criteria established in FISMA.

Scope and Methodology

We performed our review in accordance with *Quality Standards for Inspections and Evaluations* issued by the Council of Inspectors Generals on Integrity and Efficiency (CIGIE).

In doing this work we:

- Contracted with an Independent Public Accountant (IPA) to perform fieldwork regarding the evaluation procedures relating to FISMA.
- Utilized the IPA's work to evaluate SBA's performance in the eleven cyber security areas identified in the Cyberscope[1] reporting tool.
- Formulated our conclusions based on FISMA guidance and OMB Circular A-130, Management of Federal Resources.

This evaluation covered the fiscal year ending September 30, 2012.

To report on SBA's progress, we assigned a grade to each FISMA reporting area.

We considered compliance with Cyberscope reporting criteria and open recommendations when assigning a grade to each area. Grades for FY 2012 take into consideration progress made since FY 2011.

[1] The Cyberscope reporting tool is the secure platform for reporting security metrics to the Department of Homeland Security.

Key Issues

Configuration Management

The SBA continues to be severely impacted by its lack of progress in mitigating or correcting serious IT security weaknesses in the area of Configuration Management.

The SBA has seven high-priority open audit recommendations in Configuration Management dating back to January 2010.

- Implementation of these seven recommendations would reduce the risk to SBA's IT environment from exploitation or penetration.

Upon review of the results of SBA's 2012 Cyberscope Report, the OIG determined that the SBA did not have a fully operational Configuration Management program.

The OIG concluded that SBA's negative responses to nine of ten Configuration Management questions in the Cyberscope report identify SBA's inability to make improvements in its Configuration Management program over the long-term under FISMA criteria.

Telecommuting Program SOP

The SBA Standard Operating Procedure (SOP) "Telecommuting Program" (33.59.1) contains technical procedures for telework that are over 10 years old and are obsolete.

- According to SOP (90.47.3) "Information Security Program – Personnel Security Policies and Procedures" – Personnel security policies help protect SBA assets from abuse, misuse, or destruction. Personnel security involves human users and how they interact with computers, access and the authorities they need to do their job.

The SOP 33.59.1 refers to using "direct dial-up" with the employees private internet account. Additionally, the SOP calls for the installation of a software tool — Virtual Network Computing— to be installed on the SBA employee's personal computer. We conclude that these procedures are obsolete and have not been used in years. The SBA should update its procedures in the SOP 33.59.1 or refer to them by reference.

Recommendation

We recommend the *Office of Human Resource Solutions, in conjunction with the Office of Chief Information Officer,* issue a new Telework Program SOP.

- This new Telework SOP would refer to technical sections for explaining the safe and secure methods of telework. The technical sections could be referred to by reference and not be placed in the actual Telework SOP. This would allow timely changes to technical procedures.

.

Continuing Issues

36 Open Recommendations

Open Recommendations Increased

From FY 2011 to FY 2012, the SBA's Information Technology (IT) open recommendations in FISMA reporting areas increased from 30 open recommendations to 36 open recommendations.

- The 36 open audit recommendations represent long-standing security vulnerabilities in SBA's IT Security Program.
- Over half of open recommendations were in the areas of Configuration Management and Identity and Access Management.

OIG Assessment

SBA fully meets OMB requirements in three of the 11 FISMA Compliance Areas.

Areas of Improvement

The SBA was compliant in Security Capital Planning and became compliant in two areas in the past year:

- Incident Response
- Risk Management

Area of Significant Weakness

However, the SBA is severely impacted by continued open recommendations and weaknesses in Configuration Management.

This weakness put SBA's IT Security Program at risk of unauthorized access, modification, and possible penetration of SBA systems.

Each of the areas evaluated on the following page correspond to their relative FISMA requirements, as prescribed by the DHS and reported in Cyberscope, and open recommendations.

FISMA Compliance Areas

1. **Continuous Monitoring**: Provides a real-time view of agency security control operations.
2. **Configuration Management**: Provides a standard configuration baseline that minimizes exploitable system vulnerabilities.
3. **Identity Management**: Ensures that users and devices are properly authorized to access information or information systems.
4. **Incident Response**: Ensures that agencies have sound policies and planning in place to respond to incidents and report them to the appropriate authorities.
5. **Risk Management**: Provides a framework for the agency to identify, assess, and mitigate systems' risks.
6. **Security Training**: Ensures that security awareness training is provided for all employees and specialized training is provided for those with significant security responsibilities.
7. **POA&M**: Provides the agency with information on a security weakness's overall risk to the system, planned actions to address the risk, associated costs, and expected completion dates.
8. **Remote Access**: Allows the agency to provide secure access to information and information systems remotely to include telework and mobile devices.
9. **Contingency Planning:** Identifies important agency resources and potential risks to those resources. Includes development of a plan to address the consequences if those risks are realized.
10. **Contractor Systems**: Ensures that external entities that own or operate information systems on behalf of the government meet the security requirements for all systems that store or process government information.
11. **Security Capital Planning**: Ensures that security requirements are identified, resources estimated, and business cases established so that appropriate levels of security are funded.

Summary of FISMA Compliance Areas

Area of Compliance	Status at end of FY 2011	Status at end of FY 2012
1. Continuous Monitoring: Provides a real-time view of agency security control operations.	⊡	⊡
2. Configuration Management: Provides a standard configuration baseline that minimizes exploitable system vulnerabilities.	■	■
3. Identity Management: Ensures that users and devices are properly authorized to access information or information systems.	◘	◘
4. Incident Response: Ensures that agencies have sound policies and planning in place to respond to incidents and report them to the appropriate authorities.	⊡	☑↑
5. Risk Management: Provides a framework for the agency to identify, assess, and mitigate systems' risks.	⊡	☑↑
6. Security Training: Ensures that security awareness training is provided for all employees and specialized training is provided for those with significant security responsibilities.	⊡	⊡
7. POA&M: Provides the agency with information on a security weakness's overall risk to the system, planned actions to address the risk, associated costs, and expected completion dates.	◘	◘
8. Remote Access: Allows the agency to provide secure access to information and information systems remotely to include telework and mobile devices.	⊡	⊡
9. Contingency Planning: Identifies important agency resources and potential risks to those resources. Includes development of a plan to address the consequences if those risks are realized.	◘	◘
10. Contractor Systems: Ensures that external entities that own or operate information systems on behalf of the government meet the security requirements for all systems that store or process government information.	⊡	⊡
11. Security Capital Planning: Ensures that security requirements are identified, resources estimated, and business cases established so that appropriate levels of security are funded.	☑	☑

FISMA Requirements: ☑ *Fully Met* ⊡ *Mostly met* ◘ *Partially met* ■ *Not met*

Agency Comments: Recommendation 1

We provided a draft of this report to the SBA Chief Information Officer (CIO) dated March 4, 2013. On March 26, 2013, the CIO submitted formal comments and concurred with the recommendation. A summary of management's comments, followed by our responses are below.

Recommendation 1

We recommend the Office of Human Resource Solutions, in conjunction with the Office of Chief Information Officer, issue a new Telework Program SOP.

- *This new Telework SOP would refer to technical sections for explaining the safe and secure methods of telework. The technical sections could be referred to by reference and not be placed in the actual Telework SOP. This would allow timely changes to technical procedures.*

Agency Comments: The Office of Human Resource Solutions (OHRS) and Office of Chief Information Officer (OCIO) concur.

OIG Response: We consider management's comments to be responsive to the recommendation.

***