EVALUATION OF THE SMALL BUSINESS ADMINISTRATION'S INFORMATION SECURITY PROGRAM

Report Number: 07-14
Date Issued: February 22, 2007

Memorandum

U.S. Small Business Administration
Office of Inspector General

To: Christine Liu
Chief Information Officer
[Exemption 6]

Date: February 22, 2007

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Advisory Memorandum Report on SBA's Information Security Program

This report presents the results of our fiscal year (FY) 2006 evaluation of the Small Business Administration's (SBA) information security program. The Federal Information Security Management Act (FISMA) requires the Office of Inspector General (OIG) to annually assess SBA's progress in correcting weaknesses identified in last year's FISMA review and to provide input on SBA's annual FISMA report in accordance with specific reporting instructions issued by the Office of Management and Budget (OMB). Reporting instructions for FY 2006 were provided in OMB Memorandum 06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

Our input into SBA's annual FISMA report, which was submitted to OMB in October 2006, is attached in Appendix III. This input was based on tests of 11 of SBA's 19 major systems. Three of these systems were reviewed by different Independent Public Accountants using Statements of Auditing Standards (SAS) 70, Type II auditing procedures. Eight of these systems were reviewed by our Independent Public Accountants, KPMG, in accordance with the Federal Information Systems Control Audit Manual. We utilized reviews of these 11 systems along with our own reviews of SBA security documentation to come to our conclusions of SBA's information security program.

We also attempted, but were unable, to review SBA's 82 non-major systems for compliance with the certification and accreditation (C&A) provisions of FISMA.

SBA had not classified the sensitivity of information in 80 of its 82 non-major systems to determine which systems should be certified and accredited. A more detailed discussion of our scope and methodology is in Appendix I.

SBA reviewed a draft of this report and concurred with the findings and recommendations. SBA's full response is included in Appendix I of this report.

RESULTS

During FY 2006 SBA made a concerted effort to correct weaknesses identified in previous FISMA reviews. Consequently, only four recommendations remain unresolved. Of these, two involve corrective actions targeted for June 30, 2006, which are past due. SBA has not fully incorporated continuous monitoring of major applications and general support systems into its C&A requirements nor has it required that configuration management plans be included in C&A packages for all of its systems. Actions on the two remaining recommendations are to be completed in calendar year 2007. Our assessment of SBA's progress in correcting weaknesses previously identified is summarized in Appendix IV.

SBA has also made improvements in its Computer Security Program. In FY 2006, SBA fully certified and accredited 9 of the 11 systems we evaluated. The two remaining systems had interim C&As. SBA also met FISMA requirements for managing an agency-wide plan of action and milestone process to track its progress in addressing IT security weaknesses, establishing agency-wide security configuration policy and guidelines, reporting security incidents, and providing security awareness training.

Despite this progress, SBA still needs to improve its program in two areas—classifying the sensitivity of its non-major systems and ensuring that contingency plans for all contractor-operated systems are tested. FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems,* requires that all information and information systems be categorized by an appropriate risk level to ensure an appropriate level of information security. However, SBA had not classified the sensitivity of information in 80 of its 82 non-major systems to determine which systems should be certified and accredited. Consequently, we were unable to assess the adequacy of security protection for these systems.

SBA also did not ensure that three of seven disaster recovery plans for its major contractor-operated systems were tested. NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems,* and OMB Memorandum 06-20 require agencies to develop system disaster recovery plans and restoration procedures, which would recover SBA's systems based upon the business impact

to the agency. However, SBA did not have documentation to show that disaster recovery plans had been tested in FY 2006 for the:

- Business Development Management System
- Contract 7(a)/503/504 Loan Servicing System; and
- Loan/Lender Monitoring System.

Because these plans have not been tested, SBA has no assurance that they could be restored in the event of emergencies according to time frames specified in SBA's business impact analyses. SBA needs to either modify existing contract language or related service-level agreements to ensure that all of its major contractor-operated systems are annually tested for disaster recovery and that test results are documented.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Classify the FIPS 199 risk level for all non-major information systems identified in SBA's systems inventory and document these classifications in its inventory accordingly.

2. Certify and accredit all low-, moderate-, and high-impact non-major systems in accordance with FISMA requirements.

3. Ensure that current contracts or service-level agreements are modified to require that disaster recovery plans for all SBA contractor-operated systems are annually tested and the test results documented.

AGENCY COMMENTS

The Agency provided written comments on a draft of this report concurring with all findings and recommendations in the draft report. SBA's comments are summarized in the Results in Brief section, and the full text of the comments can be found in Appendix I to this report.

APPENDIX I. SCOPE AND METHODOLOGY

We performed an independent evaluation of SBA's information security program for the period, August 16, 2005, to August 15, 2006 to reach conclusions about the adequacy of the FISMA reporting areas. Our evaluation was performed in accordance with instructions provided in the Office of Management and Budget Memorandum 06-20, *FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.*

Our evaluation included tests of 11 of SBA's 19 major systems. Three of these systems were reviewed by different Independent Public Accountants using Statements of Auditing Standards (SAS) 70, Type II auditing procedures. Eight of these systems were reviewed by our Independent Public Accountants, KPMG, in accordance with the Federal Information Systems Control Audit Manual. In addition, for each major system tested we reviewed program documentation to determine whether each system maintained a valid certification and accreditation and had a tested disaster contingency plan for the fiscal year. Our findings were confirmed in discussions with SBA officials.

We also attempted, but were unable, to review SBA's 82 non-major systems for compliance with certification and accreditation provisions. SBA did not have adequate documentation to make valid conclusions. We also considered prior audits related to SBA's information systems computer security program issued by our office in fiscal year 2006.

Our evaluation was performed at SBA's headquarters office in Washington, D.C. from May 2006 through October 2006.

APPENDIX II. MANAGEMENT COMMENTS

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

Date: January 25, 2007

To: Debra S. Ritt
Assistant Inspector General for Auditing

From: Christine H. Liu [Exemption 6]
Chief Information Officer
Chief Privacy Officer

Subject: OCIO's Response to Draft Advisory Memorandum Report on SBA's Information Security Program

Please find attached OCIO's response to the recommendations addressed in the above report. If you require additional information, please contact me at (202) 205- [Exemption 2]

Attachment

cc: Jovita Carranza
Deputy Administrator

Response to Office of Inspector General's Audit Report on the Evaluation of the Small Business Administration's Information Security Program (Project No. 6028):

OIG's Recommendations

1. **Classify the FIPs 199 risk level for all non-major information systems identified in SBA's systems inventory and document these classifications in its inventory accordingly. (Agree)**

   OCIO's Response:
   OCIO's IT Security Office developed a Minor Application Certification process that includes the classification process using FIPS199 guidance. All systems/applications in the SBA inventory will be classified according to FIPS 199.
   To date, 60 systems have been rolled into a major application system or a general support system; 7 outsourced systems/applications are in the C&A process; 10 applications have been retired; and 5 outsourced systems are in the development phase. The target completion date is June 30, 2007.

2. **Certify and accredit all low-, moderate-, and high-impact non-major systems in accordance with FISMA requirements. (Agree)**

   OCIO's Response:
   (See Response to No. 1 above)

3. **Ensure that current contracts or service-level agreements are modified to require that disaster recovery plans for all SBA contractor-operated systems are annually tested and test results documented. (Agree)**

   OCIO's- Response:
   OCIO will meet with the Office of Administration to ensure that all existing contracts and service level agreements are modified to include boiler plate language requiring annual testing of all disaster recovery plans for SBA contractor-operated systems and documentation of test results. In addition, OCIO's IT Security Office will develop a method to track compliance with this new requirement. The target completion date is September 30, 2007.

Redaction Marker

Number of Withheld Pages	**7**
FOIA or PA Exemption(s)	**2**
Description	**Appendix III - FISMA Reporting Template**

Redaction Marker

Number of Withheld Pages	**2**
FOIA or PA Exemption(s)	**2**
Description	**Appendix IV – Open FISMA prior Year Recommendations**

APPENDIX V. REPORT DISTRIBUTION

Recipient	No. of Copies
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	3
Office of Management and Budget	1
U.S. Government Accountability Office	1