INDEPENDENT EVALUATION OF

SBA'S INFORMATION SECURITY PROGRAM

REPORT NUMBER 5-02

OCTOBER 7, 2004

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416

ADVISORY MEMORANDUM REPORT
Issue Date: October 7, 2004
Number: 5-02

To: Hector V. Barreto
Administrator

Stephen D. Galvan
Chief Operating Officer / Chief Information Officer

/s/
From: Robert G. Seabrooks
Assistant Inspector General for Audit

Subject: Independent Evaluation of SBA's Information Security Program

The Federal Information Security Management Act (FISMA) requires the Office of Inspector General (OIG) to perform an independent evaluation of the Small Business Administration's (SBA) information security program. This report presents the results of that evaluation in accordance with specific FISMA reporting instructions issued by the Office of Management and Budget (OMB).

OBJECTIVES, SCOPE AND METHODOLOGY

The objective of our review was to evaluate SBA's information security program in accordance with FISMA reporting requirements specified in OMB Memorandum M-04-25. We performed an independent evaluation of SBA's information security program to reach conclusions about the FISMA reporting areas. In making our evaluation, we considered prior audits related to SBA's information systems computer security program issued by our office.

Our assessment covered the 37 high-priority systems identified by SBA and its characterization of the susceptibility of those systems to unauthorized access as of September 15, 2004. OMB Memorandum M-04-25 identified that we were to report significant deficiencies in SBA's overall information systems security program or management structure. A significant deficiency under FISMA is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information,

information systems, personnel, or other resources, operations, or assets. A significant deficiency is to be reported by the Agency as a material weakness under the Federal Managers Financial Integrity Act (FMFIA) report.

We interviewed SBA officials and reviewed documentation on SBA's information security program. Our evaluation was performed at SBA's headquarters office in Washington, D.C. from April 2004 through October 2004.

OVERALL EVALUATION

Generally for FY 2004, the SBA's computer security program has shown mixed results. SBA achieved a major milestone in certifying and accrediting all of its major systems within the past fiscal year. However, SBA has not been able to sufficiently address the 248 open system risk assessment vulnerabilities and open OIG audit findings including 118 open risk assessment vulnerabilities and 14 OIG audit findings which have exceeded their estimated target date for completion to correct the issues identified.

The OIG identified five (5) significant deficiencies in SBA's computer security program. Moreover, these deficiencies were previously identified in 11 OIG recommendations, which if adopted in full, would address related security risks and exposures.

Finding 1: Computer Security Capital Planning is not FISMA Compliant

SBA does not have a capital planning process that is compliant with FISMA requirements from either a budgeting or an actual expenditure tracking capability. This occurred because SBA's capital planning process does not tie to or reconcile with the SBA Plan of Actions & Milestones (POA&M), the SBA Exhibit 53, and SBA Capital Asset Plans. Additionally, there is no expenditure tracking of security related costs in SBA's accounting system. As a result, SBA cannot be assured that those funds identified in the POA&M, requested in the Capital Asset Plans and Exhibit 53 for remediating security vulnerabilities is actually appropriated and spent for correcting security vulnerabilities in SBA systems.

According to OMB Memorandum 04-25, the POA&M identifies the resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of a POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems. The Agency POA&M must be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.

We reviewed the SBA POA&M as of 9/15/04 with the separate SBA Capital Asset Plans, and Exhibit 53. We could not reconcile or tie either the individual system

POA&M to the SBA Capital Asset Plans and SBA Exhibit 53 for specific relevant systems. Additionally, we could not reconcile or tie the "steady-state" SBA system POA&M's with the "meta" SBA Capital Asset Plan and Exhibit 53 for all SBA systems that are not in a development status. Finally, there was no specific project cost capabilities set-up within SBA's accounting system to track specific security expenditures relating to SBA systems so that their security control costs would be integrated into the life-cycle of SBA systems.

The SBA Joint Accounting and Administrative Management System (JAAMS) are reported here as an example:

	POA&M Amount Spent or Planned for Security	Exhibit 53 (5% of cost allocation)	Capital Asset Plan – 300B (5% of cost allocation)	Amount spent as recorded in SBA's accounting system
FY2004	$0	$64,150	$64,150	$0
FY2005	$56,000	$41,300	$41,250	

Recommendations: We recommend that the Chief Operating Officer in conjunction with the Office of Chief Financial Officer:

1.A. Ensure that system and program level SBA Plan of Action & Milestones (POA&M) tie or reconcile resources needed to correct system vulnerabilities to the SBA Capital Asset Plans (300B) and Exhibit 53.

1.B Create costing or charge-back capabilities within SBA's accounting system to track security related expenditures for SBA's system and program level Plans of Actions and Milestones (POA&M).

* * *

The OIG FISMA report is attached in the format prescribed and utilizing a template file which was provided by OMB.

The findings included in this report are the conclusions of the Auditing Division. The findings and recommendations are subject to review and implementation of corrective action by your office following the existing Agency procedures for audit follow-up and resolution.

Please provide us your management decision for each recommendation within 30 days. Your management decisions should be recorded on the attached SBA Forms 1824, Recommendation Action Sheet," and show either your proposed corrective action or target date for completion, or explanation of your disagreement with our recommendations.

Should you or your staff have any questions, please contact Jeffrey R. Brindle, Director, IT and Financial Management Group at (202) 205-7490.

Attachment

Withheld from public release: 17 pages of technical information.

Rationale: FOIA Exemption 2

ATTACHMENT A

REPORT DISTRIBUTION

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