INDEPENDENT EVALUATION OF

SBA'S INFORMATION SECURITY PROGRAM

REPORT NUMBER 06-01

OCTOBER 7, 2005

This report may contain proprietary information subject to the provisions of 18 USC 1905 and must not be released to the public or another agency without permission of the Office of Inspector General.

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

ADVISORY MEMORANDUM REPORT

Issue Date: October 7, 2005

Number: 06-01

To: Hector V. Barreto
Administrator

Stephen D. Galvan
Deputy Administrator
Chief Operating Officer
Chief Information Officer

Charles McClam
Acting Chief Information Officer

Delorice P. Ford
Chief Privacy Officer

/S/ Original Signed
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 U.S. Code Title 44, Chapter 35, Section 3545 as well as OMB Memorandum M-05-15. We performed an independent evaluation of SBA's information security program to reach conclusions about the adequacy of FISMA reporting areas. In making our evaluation, we considered prior audits related to SBA's information systems computer security program issued by our office in fiscal year 2005 as well as analyzing pertinent information in SBA's Information Technology Security and Privacy areas.

Our assessment covered the 20 high-priority systems identified by SBA and its characterization of compliance with FISMA requirements from September 16, 2004 to August 15, 2005. OMB Memorandum M-05-15 indicates that we were encouraged to provide any additional narrative in an appendix to the (FISMA) report to the extent those comments provide meaningful insight into the status of the agency's security or privacy program.

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 2005 through October 2005.

OVERALL EVALUATION

Generally for FY 2005, the SBA's computer security program continues to show mixed results. SBA continued to have 19 of 20 major systems (95 percent) certified and accredited as of the end of our fieldwork on August 15, 2005. However, SBA has not been able to timely or sufficiently address 161 unimplemented system risk assessment vulnerabilities and 50 unresolved OIG audit findings for which recommendations had exceeded their estimated target date for completion to correct the issues identified. A number of these unimplemented audit recommendations and risk assessment weaknesses are significant to SBA's information technology environment.

For FY 2005, OMB requested an in depth review of SBA's Certification and Accreditation Process. We have identified the following areas which came to our attention during the FISMA review process.

Finding 1: SBA's Certification and Accreditation Program Does not Meet all Necessary Aspects of NIST Requirements

We found most processes with respect to SBA's certification and accreditation (C &A) program were implemented appropriately. However, we found three areas that did not fully meet existing National Institute Standards and Technology (NIST) guidance for performing C&A activities. Given the scope of the three exceptions in relation to the overall program, we rated the quality of SBA's C&A process as "Satisfactory" in the annual FISMA evaluation.

a. Continuous Monitoring of SBA systems is not Incorporated into SBA's Certification and Accreditation Requirements

SBA had not fully incorporated continuous monitoring of its information systems into any of the five Certifications and Accreditations (C&A) issued after September 2004. As a result, SBA is not fully ensuring that its systems are fully protected during certification reviews.

According to Guidelines for Certification and Accreditation (NIST 800-37) Section 3.4 Task 9, the objective of the security control monitoring task is to: (i) select an appropriate set of security controls in the information system to be monitored; and (ii) assess the designated controls using methods and procedures selected by the information system owner. The continuous monitoring of security controls helps to identify potential security-related problems in the information system that are not identified during the security impact analysis conducted as part of the configuration management and control process. The authorizing official and information system owner should agree on the subset of security controls and the frequency of monitoring activity.

We reviewed C&A packages for five systems finalized after September 2004. We could not identify an appropriate set of security controls in the information system to be monitored for any of the five C&A packages finalized since September 2004. Additionally, we noted in OIG Audit 5-12 issued on February 22, 2005 that:

> Logging and monitoring controls at the network and application level were weak. SBA had no policies and procedures identifying which activities should be logged and how to determine these activities, and had not specified who should review logs and how often. SBA briefly discussed logging in their Procedural Notice 9000-1407 and SOP 90-47-1; however, not at a level sufficient to ensure that individuals know what to log, who should review the logs, what the logs should be reviewed for, and how often they should be reviewed.
>
> We previously recommended in the Audit of SBA's Information Systems Controls for FY 2004, Audit Report 5-12, that the Chief Information Officer for all SBA internal and contractor supported general support systems and major applications, e.g. Egan Mainframe; SBA and Corio UNIX; Network and Windows 2000; Loan Accounting System, Sybase; JAAMS Oracle, and related application functions:
>
> - Develop and document policies and procedures clearly outlining what activities should be logged, who should be responsible for reviewing logs, what the logs should be reviewed for, how often logs should be reviewed, and how long logs should be retained.
> - Assign responsibility within OCIO Security for the review of application and general support system security logs.
> - Retain audit logs for a sufficient period of time (at least 90 days).

b. SBA had not Implemented a Comprehensive Configuration Management Capability

SBA has not fully incorporated a comprehensive configuration management capability into four of five C&A's issued since September 2004. As a result, SBA is not ensuring that changes to its systems are documented and controlled. Additionally, the assessment of changes to the security of a system are an essential aspect of maintaining valid accreditations of SBA systems.

According to Guidelines for Certification and Accreditation (NIST 800-37) Section 3.4 Task 8, the objective of the configuration management and control task is to:

(i) document the proposed or actual changes to the information system; and (ii) determine the impact of proposed or actual changes on the security of the system.

We requested configuration management plans for all five systems with C&A's finalized after September 2004. SBA provided a copy of one configuration management plan for the Disaster Credit Management System (DCMS) which had been finalized after September 2004. However, we identified that this configuration management plan was for identifying changes to DCMS during development and not for the production environment. Therefore, that configuration management plan was not applicable to maintaining the DCMS system.

The SBA Systems Development Methodology requires that configuration management plans be created for all new Agency applications and that these plans include configurations down to the software or product level.

At the time of our review, OIG identified that a configuration management plan for the contractor operated systems Section 8(a) Small Disadvantaged Business Management Information System and Contract Loan Servicing were not obtained by SBA. In addition, SBA could not provide configuration management plans for its internal LAN/WAN system. The C&A documentation for those systems refer to the SBA Systems Development Methodology (SDM) as the standard for configuration management.

We concluded that each SBA system should contain a system configuration management plan which would document the change control process for that particular system. SBA should also have its own configuration management plans which document the change control process when SBA requests changes to contractor provided systems. These plans should identify who at SBA would request a change, how that change would be programmed, tested, and moved into production in a controlled manner by SBA's contractors. These configuration management plans should be validated and tested in the C&A process before a system is accredited.

c. SBA's Local Area Network / Wide Area Network was Improperly Accredited

SBA improperly fully accredited its Local Area Network / Wide Area Network (LAN/WAN) general support system during its most recent accreditation on May 19, 2005. This occurred because the LAN/WAN was categorized as "high" during its Federal Information Processing (FIPS) 199 system categorization review, and according to accreditation documents signed as of May 19, 2005 the LAN/WAN lacked a disaster recovery plan and a back-up recovery facility. As a result, SBA should not have fully accredited its LAN/WAN, but issued an "interim authority to operate" accreditation while SBA obtained the necessary back-up recovery plan and facility.

According to NIST Guidelines for Certification and Accreditation of Federal Information Systems, if, after assessing the results of the security certification, the authorizing official deems that the risk to the agency operations, agency assets, or individuals is unacceptable, but there is an overarching mission necessity to place the information system into operation or continue its operation, an interim authorization to operate may be issued. An interim authorization to operate is rendered when the identified security vulnerabilities in the information system resulting from deficiencies in the planned or implemented security controls are significant but can be addressed in a timely manner.

Ancillary documentation provided by SBA identified that a backup recovery plan and facility had actually been acquired and tested before the certification and accreditation was signed by SBA. However, this information was not in the finalized accreditation package and therefore the accreditation documentation was not current at the time of signature. SBA should have either issued an interim authority to operate for the LAN/WAN or ensured that significant risks to the system identified in the LAN/WAN POA&M were accurately reflected before signature.

Recommendations: We recommend that the Chief Information Officer:

1.A Fully incorporate "Continuous Monitoring" of major applications and general support systems as a task within SBA's Certification and Accreditation program in accordance with NIST Guidelines for Certification and Accreditation (NIST 800-37).

1.B Require that configuration management plans be incorporated within Certification and Accreditation packages for all SBA systems, including those systems operated by contractors.

Finding 2: SBA's Privacy Impact Assessment Program did not Meet all Necessary Aspects of OMB Requirements

A number of newly created Privacy Impact Assessments (PIA) for SBA's major systems did not contain information to address all necessary aspects of a PIA. This occurred because SBA had not analyzed the systems or evidence accompanying the systems beyond completion of the questionnaire. For example, there was no analysis or assessment of whether the system complied with privacy requirements based on the questionnaire results or a description of any new or planned changes to the system based on the results of the PIAs. Additionally, there were no measures to mitigate risks identified for each alternative and the rationale for making changes to the system or implementing controls over the utilization of the data.

OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires that each agency conduct PIAs for electronic information systems and collections and, in general, make them publicly available. The PIA must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA. For major information systems, PIAs conducted for these systems should reflect a more extensive analyses of: (1) the consequences of collection and flow of information, (2) the alternatives to collection and handling as designed, (3) the appropriate measures to mitigate risks identified for each alternative, and (4) the rationale for the final design choice or business process.

We identified that the answers to the questionnaires which made up SBA PIA's were not in sufficient detail commensurate to the size and complexity for SBA's major information systems and did not address fully areas of previously identified vulnerabilities. The following two examples are identified from our review:

a. **The Joint Accounting and Administrative System (JAAMS):** OIG's audit report "SBA's Implementation of the Joint Accounting and Administrative System (3-32) issued on June 30, 2003; [FOIA Ex. 2].

   a. The following questions were answered as not applicable in the PIA questionnaire – Section E. Maintenance of Administrative Controls:

      [FOIA Ex. 2]

      We concluded that each of these questions should have been completed in the affirmative. Additionally, an in depth analysis should have been performed identifying what controls either systematic or manual should have been implemented to prevent or detect unauthorized monitoring of employee information within the JAAMS system.

b. **Contract Loan Servicing:** During OIG audit "SBA's Oversight of the Fiscal Transfer Agent For The 7(A) Loan Program (3-08) issued on January 30, 2003; we had reviewed the Fiscal Transfer Agent's (FTA) internal procedure manual for setting up loans within the FTA's information system. The internal procedure manual identified that borrower SSN and co-owner name and address are to be entered into the FTA system.

   a. The following questions were answered as "No" in the PIA questionnaire – Section B. System Application/General Information:

      i. Does this system contain any information about individuals? – No.
         1. Is this information identifiable to the individual? – No.

      We concluded that both of these questions should have been completed in the affirmative. Additionally, a further review of Contract Loan Servicing was warranted before the PIA was finalized.

Overall, the Senior Agency Official for Privacy has taken actions to increase awareness of privacy issues and improve the quality of PIAs. Among the actions taken or planned for the near future are: Implement a new privacy regulation, improve PIA guidance, conduct internal monitoring and auditing, conduct privacy training and develop open lines of communication with system owners and the Inspector General.

Recommendations:

We recommend that the Senior Agency Official for Privacy:

2.A Ensure that PIAs contain an analysis of the questionnaire answers and an overall assessment of the system compliance to the Privacy Act.

2.B Require that PIAs for major systems reflect a more extensive analysis of the consequences of collection and flow of information, the alternatives to collection and handling as designed, the appropriate measures to mitigate risks identified for each alternative and the rationale for the final design choice or business process.

* * *

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-[FOIA Ex. 2].

Attachment

Section C: Inspector General Questions 1, 2, 3, 4, and 5

Agency Name: U.S. Small Business Administration

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance in FY 05 by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						Question 2					
		a. **FY 05 Agency Systems**		**b.** **FY 05 Contractor Systems**		**c.** **FY 05 Total Number of Systems**		**a.** **Number of systems certified and accredited**		**b.** **Number of systems for which security controls have been tested and evaluated in the last year**		**c.** **Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Agency Totals	**High**	2	2	3	3	5	5	5	100.0%	2	40.0%	[redacted]	[redacted]
	Moderate	11	11	4	4	15	15	14	93.3%	5	33.3%	[redacted]	[redacted]
	Low											[redacted]	[redacted]
	Categorized											[redacted]	[redacted]
Total		13	13	7	7	20	20	19	95.0%	7	35.0%	[redacted]	[redacted]

FOIA Ex. 2

Question 3

In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Almost Always, for example, approximately 96-100% of the time
3.b.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 96-100% complete
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	Yes

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below

For items 4a.-4.f, the response categories are as follows:

- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Mostly, for example, approximately 81-95% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s)	- Almost Always, for example, approximately 96-100% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Mostly, for example, approximately 81-95% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time

Comments: See below:

Question 2.2.a. Nineteen out of 20 SBA systems had a valid Certification and Accreditation as of end of fieldwork on August 15, 2005.

Question 2.2.b. Seven of 20 SBA systems had a full scope Security Test & Evaluation (ST&E) performed between September 16, 2004 and August 15, 2005.

Question 2.2.c. OIG Audit 5-17 on Contingency of Operations Planning (COOP) identified that all of SBA's System Disaster Recovery Plans (SDRP) were in "draft" status as of Mach 2005. Further, SBA did not use its SDRP's to actually recover its major systems during recovery test exercises, but relied upon the expertise of certain personnel who had in depth knowledge of SBA systems to recover its systems during test exercises. OIG recommended "finalization" of all SBA SDRP's and the utilization of those SDRP's to actually test recovery of SBA systems. As of the end of FISMA fieldwork, SBA had finalized all of its internal SDRPs. SBA also tested 3 SDRP's for its internally owned systems after SDRP plan finalization. We analyzed four SAS-70 reports on contractor provided systems and gave credit for three contractor provided systems whereby Disaster Recovery Capability had been verified in SAS-70 audits of SBA's contractor computing environment.

Question 4.a. The SBA POA&M identified 292 of 346 (84.39%) open risk assessment vulnerabilities and audit recommendations.

Question 4.e. The SBA POA&M contained 106 of 117 (90.60%) open OIG audit recommendations.

Question 4.f. The SBA POA&M identified that all 307 weaknesses identified as open were prioritized. The SBA POA&M also identified that 161 of the 307 (52.44%) of weaknesses identified as open had exceeded their corrective action date. SBA needs to ensure that significant security issues are addressed in a timely manner and receive appropriate resources.

Question 5

OIG Assessment of the Certification and Accreditation Process OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance and standards Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004 This includes use of the FIPS 199 (February, 2004) "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level as well as associated NIST documents used as guidance for completing risk assessments and security plans .

Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Satisfactory

Comments for Question 5: We reviewed five Certification and Accreditations finalized after between October 2004 and August 2005. See the comments below on SBA's C&A process.

Comment 1: SBA's Certification and Accreditation process did not include a strategy for "Continuous Monitoring" as identified in NIST 800-37, Section 2.7 for any of the 5 C&A's finalized after September 2004.

Comment 2: SBA's accreditation decision for one system rated as "high" for data sensitivity was at the time improper based upon the fact that according to accreditation documentation, the system did not have a complete and tested disaster recovery capability. Ancillary information identified that the risk had been corrected, however this was not reflected in accreditation documentation signed by SBA.

Comment 3: SBA did not require finalization of documented Configuration Management plans for 4 of 5 systems reviewed before it fully accredited those four major systems.

Section B: Inspector General. Question 6, 7, 8, and 9.

Agency Name: Small Business Administration

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.		[ ]
	[ ]		
6.b.	Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.		
Product	Addressed in agencywide policy? Yes, No, or N/A.	Do any agency systems run this software? Yes or No.	Approximate the extent of implementation of the security configuration policy on the systems running the software. Response choices include: - Rarely, or, on approximately 0-50% of the systems running this software - Sometimes, or on approximately 51-70% of the systems running this software - Frequently, or on approximately 71-80% of the systems running this software - Mostly, or on approximately 81-95% of the systems running this software - Almost Always, or on approximately 96-100% of the systems running this software

[ ]

FOIA Ex. 2

Question 7

Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.

7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes

Comments: During the year, SBA submitted 9 of 12 monthly reports to FedCIRC on time. SBA delayed up to three months in submitting its reports to FecCIRC between 10/01/04 - 12/31/04.

Question 8

8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training
Comments:	SBA provided records that 3,053 of 3,458 (88.3%) of personnel took "End-User Security Training in FY 2005.	SBA has not implemented an adequate training program for those employees and contractors with significant IT security responsibilities.

Question 9

9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

ATTACHMENT A

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