ADVISORY MEMORANDUM REPORT ON

SBA'S INFORMATION SECURITY PROGRAM

REPORT NUMBER 2-28

SEPTEMBER 12, 2002

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: September 12, 2002
Number: 2-28

To: Hector V. Barreto
Administrator

Robert G Seabrook

From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Independent Evaluation of SBA's Information Security Program

The Government Information Security Reform Act (GISRA) 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 GISRA reporting instructions issued by the Office of Management and Budget (OMB).

BACKGROUND

GISRA amended the Paperwork Reduction Act (PRA) of 1995 and added a new subchapter on information security. GISRA focused on the program management, implementation and evaluation aspects of the security of unclassified and national security systems. Generally, GISRA codified existing OMB security policies, Circular A-130, Appendix III, the PRA, and the Clinger-Cohen Act of 1996. SBA processes sensitive but unclassified information on its computer systems and is therefore subject to GISRA requirements. SBA operates or contracts for computer system services on 37 high-priority computer systems that are the subject of GISRA.

OBJECTIVES, SCOPE AND METHODOLOGY

The objective of our review was to evaluate SBA's information security program in accordance with GISRA reporting requirements specified in OMB Memorandum 02-09. We performed an independent evaluation of SBA's information security program to come to our conclusions about the GISRA reporting areas. In making our evaluation, we considered prior audits issued by our office. We also augmented our prior audit coverage with independent evaluations of SBA's computer security program.

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 August 31, 2002. As part of our evaluation, we accompanied Integrated Management Services Incorporated (IMSI), the SBA contractor, on selected reviews to identify and assess sensitive SBA systems. We interviewed SBA officials and reviewed documentation on the SBA security program.

Our evaluation was performed at SBA's Central Office in Washington, D.C. from July 2002 through August 2002.

OVERALL EVALUATION

Generally, SBA's information security program continues to improve for high priority financial management and general support systems. However, vulnerabilities continue to exist in computer security program monitoring, computer incident response reporting, system access controls, computer security system testing, and disaster recovery and contingency planning.

EVALUATION RESULTS

OMB Question A.2. Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

In last year's report, SBA identified 95 high priority systems. Fifty-eight (58) of the 95 systems identified last year were actually subsystems of 37 high priority systems. In this year's report, SBA is identifying only the high priority systems, not their subsystems. Accordingly, the number of systems shown in the table below for last year (FY 2001) has been revised downward from 95 to 37.

Since last year's report a new financial accounting system (Joint Accounting and Administrative Management System) became operational this year. It replaced the Federal Financial System that SBA used last year through a cross-servicing agreement with the Department of the Treasury. SBA's use of the Federal Financial System was identified last year as a high priority SBA system.

Table 1.
High Priority Systems Reviewed by OIG

	FY01	FY 02
a. Total number of agency programs.	7	7
b. Total number of agency systems.	37	37
c. Total number of programs reviewed.	4	4
d. Total number of systems reviewed.	11	14

The Office of the Inspector General has overseen or performed independent audits or evaluations for the past two fiscal years on SBA general support systems and major applications that support SBA's high-priority systems. This includes audits of:

- Information System Control for fiscal years 2000 and 2001
- Critical Infrastructure Protection Program
- Development of the Loan Monitoring System
- SBA Computer Security Program
- SBA's UNIX Servers

The Information System Controls reviews were performed in accordance with the General Accounting Office (GAO) Federal Information System Controls Audit Manual. The SBA Computer Security review was a further evaluation of SBA's computer security program with specific emphasis on GISRA reporting requirements.

The Office of Inspector General also reviewed the assessments conducted by SBA program officials with the assistance of a contractor, IMSI. These assessments followed the process and checklist found in the National Institute of Standards and Technology (NIST) Special Publication (SP) Number 800-26, "Security Self-Assessment Guide for Information Technology Systems." The assessments also included questions specific to SBA's computer systems environment. The SBA Office of the Chief Information Officer (OCIO) coordinated IMSI efforts. An OIG auditor observed IMSI's conduct of assessments and found them to be reliable.

Table 2.
High-Priority Systems Reviewed by SBA

	FY01	FY02
a. Total number of agency programs.	7	7
b. Total number of agency systems.	37	37
c. Total number of programs reviewed.	7	7
d. Total number of systems reviewed.	34	37

OMB Question A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY02.

Last year, no material weaknesses were reported in SBA's computer security program regarding policies, procedures or practices. However, significant security issues existed at that time including:

- Weak security controls including identification and authentication and separation of duties on individual systems (a material weakness for FY 2002),
- Inadequate security and intrusion detection monitoring and failure to consistently report security incidents (a material weakness for FY 2002),
- Incomplete planning and certification of major applications and general support systems (a material weakness for FY 2002),
- Limited supervision of contractor provided services (a material weakness for FY 2002), and
- Inadequate security training.

For FY 2002, OIG reaffirmed the significant security weaknesses identified in FY 2001. From the review of the SBA plan of action and milestones (POA&M) as of April 30, 2002 and OIG's knowledge of SBA's computer security program, none of the significant security issues can be withdrawn at this time.

The first four weaknesses in the FY 2001 list are considered material weaknesses for FY 2002 for Security Act reporting purposes. Two additional material weaknesses are added for FY 2002:

- Inadequate security testing and evaluation program, and
- Incomplete disaster recovery and contingency planning and testing.

Table 3.
Number of Material Weaknesses

	FY01	FY02
a. Number of material weaknesses reported.	0	6
b. Number of material weaknesses repeated in FY02.	0	0

OMB Question B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

A draft memorandum from the Administrator that will set forth duties and responsibilities for SBA program officials is being finalized. The draft stated that the OCIO will continue to lead SBA's initiative to enhance the Agency's computer security program and its responsibilities under the Security Act. OCIO will assist program offices in fulfilling IT security responsibilities as mandated by the Security Act.

Currently SBA Standard Operating Procedure 90 47, *Information System Security Program*, states the following responsibilities for the SBA Administrator:

> The SBA Administrator is responsible for establishing a management control process to ensure that appropriate administrative, physical, and technical safeguards are incorporated into all new applications and into significant modifications to existing applications. The Administrator has delegated this responsibility to the Chief Information Officer (CIO).

A major operating component of the agency cannot make a significant IT investment decision without review by and concurrence of the agency Business Technology Investment Council (BTIC). The Council is composed of senior agency executives and chaired by the CIO. The CIO ensures compliance with SBA infrastructure and architecture standards and advises the BTIC on technical matters. The BTIC is responsible for reviewing and making decisions on all major IT investments, including screening, scoring, and prioritizing new initiatives, monitoring ongoing investments, and evaluating implemented investments.

OMB Question B.2. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.) During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system?

According to SBA Standard Operating Procedure 90 47, *Information System Security Program*, the Administrator has delegated the creation of information security plans to the Chief Information Officer. During the FY 2002 reporting period, the CIO in concert with SBA program officials prepared system security plans for seven additional SBA systems as compared to the FY 2001 totals.

The CIO stated that after the initial 3-year certification, accreditation, assessment of risk, and system security plan creation for all SBA systems, it will be the responsibility of the SBA system owners to schedule, fund and create or update their own system security plans. The initial accreditation procedure was funded through the OCIO so that a formalized approval process could be created with baseline security documentation created.

The Agency has not codified through an SOP how security will be enforced for SBA systems throughout a system's life cycle. An information notice was issued in November 2001 that requires all internally developed systems to follow the SBA's Systems Development Methodology (SDM). No SOP covers the broad areas of systems development or acquisition. As part of SBA's "Ten Management Challenges," OIG recommended that such an SOP be developed. The envisioned SOP should include policies, procedures, and processes needed to address areas such as requirements management, project planning, project tracking and oversight, software quality assurance, configuration management, acquisition planning, solicitation, contract tracking and oversight, product evaluation, and transaction support. Additionally, a comprehensive SOP would be a framework for aiding the other SBA offices as those offices begin the process of managing new systems.

OMB Question B.3. How has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?

Prior to March 2001, SBA did not include protection of physical assets in its Critical Infrastructure Protection Plan (CIPP). In response to OIG Audit Report Number 1-09, "SBA's Planning and Assessment for Implementing Presidential Decision Directive 63," dated March 26, 2001, SBA named a Deputy Chief Infrastructure Assurance Officer (CIAO) for Physical Infrastructure. Unlike the CIAO, the Deputy CIAO is not located in the Office of the Chief Information Officer. Organizationally, both the CIAO and the Deputy CIAO are within groups under control of SBA's Chief Operating Officer. Continuity of operations for SBA systems is assigned to the CIAO. Physical and operational security are assigned to the Deputy CIAO.

The SBA has separate staffs assigned to physical security and information system security. There is little or no duplication of effort. The two sections can work in concert on issues of mutual importance and periodically meet to discuss Critical Infrastructure issues.

OMB Question B.4. Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

SBA has undergone the discovery phase of a Project Matrix Review. The review determined that SBA systems do not meet the threshold for a full Project Matrix review. The Department of Commerce therefore declined to further evaluate SBA using Project Matrix criteria. No SBA system impacts national security, national economic stability, or critical public health and safety.

SBA initially attempted to identify its critical information systems and assets in response to Presidential Decision Directive 63. The initial Critical Information Protection Plan (CIPP) was written in 1998. The CIPP identified 5 broad business functions and program areas within SBA that were considered critical. From the broad business functional areas SBA then performed a "workload assessment" in 1999. The workload assessment drilled down from the functional business areas to the actual SBA systems. A computerized model was used to identify and rank the sensitivity of SBA systems using defined criteria. The initial assessment was a success as far as it went, but did not include contractor provided services, nor systems purchased by separate SBA offices and operated on OCIO general support systems.

SBA currently uses system security plans and a mix of full system risk assessments and GISRA self assessments to identify its critical systems. SBA has not developed an agency-wide integrated security plan for implementing and integrating SBA's computer security program across all general support systems and major applications. Therefore, full interdependencies and interrelationships between critical systems have not been fully established agency-wide.

For disaster recovery and contingency planning purposes, SBA has drafted, but not finalized, a written plan that identifies the sensitivity of SBA systems by the time needed for recovery. For example, SBA has not determined which mission critical general support systems and major applications must be recovered in the event of a full emergency in which all systems are disabled. A timeline for recovery of 0-3 days, 4-10 days, 11-30 days, and 30 or more days should be determined for all systems. Then, appropriate disaster recovery and contingency planning should be undertaken.

OMB Question B.5. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

According to SBA Standard Operating Procedure 90 47, *Information System Security Program*, the Administrator has delegated reporting of security incidents to the Chief Information Officer who then further delegated responsibility to the Agency Computer Security Program Manager. OCIO issued SBA Computer Emergency Response Team (CERT) procedures manual to report security incidents to the Agency Computer Security Program Manager who would then report those incidents to FedCIRC.

The SBA and FedCIRC developed a Memorandum of Understanding in June 2000 that requires a quarterly report of security incidents to FedCIRC. The first quarterly report was not submitted until two years later in July 2002. SBA had seven probes or scans of its internet router that met FedCIRC's criteria for reporting immediately and did not report them until the July 2002 quarterly report was submitted. In our judgment, SBA does not share incident information with FedCIRC in a timely manner.

Table 4
Agency Components

a. Total number of agency components including bureaus, field activities.	1
b. Number of agency components with incident handling and response capability.	1
c. Number of agency components that report to FedCIRC	1
d. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	No
e. What is the required average time to report to the agency and FedCIRC following an incident?	The Agency has not established and does not track average time to report either internally or to FedCIRC.
f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	Security personnel within the Office of the Chief Information Officer communicate with SBA systems administrators by email to confirm that new patches for operating systems have been installed. This procedure was implemented in May 2002 in response to OIG Audit Report No. 2-18, dated 5-16-02. Previously, SBA did not confirm that patches were installed. SBA does not confirm that patches for contractor-operated systems are installed timely.

Table 5
Incident Reporting

	FY01	FY02
g. By agency and individual component, number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported by each component	SBA (one component)	SBA (one component)
- Successful/unsuccessful network penetrations	Unknown	Unknown
- Root or user account compromises	Unknown	Unknown
- Denial of service attacks	Unknown	Unknown
- Website defacing attacks	Unknown	Unknown
- Malicious code and viruses	1	7,509
- Probes and scans	30 (estimated)	7
h. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.	1	7,553

OMB Question C.1. Have agency program officials: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting

the operations and assets under their control; and 4) tested and evaluated security controls and techniques? (Section 3534(a)(2) of the Security Act.)

Last year (FY 2001), SBA had 37 major applications and general support systems. This year (FY 2002) SBA has 37 different major applications and general support systems.

Table 6
Number of SBA Systems

COMPONENT OR BUREAU NAME	TOTAL NUMBER OF SYSTEMS	
Small Business Administration	37 in FY01	37 in FY02

Table 7
System Risk Assessments

	FY01	FY01	FY02	FY02
	#	%	#	%
a. Systems that have been assessed for risk.	14	39%	22	59%
b. Systems that have been assigned a level of risk after a risk assessment has been conducted (e.g., high, medium, or basic).	14	38%	22	59%
c. Systems that have an up-to-date security plan.	15	40%	22	59%
d. Systems that have been authorized for processing following certification and accreditation.	14	39%	22	59%
e. Systems that are operating without written authorization (including the absence of certification and accreditation).	22	61%	15	41%
f. Systems that have the costs of their security controls integrated into the life cycle of the system.	0	0%	0	0%
g. Systems for which security controls have been tested and evaluated in the last year.	0	0%	1	3%
h. Systems that have a contingency plan.	7	19%	7	19%
i. Systems for which contingency plans that have been tested in past year.	0	0%	8	22%

OMB Question C.2 For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

SBA has a cross servicing agreement with USDA NFC for payroll services. SBA relies upon the USDA OIG to perform audit services to ensure that SBA's payroll services are adequately secure and meet federal processing standards. As indicated in the table below, SBA reviewed the security of services provided by two contractors in FY 2002. These two contractors were Colson Services Corporation and Applied Computer Services.

Table 8

Contractor Facilities

	FY01	FY02
a. Number of contractor operations or facilities.	3	3
b. Number of contractor operations or facilities reviewed.	0	2

OMB Question D.1. Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5)) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

Table 9

Security Reviews

	FY01	FY02
a. Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews?	N/A	N/A
b. What percentage of components and field activities have had such reviews?	N/A	N/A
c. Number of agency employees including contractors. (see note c. below)	4,112	4,022
d. Number and percentage of agency employees including contractors that received security training. (see note d. below)	3,906 95%	3,411 85%
e. Number of employees with significant security responsibilities. (see note e. below)	231	251
f. Number of employees with significant security responsibilities that received specialized training.	56	215
g. Briefly describe what types of security training were available.	See note g. below.	See note g. below.
h. Total costs for providing training described in (g).	$136,000	$89,235
i. Do agency POA&Ms account for all known agency security weaknesses including of all components and field activities? If no, why not? (see note i. Below)	N/A	No. There were 74 weaknesses not listed in the 4/30/02 POA&M.
j. Has the CIO appointed a senior agency information security official?	Yes	Yes

Notes:

a. The SBA is one Agency with no components or separate field activities. Therefore this question is not applicable to SBA. This determination was made after attending a question and answer session with OMB on July 31, 2002.

b. The SBA is one Agency with no components or separate field activities. Therefore this question is not applicable to SBA. This determination was made after attending a question and answer session with OMB on July 31, 2002.

c. The figure of 4,112 for FY01 includes SBA employees only; no contractors were included. The figure of 4,022 for FY02 includes both employees and contractors.

d. The figures of 3,906 and 3,411 include both employees and contractors. Consequently, the percentage of personnel who received training in 2001 was overstated.
e. There were 231 Designated Security Officers in FY01 and FY02. The figure of 251 for FY02 includes 20 security administrators.
f. The figures of 215 for FY02 includes 137 Designated Security Officers and 78 individuals who completed systems administrator security training. There are fewer than 78 security administrators at SBA. In our opinion, SBA does not offer adequate technical security training at the network or application level for security administrators as we reported in SBA OIG Audit Report Number 2-18 dated May 6, 2002.
g. SBA requires all employees to annually complete basic computer security awareness training. SBA requires additional training modules for employees who are a Functional Program Manager, Designated Security Officer (DSO)/Information Resources Manager (IRM), and System Administrator (S/A).
i. The POA&M did not include 74 security vulnerability issues in the April 2002 submission to OMB. These 74 issues included open audit findings from the OIG audit tracking system. Additionally, a large number of security vulnerabilities identified from other sources such as system risk assessments were not included. Furthermore, security risks that have been "accepted" by management were omitted from the report. This was specifically noted for SBA's Loan Accounting System.

OMB Question D.2. For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

Table 10

Contractor Operations Reviewed

	FY01	FY02
a. Number of contractor operations or facilities.	1	2
b. Number of contractor operations or facilities reviewed.	1	1

The SBA has a contract with Unisys to provide mainframe and midrange computing services for SBA's high priority systems. Security personnel within the Office of the Chief Information Officer reviewed computer security at the Unisys facility in Egan, Minnesota in FY 2002.

The SBA has a contract with Iron Mountain Data Services. Performance began in early 2002. No review of the Iron Mountain facility was performed in FY 2002.

OMB Question D.3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If not, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

Table 11

Capital Asset Planning

	FY03 Budget Materials	FY04 Budget Materials
a. Number of capital asset plans and justifications submitted to OMB?	1	
b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs?	1	
c. Were security costs reported for all agency systems on the agency's exhibit 53?	No	
d. Have all discrepancies been corrected?	No	
e. How many have the CIO/other appropriate official independently validated prior to submittal to OMB?	None	

The Agency Capital Asset Plans, Justifications, and Exhibit 53 for FY 2004 were not completed and provided to the OIG in time for inclusion in this evaluation.

* * *

This report does not contain any recommendations; therefore, a reply is not necessary. Should you or your staff have any questions, please contact Robert G. Hultberg, Director, Business Development Programs Group at (202) 205-7577.

Attachment

ATTACHMENT

REPORT DISTRIBUTION

Recipient	Number of Copies
Associate Deputy Administrator for Management and Administration	1
Chief Information Officer	1
General Counsel	2
General Accounting Office	1
Chief Financial Officer Attention: Jeff Brown	1