

**ADVISORY MEMORANDUM REPORT ON
SBA'S COMPUTER SECURITY PROGRAM**

ADVISORY REPORT NUMBER A1-06

SEPTEMBER 28, 2001

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.



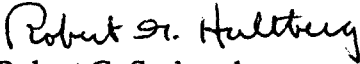
**U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416**

**MEMORANDUM ADVISORY
REPORT**

Issue Date: September 28, 2001

Number: A1-06

To: Lawrence E. Barrett
Chief Information Officer

From: *for* 
Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Evaluation of SBA's Computer Security Program

The Government Information Security Reform Act (GISRA) requires that the Inspector General perform an independent evaluation of the Small Business Administration (SBA) information security program. This report presents the results of that evaluation.

BACKGROUND

The Government Information Security Reform Act 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, the Act codified existing Office of Management and Budget (OMB) security policies, Circular A-130, Appendix III, the PRA, and the Clinger-Cohen Act of 1996. The SBA processes unclassified but sensitive information on its computer systems and is therefore subject to GISRA requirements. SBA operates or contracts for computer system services on 96 high-priority computer systems that are the subject of GISRA.

OBJECTIVES, SCOPE AND METHODOLOGY

The objective of our review was to evaluate SBA's computer security program and assess management controls over safeguarding of information in accordance with GISRA requirements. We reviewed prior audits issued by our office on selected information systems and considered the results of the information security controls evaluated as part of SBA's financial statement audit using the Federal Information System Controls Audit Manual (FISCAM) for fiscal years 1998, 1999 and 2000. We also

augmented our prior audit coverage with independent evaluations of SBA's computer security program to come to our conclusions on GISRA reporting areas.

Our assessment covered the 96 high priority systems identified by SBA and its characterization of the susceptibility of those systems to unauthorized access as of July 31, 2001. As part of our evaluation, we accompanied Integrated Management Services Incorporated (IMSI), the contractor SBA hired to identify and assess sensitive SBA systems. IMSI identified and assessed those systems that had not been previously reviewed during SBA's certification and accreditation reviews. During these assessments, we interviewed SBA program officials and others in the Office of the Chief Information Officer (OCIO).

The results of our evaluation have also been reported in an OIG Executive Summary as requested by OMB in its Reporting Instructions for the Government Information Security Reform Act (Memorandum 01-24). Our work was performed at SBA's Central Office in Washington, D.C. from June 1, 2001 through July 31, 2001. This report covers those computer security program areas that we identified in the OIG Executive Summary that need improvement or increased management emphasis. All areas where SBA maintains a satisfactory information security program are excluded from this report.

EVALUATION RESULTS

SBA generally maintains a satisfactory information security program for its high priority financial management and general support systems. Additionally, SBA has developed and issued policies and procedures to address security protections agency-wide. However, SBA information security vulnerabilities continue to exist in computer security system testing, computer security program monitoring, system access controls and disaster recovery and contingency planning. These vulnerabilities will require continued management emphasis in information security with the appropriate underlying resources to ensure that the security and continuity of SBA systems will be improved. We are making recommendations to establish a security system testing program, upgrade computer security monitoring capabilities, strengthen access controls and fully implement disaster recovery and contingency planning along with several other recommendations to strengthen SBA's administration of the computer security program.

Finding 1: Improving SBA's Certification and Accreditation Program

As part of the GISRA evaluation, the OIG reviewed the Certification and Accreditation¹ packages that have been completed for SBA systems. Certification and

¹ Certification is the comprehensive evaluation of the technical and non-technical security features of a major application or general support system to measure compliance with security requirements, including all applicable Federal laws and regulations, and SBA policies and standards.

Accreditation packages include preparing risk assessments and security plans for SBA systems. We identified the following areas that need improvement in SBA's Certification and Accreditation program.

Completion of Risk Assessments and Security Plans

System risk assessments and security plans have been completed for about 33 of 95 Agency high-priority systems as part of the SBA Certification and Accreditation program. Additionally, three more risk assessments and two security plans are in progress and the remaining risk assessments and security plans need to be completed.

Implementing a Management Control Process

The OIG reviewed the risk assessments that have been completed as part of the Certification and Accreditation process. SBA OCIO had internally identified 122 risks to SBA systems, however, there was no management control process to identify which risks had been corrected, mitigated or accepted without correction. Additionally, there was no estimated scheduled date to correct risks in the future or assign funding to correct a risk as part of SBA's Capital Asset Plan. Consequently, the lack of a formalized process could result in these risks remaining uncorrected.

The following is a summation of the 122 risks for the risk assessments that OIG considered the most serious:

- Eight of the 122 risks ranked as either "high" or "medium" were in monitoring the security of SBA systems
- Thirteen of the 122 risks ranked as either "high" or "medium" were related to disaster recovery or contingency planning
- Eighteen of the 122 risks ranked as "medium" were related to weak system access controls

Implementing a Security Test and Evaluation Program

OIG identified that SBA does not have a Security Test and Evaluation (ST&E) program. While OCIO does have a ST&E procedure document, it has not been implemented and used to test Agency general support systems and major applications. ST&E testing by OCIO should be considered as part of the Certification process before a major application or general support system is implemented.

Accreditation is the formal process whereby a responsible SBA official authorizes a major application or general support system to operate based on: prescribed security safeguards, defined threats, vulnerabilities and an acceptable level of risk for which the accrediting official has assumed responsibility.

Recommendations:

We recommend that the Chief Information Officer:

- 1A. Complete risk assessments and system security plans for SBA's high-priority systems that have been identified as needing risk assessments and security plans.
- 1B. Create a formalized management control process that identifies if risks have been corrected, mitigated, accepted or need ongoing corrective action from the risk assessments performed for SBA systems.
- 1C. Include in its management control process a schedule to correct the identified deficiencies within the risk assessments including responsibilities, milestone dates for completion, and funding requirements for inclusion in the Agency Capital Asset Plan, Exhibit 53 to OMB.
- 1D. Correct, mitigate or accept the vulnerabilities identified in SBA's risk assessments. The most severe vulnerabilities include security monitoring, access controls, and disaster recovery and contingency planning.
- 1E. Develop a program to perform Security Test & Evaluation (ST&E) reviews on all of SBA's high-priority computer systems.

Finding 2: Improving SBA's Computer Security Training Program

During the GISRA evaluation, OIG identified areas that need improvement in the SBA computer security-training program. While we note that the OCIO computer security-training program satisfactorily trained a high percentage of the Agency's computer end-users through July 2, 2001, the following areas need improvement.

Ensure Training of Designated Security Officers / Information Resource Managers

OCIO did not ensure that Designated Security Officers/Information Resource Managers (DSO/IRM) and back-ups completed the Computer Based Training Course for DSO/IRM. OIG identified that only 56 of 231 (24%) DSO/IRM and designated back-ups completed the SBA security-training course as of July 2, 2001.

Provide In Depth Security Training to System Administrators

In a separate audit report, the OIG identified an individual who had operational security duties for operating one of SBA's general support systems and did not have adequate platform-specific security training. Additionally, this individual was not aware of SBA Standard Operating Procedure "Automated Information Systems Security Program" (SOP 90-47). While the scope for that report was for only that general support system, more in depth platform specific security training is warranted Agency-wide.

Improve Tracking and Follow-up Mechanisms for Computer Security Training Courses

OIG identified that the list of personnel taking the OCIO computer security training courses was not always accurate. This occurred because the tracking mechanism for verifying which individuals took which training course was not accurate. Additionally, SBA could not identify the universe of individuals who should have taken the four training courses. Therefore, accurate follow-up by OCIO and agency program managers was hindered. Improving the tracking of who has taken the computer security training courses will allow SBA to identify the percentage of individuals who should be taking the courses and allow for improved follow-up by agency managers.

Recommendations:

We recommend that the Chief Information Officer:

- 2A. Identify agency personnel who should be required to undertake security training as Designated Security Officers, Information Resource Managers and back-up personnel; and require those individuals to take the course on DSO/IRM security training.
- 2B. Identify and ensure that there is in depth training for those agency personnel who perform significant security duties.
- 2C. Work with agency managers to fully identify the universe of agency personnel who should be required to undertake security training as computer end-users, Designated Security Officers and back-ups, Information Resource Managers, and Program Managers.
- 2D. Improve the tracking mechanism for identifying who has taken each computer security training course to ensure that all responsible individuals take the required computer security training courses.

Finding 3: Update the Project Matrix Review

SBA last performed a formal Project Matrix Review in December 1999. It did not, however, fully cover contractor provided services, nor identify all systems that use Commercial-Off-The-Shelf (COTS) software. Additionally, systems that contained sensitive information, but are not considered major applications were not within the scope of the original review. According to the Agency Computer Security Program Manager, continuous updates to the Project Matrix Review occur, however, we have noted that no formal update has been completed since 1999.

A Project Matrix Review is an internal review that lists the criticality and sensitivity of SBA high-priority systems. A Project Matrix Review allows agencies to identify which systems should have Certification and Accreditation packages performed

and in what order. A Project Matrix Review also aids in determining which systems should be recovered and in what order for disaster recovery and contingency planning purposes.

Recommendation:

- 3A. We recommend that the Chief Information Officer formally update the agency Project Matrix to include major contractor provided services, Commercial Off-The-Shelf (COTS) software, and systems that contain sensitive information but are not considered major agency applications.

Finding 4. Improving Performance Measures Used by SBA

During the GISRA evaluation, OIG identified that certain performance measures reported to the Office of Management and Budget (OMB) need to be articulated or formalized to improve the SBA computer security program.

Requiring Use of the Systems Development Methodology

The SBA Chief Information Officer has issued an internal procedure manual for developing SBA systems. This manual known as the System Development Methodology (SDM) is an internal OCIO document and is not mandated by SBA Standard Operating Procedure (SOP). Therefore, the practices and procedures contained within the SDM are not required by SBA policy and would not need to be followed by other SBA Offices in implementing systems.

Performance Measures Used by the Chief Information Officer

According to SBA’s GISRA report to OMB, the Chief Information Officer ensures the effective implementation of the computer security program and evaluates the performance of major agency components primarily by using internal and external reviews and audits. While we recognize that audits and reviews play a key role in evaluating the CIO’s performance, we believe the CIO should develop internal performance measures with the aid of other SBA offices to ensure that the CIO provides the type of security, systems and services needed by the SBA.

Recommendations:

We recommend that the Chief Information Officer:

- 4A. Update SBA’s Standard Operating Procedure “Automated Information Systems Security Program” (SOP 90-47) to include the requirement for the Agency to follow the Systems Development Methodology when developing or acquiring new systems.

- 4B. Develop internal performance measures for SBA's Computer Security Program and other aspects of the operations of the Office of the Chief Information Officer to provide the type of security, systems, and services needed by SBA.

SBA MANAGEMENT'S RESPONSE

SBA's Chief Information Officer agreed with the recommendations. See Attachment 1 for the full text of his response.

* * *

The findings included in this report are the conclusions of the Office of Inspector General's Auditing Division. The findings and recommendations are subject to review, management decision, and corrective action by your office in accordance with 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 and target date for completion, or explanation of your disagreement with our recommendations.

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

Should you or your staff have any questions, please contact Robert G. Hultberg, Director, Business Development Programs Group at (202) 205-7577.

Attachments

Attachment 1



U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

Date: September 5, 2001
To: Robert G. Seabrooks, Assistant Inspector General for Auditing
From: Chief Information Officer
Subject: Evaluation of SBA's Computer Security Program

The Office of the Chief Information Officer (OCIO) agrees with the recommendations identified in your draft advisory memorandum report on your independent evaluation of SBA's information security program which was required by the Government Information Security Act (GISRA).


Lawrence E. Barrett

cc: Louise Wilson, OCFO
Thomas Dumaresq, Acting ADA/M&A

REPORT DISTRIBUTION

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