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

AUDIT REPORT
Issue Date: September 2, 1999
Report Number: 9-19

TO: Fred P. Hochberg
Deputy Administrator

Lawrence E. Barrett
Chief Information Officer

Joseph P. Loddo
Acting Chief Financial Officer

Bernard Kulik
Associate Administrator for
Disaster Assistance

FROM: John E. Dye
Acting Assistant Inspector General for Auditing

SUBJECT: Audit of SBA's Information Systems Controls

Attached is the Independent Accountant's Audit Report issued by Cotton & Co., CPAs. This report is part of the audit of SBA's FY 1998 Financial Statements pursuant to the Chief Financial Officers Act of 1990. The audit report on the financial statements will be issued separately. As a part of the audit of the financial statements, Cotton & Co. reviewed SBA's general information systems controls to determine if they complied with established policies and procedures. The auditors concluded that SBA's general controls were not fully in compliance with established policies and procedures. For example, (1) SBA had not funded and implemented an entity-wide security program, (2) unnecessary and excessive access privileges reduced accountability and created segregation of duties weaknesses, (3) application development and change control procedures were not consistently applied in systems outside OCIO's control, (4) programmers' abilities to access operating systems could not be monitored, and (5) security administrators and program managers needed training.

The report also includes two recommendations for establishing an ongoing agency-wide information systems security program. The agency response to the draft report stated that your offices will be establishing a committee to work on this issue.

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.**

We request that the Office of the Chief Financial Officer provide the management decisions for the two recommendations in this report. Please provide your proposed management decisions for the recommendations on the attached SBA Forms 1824, Recommendation Action Sheet, within 30 days. If you disagree with a recommendation, please provide your reasons in writing.

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 Victor R. Ruiz, Director, Business Development Programs Group at (202) 205-7204.

Attachments

COTTON & COMPANY
CERTIFIED PUBLIC ACCOUNTANTS, LLP

333 NORTH FAIRFAX STREET • SUITE 401 • ALEXANDRIA, VIRGINIA 22314

COTTON, CPA, CFE
HAYWARD, CPA, CFE

MICHAEL W. GILLESPIE, CPA, CFE
CATHERINE L. NOCERA, CPA

ELLEN P. REED, CPA
MATTHEW H. JOHNSON, CPA

August 26, 1999

Mr. Victor R. Ruiz
U.S. Small Business Administration
Office of Inspector General
409 Third Street, SW
Mail Code 4110
Washington, DC 20416

Dear Mr. Ruiz:

Attached is the summary of results on Areas for Improvement in Computer Controls, Fiscal Year 1998 Financial Statement Audit. Please call if you have questions.

Very truly yours,

COTTON & COMPANY, LLP

By: _____
Matthew H. Johnson, CPA

Enclosure

AREAS FOR IMPROVEMENT IN COMPUTER CONTROLS
FISCAL YEAR 1998 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Cotton & Company, LLP, is engaged in the Fiscal Year (FY) 1998 financial statement audit of the U.S. Small Business Administration (SBA), and will issue an audit report on those statements upon audit completion. The purpose of this report is to communicate the results of general controls testing conducted on SBA's information systems as part of that audit.

BACKGROUND

General controls are the policies and procedures that apply to all or a large segment of an entity's information systems and help ensure their proper operation. They impact the overall effectiveness and security of computer operations rather than specific computer applications. General controls are intended to:

- Ensure that an adequate computer security planning and management program is in place.
- Protect data, files, and programs from unauthorized access, modification, and destruction.
- Prevent the introduction of unauthorized changes to systems and applications software.
- Ensure that the important duties of system and applications software development and maintenance, computer operations, security, and quality assurance are segregated.
- Ensure recovery of computer processing operations in the event of a disaster or other unexpected interruption.

As part of the audit of SBA's FY 1997 financial statements, we recommended improvements in each of those areas. Specifically, we recommended that:

1. The Chief Information Officer (CIO) request (a) priority attention be given to his request for resources to develop and implement the agency-wide security program and (b) interagency agreements and contracts for data processing administered by other program offices are submitted for his review to ensure that security and business continuity issues are addressed.

2. As resources become available, the CIO implement an agency-wide security program and application development standards in accordance with Office of Management and Budget (OMB) Circulars A-123 and A-130.

3. The CIO and Chief Financial Officer (CFO) periodically review programmer access privileges, maintain them at the lowest possible level, and require supervisory review of all emergency program fixes (actual program instructions) within 48 hours.

4. The CIO develop guidance and requirements for SBA program offices to identify incompatible positions and ensure adequate segregation of duties.

The CIO agreed that improvements were needed, but stated the necessary resources were not available. During the course of the FY 1998 audit, we found that while progress had been made, improvements were still needed. The CIO agreed and indicated that the lack of necessary resources placed constraints on the amount of progress that could be made each year. The CIO provided the following statement demonstrating the importance of information systems security:

> Security is going to be a big issue for the 21st century SBA. We expect to receive and disseminate most of our data and information electronically so the people we interact with are going to be very interested in our security from both a policy and operations perspective. The integrity, confidentiality, and availability of information will be the basis of maintaining the trust and confidence of our customers. New and emerging technologies require end-to-end security. Worldwide networks provide access from anywhere in the world and a new generation of highly skilled hackers is developing to exploit the increased use of e-commerce. To be a viable 21st century organization we need to give priority to this area.

SBA'S INFORMATION SYSTEMS ENVIRONMENT

SBA's financial management information systems environment is decentralized. It is comprised of seven components that are operated and maintained by all the SBA offices as well as external contractors. These major components are:

- *(FOIA Deletion)*, a set of mainframe programs that process and maintain the accounting records and provide management reports for SBA's loan programs. The Office of Chief Information Officer (OCIO) is responsible for developing and maintaining the *(FOIA Deletion)* system software and hardware, which is currently operated under contract with SBA by the *(FOIA Deletion)* at its *(FOIA Deletion)*, facility. During the FY 1998 audit period, however, *(FOIA Deletion)*, operated the *(FOIA Deletion)*.

- *(FOIA Deletion)*, a mini-computer system maintained and operated at each of SBA's four Disaster Area Offices. *(FOIA Deletion)* is used to track and process disaster loan applications. After loan approval, it interfaces with *(FOIA Deletion)* to update SBA's loan records. The Office of Disaster Assistance (ODA) operates *(FOIA Deletion)* and is responsible for developing and maintaining system software and hardware.

- *(FOIA Deletion)* , a variety of specialized programs developed and maintained by the Office of the Chief Financial Officer (OCFO). These programs perform various functions such as (1) exchanging data with SBA's business partners, (2) processing and maintaining disbursement and collection records, and (3) interfacing with the *(FOIA Deletion)*.

- *(FOIA Deletion)* , a mainframe financial management system used by all SBA offices for administrative accounting functions. The Department of Treasury's Financial Management Service (FMS), under a contract administered by OCFO, is responsible for software and hardware development and maintenance.

- **Local and Wide-Area Networks (LANs and WANs)**, communications systems maintained and operated by all the SBA offices to (1) provide gateways to *(FOIA Deletion)*, (2) allow the offices to share files and communicate electronically, and (3) transfer data between systems. OCIO develops and disseminates guidance and procedures for the operation of these systems and periodically monitors to ensure compliance.

- *(FOIA Deletion)* , a client server system developed and maintained by OCIO that processes SBG program records and exchanges accounting information with *(FOIA Deletion)*.

- **External Contractor Systems**, various systems developed, maintained, and operated by commercial vendors, such as *(FOIA Deletion)*, for processing and exchanging data related to loan servicing, and fee collections.

As a result of this decentralized environment, OCIO is not directly involved in the general controls over several of the systems that record, process, and report financial and program information.

OBJECTIVE AND METHODOLOGY

As part of the FY 1998 financial statement audit, we reviewed controls over SBA's information systems following the guidance provided in the General Accounting Office's (GAO's) *Federal Information System Control Audit Manual* (FISCAM). The objective was to determine if SBA's entity-wide internal control system complied with established policies and procedures in the following areas:

- **Entity-wide security program planning and management** to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.

- **Access controls** to limit or detect access to computer resources (data, program, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.

- **Application software development and program change controls** to prevent implementation of unauthorized programs or modifications to existing programs.

- **System software controls** to limit and monitor access to powerful programs and sensitive files that (1) control computer hardware and (2) secure applications supported by the system.

- **Segregation of duty controls** to provide policies, procedures, and an organizational structure so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

- **Service continuity controls** to ensure when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected from destruction.

RESULTS

SBA's information systems general controls were not fully in compliance with established policies and procedures. For example, SBA had not funded and implemented an entity-wide security program, unnecessary and excessive access privileges reduced accountability and created segregation of duties weaknesses, application development and change control procedures were not consistently applied in systems outside OCIO control, programmers' ability to access operating systems could not be monitored, and security administrators and program managers needed training. Attachment 1 provides a summary of these results.

1. Entity-Wide Security Program Planning and Management

A comprehensive program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. OMB Circulars A-123 and A-130 require agencies to (1) periodically assess potential risks and controls over sensitive information systems, (2) develop security plans that include a security management structure with clearly defined responsibilities, and (3) perform security awareness training, monitoring, and reporting. The Information Technology Management Reform Act of 1996 (ITMRA), also known as the Clinger Cohen Act, requires CIOs to monitor and evaluate information system performance.

SBA has not demonstrated the senior management commitment, implemented the policies and procedures, or established the organizational structure necessary to meet Congressional and OMB requirements for information systems security. According to the CIO, his office has not been given sufficient funding and staffing to implement a comprehensive information systems security program. In addition, as discussed above, the CIO has only indirect involvement with many of the systems used to record, process, and report financial and program information. Responsibilities for daily information systems activities and security administration are fragmented among all of SBA's field and program offices, without sufficient centralized oversight.

To implement a comprehensive security program, SBA needs to develop, fund, and execute annual security program budgets that ensure the following:

- Periodic risk assessments, reviews of security and application controls, and development of security plans for key business applications.
- Current and comprehensive security policies and procedures.
- Adequately staffed security management structure with clearly defined authorities and responsibilities.
- Implementation of the security awareness training program that has been developed.
- Security monitoring and reporting.
- Senior management oversight program to ensure timely and effective corrective action.
- Comprehensive 5-year strategic information systems plan updated annually as technology and business activities change.

Without a comprehensive security program, SBA has reduced assurance that controls are commensurate with the risks, and that financial records are accurate, complete, and reliable. Further, the risk that fraud or other unauthorized activities will occur and not be detected is increased.

2. Access Controls

OMB Circular A-130 requires agencies to (1) establish and implement effective internal controls, and (2) establish a security administration program to safeguard assets, data, and hardware from unauthorized activities, and assign personnel who have the necessary skills, knowledge, and training to carry out their duties. Additionally, OMB Circular A-127 requires agencies to establish and implement controls over data entry and transaction processing to ensure the validity of the information. The objectives of access controls are to ensure that:

- Users have only the access needed to perform their duties.
- Access to sensitive resources such as security software programs is limited to very few individuals.
- Employees are restricted from performing incompatible functions or functions beyond their responsibility.

The following table summarizes access control requirements and weaknesses related to sensitive, financial, and mission-critical data in the *(FOIA Deletion)* systems.

Access Control Weakness	*(FOIA Deletions)*			
Users have inappropriate access to production data and software.	✔	✔	✔	✔
User passwords *(FOIA Deletion)*.	✔	✔		
Security personnel have unrestricted access to passwords.	✔	✔		
Security personnel do not monitor access rights and privileges.	✔	✔	✔	✔
Users are not automatically prompted to change passwords.	✔		✔	✔
Users have multiple user IDs.	✔		✔	
Security personnel do not have an adequate understanding of system security features.	✔	✔	✔	✔
Security personnel do not have adequate position descriptions.	✔	✔	✔	✔

As a result of these weaknesses, SBA personnel, contractors, and business partners have access to information and functions involving loan applications, financial obligations, collections, disbursements, and write-offs that may (1) be unnecessary, (2) reduce accountability or (3) create segregation of duties problems. This increases the risks of financial loss and misuse of information.

SBA needs to improve its procedures and guidance to security administrators at headquarters and field offices for granting access and privileges within SBA's systems. Procedures that do exist are not consistently applied, in part because security is administered in a decentralized manner by individual offices and the proficiency of the security administrators varies from location to location. Further, SBA does not have standard job descriptions stating required technical skills for security administration positions and has not established and implemented a training program for security personnel.

OCIO was developing a security administration training program, which will be available for users on the intranet. In FY 1999, the OCFO entered into a contract to review the *(FOIA Deletion)* security program and user profiles.

3. Application Software Development and Program Change Control

OMB Circulars A-127 and A-130 require agencies to establish controls that ensure newly developed systems and program changes work as intended and meet user needs. Further, OMB Circular A-127 requires that (1) systems be certified to ensure that adequate controls are built in; (2) systems process information completely, accurately, and reliably; and (3) reliance can be placed on system records.

SBA's System Development Life Cycle and Program Change control procedures were not consistently applied for systems outside the control of OCIO. As a result, program changes and

new systems have been put into production without adequate testing to ensure they work as intended.

For example, SBA outsourced the servicing of one-third of its disaster loan portfolio to a contractor, *(FOIA Deletion)*, before testing the contractor's system. *(FOIA Deletion)* system was unable to process collections in accordance with SBA requirements. As a result, it incorrectly updated SBA's loan accounting records. SBA, in turn, had to correct the data processed by the contractor and reassume responsibility for processing collections.

4. System Software Controls

OMB Circular A-130 requires limiting programmer and system personnel access to operating systems, system utilities, and production data and software. Further, it requires that agencies establish security controls to monitor access and use of powerful operating system utilities.

Access controls to system software need to be established to limit programmers' access. SBA programmers have access to operating system software utilities, thus making the systems vulnerable to unauthorized changes. [

(FOIA Deletion)

]

SBA has not implemented controls to restrict and monitor programmer access to operating systems and utilities. As a result, SBA cannot be assured that programmers are performing only authorized activities.

5. Segregation of Duties

OMB Circular A-130 requires agencies to establish separation of duty controls that allow personnel to perform assigned duties, but prevent or minimize exposures associated with overriding security and internal controls. To help reduce the potential for unauthorized activities, SBA has a "Rule of Two" policy that requires two different people to sign certain documents and approve certain types of transaction. SBA personnel, however, have privileges in *(FOIA Deletion)* that weaken the "Rule of Two" for processing and approving loans, releasing funds, and changing financial records. For instance:

- [*(FOIA Deletion)*]
- [*(FOIA Deletion)*]

Security administrators and supervisory personnel lack understanding of the activities that can be performed with certain privileges, and SBA has not reassessed segregation of duty controls as software and hardware changes occurred. Additionally, SBA has not provided

adequate training to security personnel and program office managers to enable them to determine if segregation of duties is affected by the access privileges granted through various programs.

The lack of adequate segregation of duties increases the potential for unauthorized loan activities to occur and to remain undetected, which could result in financial loss to SBA.

6. Service Continuity Controls

SBA has not implemented disaster recovery or business continuity plans to minimize disruptions in the event of a local or national disaster. As a result, SBA cannot ensure that it will be able to provide Congressionally mandated services to disaster victims and the small business community.

OMB Circular A-130 requires agencies to perform risk assessments of the impact of a local or national disaster or significant disruption to its business operation and to develop disaster recovery and business continuity plans to address risks and minimize the impact.

OCIO began development of a comprehensive disaster recovery and business continuity plan in 1998, and, according to the CIO, SBA has recently allocated funds to finish development and testing of the plan.

Without disaster recovery and business continuity plans, SBA could suffer significant disruptions both locally and nationally to normal business activities, which could cause significant hardship to natural-disaster victims. Additionally, small businesses and lenders would be adversely affected by delays in loan processing and approval and providing guarantees.

RECOMMENDATIONS

We recommend that the SBA Administrator establish a senior management group that, as a minimum, includes the Associate Administrator for Disaster Assistance, Chief Financial Officer, and Chief Information Officer. The group should be responsible for developing and implementing an ongoing, agency-wide information systems security program.

In addition, we recommend that this senior management group develop, fund and execute an annual budget for an ongoing, agency-wide information systems security program that as a minimum includes:

- A multi-year plan and schedule for consolidating security administration duties, conducting risk assessments and control reviews, and preparing security plans for all of SBA's critical information systems.

- Annual training for all SBA employees and contractors on their information system security responsibilities.

- Policies and procedures for security monitoring and reporting for each major system.

- Revision of the position descriptions for personnel with security administration responsibilities to include those responsibilities, as well as appropriate performance measures in their annual performance plans.

- Use of OCIO approved System Development Life Cycle standards and techniques for all new systems, system enhancements, and program changes.

- Quality control measures for all test plans and results for new systems, system enhancements, and program changes to ensure results are documented and that the system works as intended, and test-support documentation is retained.

- Procedures to ensure OCIO review and approval of all agency contracts for information system services, and testing of the systems before they are placed into production.

- Procedures to limit and monitor programmers' access to operating systems, system utilities, application software, and production data.

- Assessment of critical system functions and access controls to identify incompatible duties and enforce SBA's "Rule of Two."

- Completion of the agency's disaster recovery and business continuity plans and local disaster recovery plans, and annual testing of major portions of the plans.

SBA MANAGEMENT COMMENTS

Management agrees to establish a senior management group to develop solutions to the audit findings. Enclosed is the entire response (Attachment 2).

Attachment 1

FY 1998 CFO AUDIT – INFORMATION SYSTEMS CONTROLS REVIEW	**SYSTEM**					
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	*(FOIA Deletions)*					
SECURITY PROGRAM, PLANNING AND MANAGEMENT						
Risks are periodically assessed.	2	2	2	3	2	3
Security program is documented.	2	2	2	2	2	2
Security management structure is in place and responsibilities assigned.	2	2	2	2	2	2
A personnel security policy is established.	2	2	2	2	2	2
A security monitoring program is established.	2	2	2	2	2	3
ACCESS CONTROLS						
Information is properly classified.	1	2	1	1	3	3
User access and privileges are authorized.	2	2	2	2	2	2
Physical and logical controls prevent and detect unauthorized activities.	2	2	1	2	1	3
Apparent unauthorized activities are monitored and investigated.	3	2	2	2	1	3
APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL						
Program modifications are documented, reviewed, tested, and approved.	1	1	4	3	4	3
Program changes are documented, reviewed, tested, and approved before releasing to production.	1	1	4	3	4	3
Movement of programs in and out of libraries is authorized.	1	1	4	3	4	2
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	2	3	2	3	3	4
System access is monitored.	3	3	3	3	3	3
Changes to system are authorized and documented.	1	2	1	2	1	2
SEGREGATION of DUTIES CONTROLS						
Incompatible duties are identified.	2	2	2	3	4	2
Segregation of duties is enforced through access controls.	2	2	2	3	4	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	2	2	2	3	4	2
SERVICE CONTINUITY CONTROLS						
Critical data and resources for recovery and establishment of emergency processing procedures and identified.	2	2	3	2	2	2
Procedures exist for effective backup and offsite storage of data and application and system software.	1	2	2	2	2	2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	1	3	4	2	2	3

LEGEND

1. Control in place and effective. 2. Control in place but not fully effective. 3. Control not in place. 4. Control not tested.

[1] GAO reported that "Information is FMS's systems is at significant risk because of serious general control weaknesses." (GAO/AIMD-99-10, *Financial Management Service: Areas for Improvement in Computer Controls)*

ATTACHMENT 2

SMALL BUSINESS ADMINISTRATION'S RESPONSE

Championing America's Entrepreneurs

DATE: August 18, 1999

TO: Victor Ruiz
Acting Director of Internal Audit

THRU: Fred Hochberg, Deputy Administrator

FROM: Larry Barrett, Chief Information Officer
Bernard Kulik, AA for Disaster Assistance
Joe Loddo, Acting Chief Financial Officer

SUBJECT: Response to FISCAM Audit on Information System Controls

We have reviewed your Federal Information Systems Control Audit Manual (FISCAM) audit report dated August 9, 1999 and have worked together to develop this response to the audit. The SBA will use a new Information Systems Control Committee to address the issue of information system security. This committee will include representatives from our offices and will meet monthly to work on the FISCAM issues in the audit report:

- Entity Wide Security
- Access Controls
- Application Software Development and Change Control
- System Software Controls
- Segregation of Duties Controls
- Service Continuity Controls.

The Information Systems Control Committee will address these issues for the OCIO, ODA and OCFO to develop solutions to the audit findings and to implement the solutions. We invite the Office of the Inspector General to participate along with us to find workable solutions to the findings of the FISCAM audit. The first meeting of the committee will be on September 2nd when we will begin work to develop a detailed plan within 90 days to address each of the FISCAM findings. The plan will include actions required, responsible individuals and timeframes for accomplishing them.

We look forward to working together, along with the OIG, to address this important issue.

REPORT DISTRIBUTION

Recipient	Copies
Administrator	1
Deputy Administrator	1
Associate Deputy Administrator for Management & Administration	1
Associate Administrator for Field Operations	1
Assistant Administrator Office of Congressional & Legislative Affairs	1
Associate Administrator Office of Financial Assistance	1
Chief Financial Officer	1
Chief Information Officer	1
General Counsel	2
General Accounting Office	2