

AUDIT OF SBA'S FY 1999 FINANCIAL STATEMENTS

INFORMATION SYSTEMS CONTROLS

AUDIT REPORT NO. 0-16

APRIL 25, 2000

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**

AUDIT REPORT
Issue Date: April 25, 2000
Report Number: 0-16

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

[FOIA ex. 6]

FROM: Robert G. Seabrooks
Assistant Inspector General for Auditing

SUBJECT: Audit of SBA's Information Systems Controls

Attached is the Independent Accountant's Audit Report on Information Systems Controls, issued by Cotton & Co., LLP. As part of the audit of SBA's FY 1999 financial statements, the auditors reviewed the general controls over SBA's financial management systems to determine if those controls complied with various Federal requirements. General controls are the policies and procedures that apply to all or a large segment of an entity's information systems to help ensure their proper operation. They impact the overall effectiveness and security of computer operations, rather than specific computer applications. Federal requirements for general controls include Office of Management and Budget (OMB) Circular A-130, Security of Federal Automated Information Resources and the Computer Security Act of 1987.

The auditors concluded that SBA has made significant progress toward implementing an agencywide systems security program, but that improvements are still needed. The report describes, for example, how (1) security policies and plans need to be established and implemented; (2) access controls need strengthening to reduce the

risk of unauthorized activities; (3) application development and change control procedures need to be consistently applied; (4) programmers' access to operating systems needs to be controlled and monitored; (5) segregation of duties controls need improvement; and (6) disaster recovery plans need to be completed and tested. The report also includes several recommendations for further implementing the agencywide systems security program.

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 Information Officer provide the management decision for the recommendations in this report. Please provide the proposed management decision on the attached SBA Form 1824, Recommendation Action Sheet, within 30 days. If you disagree with the recommendations, 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 Robert Hultberg Director, Business Development Programs Group at (202) 205- [FOIA ex. 2]

Attachments

COTTON & COMPANY LLP

CERTIFIED PUBLIC ACCOUNTANTS

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

CHARLES HAWARD, CPA, CFE, CISA
MATTHEW H. JOHNSON, CPA, CGFM

DAVID L. COTTON, CPA, CFE, CGFM
NEVILLE W. GILLESPIE, CPA, CFE
SANDRA A. HENLEY, CPA, CGFM

CATHERINE L. NICKERA, CPA
COLETTE Y. WILSON, CPA

February 14, 2000

COMPUTER CONTROLS INDEPENDENT AUDIT OF FISCAL YEAR 1999 FINANCIAL STATEMENTS

Inspector General
U.S. Small Business Administration

We have audited the U.S. Small Business Administration (SBA) principal financial statements as of September 30, 1999, and for the year then ended, and have issued our reports, dated February 14, 2000, to SBA under separate cover. Those reports included our reports on SBA's internal control and compliance with laws and regulations.

The purpose of this letter is to communicate the details of the material weaknesses over SBA's computer controls.

This letter is intended solely for the information and use of the SBA management.

We would like to express our appreciation to the SBA representatives who assisted us in completing our audit. They were always courteous, helpful, and professional.

Very truly yours,

COTTON & COMPANY LLP

By: [FOIA ex. 6]
Matthew H. Johnson, CPA

**AREAS FOR IMPROVEMENT IN COMPUTER CONTROLS
FISCAL YEAR 1999 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION**

Cotton & Company LLP audited the Fiscal Year (FY) 1999 financial statements of the U.S. Small Business Administration (SBA). As part of that audit, we reviewed general controls over SBA's information systems following guidance provided in the General Accounting Office's (GAO's) *Federal Information Systems Control Audit Manual* (FISCAM). The purpose of this report is to communicate the results of that review. Although weaknesses continued to exist, we commend the agency for the substantial progress it has made toward implementing an agency-wide information systems security program.

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. GAO categorizes general controls as follows:

- **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 to prevent one individual from controlling key aspects of computer-related operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records.
- **Service continuity controls** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected from destruction.

SBA'S INFORMATION SYSTEMS ENVIRONMENT

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

- **Loan Accounting System (LAS)**, a set of mainframe programs that process and maintain accounting records and provide management reports for SBA's loan programs. The

Office of the Chief Information Officer (OCIO) is responsible for developing and maintaining LAS system software and hardware. LAS is operated under contract with SBA by the Unisys Corporation at its Eagan, Minnesota, facility.

- **Automated Loan Control System (ALCS)**, a mini-computer system maintained and operated at each of SBA's four Disaster Area Offices. ALCS is used to track and process disaster loan applications. After loan approval, it interfaces with LAS to update SBA's loan records. The Office of Disaster Assistance (ODA) operates ALCS and is responsible for developing and maintaining system software and hardware.
- **Denver Finance Center Systems (DFC)**, 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 LAS.
- **Federal Financial System (FFS)**, 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 LAS, ALCS, and FFS, (2) allow the offices to share files and communicate electronically, and (3) transfer data among systems. OCIO develops and disseminates guidance and procedures for the operation of these systems and periodically monitors to ensure compliance.
- **Surety Bond Guarantee (SBG) System**, a client server system developed and maintained by OCIO that processes SBG program records and exchanges accounting information with FFS.
- **External Contractor Systems**, various systems developed, maintained, and operated by commercial vendors, such as Colson, Inc., and ACS -GSG formerly known as CDSI, for processing and exchanging data related to loan servicing and fee collections.

FY 1999 AUDIT RESULTS

In FY 1999, SBA took several key steps toward implementing an agencywide security program. In response to FY 1998 recommendations, SBA established a senior-management group, provided funding to increase the security administration staff and obtain contractor support, and took the following actions:

- OCIO developed a system Certification & Accreditation (C&A) Handbook and a schedule for conducting C&A reviews, improved guidelines for software development and program change controls, and conducted disaster recovery tests for the Loan Accounting System.
- OCFO conducted a risk assessment of FFS access privileges to reduce exposure and strengthen segregation-of-duty controls, and drafted system development and program change control procedures and a security plan.

- ODA issued new procedures for conducting inventories of existing systems and applications, improved system development controls, and drafted a security plan.

Further work is needed, however, to fully implement the program to meet the requirements of Office of Management and Budget (OMB) Circular A-130, Security of Federal Automated Information Resources; OMB Circular A-123, Management Accountability and Control; and OMB Circular A-127, Financial Management Systems. These circulars incorporate the information system security requirements imposed by the Computer Security Act of 1987, Federal Managers' Financial Integrity Act, Federal Financial Management Improvement Act of 1996, and Paperwork Reduction Act of 1995.

1. Entity-Wide Security Program Planning and Management

A comprehensive program for security planning and management is the foundation of an entity's security controls 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. Although the agency made significant progress, as of the end of FY 1999, several basic requirements had not been met. Specifically:

- Formal agencywide security policies and procedures reflective of the current technological environment had not been established. A draft Standard Operating Procedure for information system security was in clearance, but not yet established as official agency policy.
- Security plans with acceptable risk levels and rules of behavior for each system had not been developed. OCIO planned to develop security plans in conjunction with its C&A reviews.
- Security awareness training was needed. [FOIA ex. 2

].

2. Access Controls

OMB Circular A-130 requires agencies 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 those who need this access to perform their duties.
- Employees are restricted from performing incompatible functions or functions beyond their responsibility.

As summarized in the table below, SBA procedures did not ensure that SBA and contractor personnel had only the access necessary to perform their duties.

Access Control Requirement	LAS	FFS	ALCS
Criteria and guidelines for granting users system access and privileges in the system were adequately defined.	[FOIA ex. 2]		
Users access to production data and software was adequately restricted.			
User passwords were encrypted.			
Security personnel access to users' passwords was restricted. ¹			
Security personnel monitored access rights and privileges.			
Users were automatically prompted to change passwords.			
Accounts were deactivated promptly upon termination of employment or transfer to a position no longer requiring the account.			
Users were restricted to one user ID.			
Security personnel had an adequate understanding of system security features.			
Security personnel position descriptions specified required technical skills.			

N/A = Not Applicable

Other access control issues that we noted included:

- Of 1,819 user accounts in several systems at various offices, 199 users were no longer on staff.
- [FOIA ex. 2]
- [FOIA ex. 2]
- [FOIA ex. 2]

3. Application Software Development and Program Change Control

OMB Circulars A-127 and A-130 require agencies to establish controls to ensure that 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.

¹ SBA management is aware of the risks associated [FOIA ex. 2]

] Further, management contends that compensating controls minimize agency exposure.

During FY 1999, OCIO improved its software development and program change controls to provide reasonable assurance that only approved and tested LAS program changes were implemented. These controls were not in place, however, for other SBA systems. For example, ODA's ALCS controls did not ensure that all program changes were authorized, tested, and reviewed prior to placing the change into production. Additionally, procedures were not developed to ensure that server-based programs developed by and for various field and program offices followed system development and program change control procedures to ensure that the programs work as intended and provide accurate and reliable information for decision making and reporting purposes.

4. System Software Controls

OMB Circular A-130 requires that access to operating systems, system utilities, and production data and software be limited. It also requires that agencies monitor the access and use of powerful operating system utilities. System software controls are intended to provide reasonable assurance that operating-system-based security controls are not compromised and the system will not be impaired.

CFDIA x. 2

3.

5. Segregation-of-Duty Controls

OMB Circular A-130 requires agencies to establish 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 individuals to sign certain documents and approve certain transaction or perform specific transactions within an application.

The FY 1998 audit recommended that SBA enforce the "Rule of Two" by assessing critical system functions and access controls to identify incompatible duties. [FOIA ex. 2]

the following continued in FY 1999:

- [FOIA ex. 2]

].

- [FOIA ex. 2]

].

Lack of training was the primary reason that users were provided with system privileges that nullified the "Rule of Two." Security administrators and supervisory personnel lacked understanding of the activities provided by certain privileges and were not provided system-specific training.

6. Service Continuity Controls

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 impact. In July 1999, OCIO developed a disaster recovery plan in place for LAS that adequately addresses National Institute of Standards and Technology (NIST) requirements. The DFC and Disaster Area Offices had only partial plans in place, and the plans had not been tested. SBA could also suffer significant business disruptions, because FMS did not have a disaster recovery plan for FFS.

CONCLUSION

The control weaknesses in each of these six areas reduce assurance that:

- Financial records are complete, accurate, and reliable.
- Fraud or other unauthorized activities do not occur and remain undetected.
- Only authorized users have access to SBA's systems.
- Only authorized transactions are recorded.
- Only authorized programs and programs changes are implemented.
- Programs and data are adequately safeguarded from computer viruses.
- Individuals cannot control multiple aspects of key operations, such as loan approval, disbursement, and write-off.
- Contingency plans exist to ensure continuous operations.
- Critical and sensitive data are protected from destruction.

RECOMMENDATIONS

We recommend that SBA continue its efforts toward implementing an agency-wide information systems security program, and that it establish responsibilities and milestones to develop and implement policies and procedures to:

- Assign responsibility for security of each major application to a management official knowledgeable in the nature of the program supported by the application.
- Provide annual security training for all SBA employees and contractor personnel on their information system security responsibilities.
- Notify security administrators of changes in the employment status of all personnel and promptly eliminate unnecessary user accounts, and to notify security administrators in advance when personnel are being discharged under adverse conditions.
- Develop a consolidated listing of all user accounts and privileges granted for all SBA employees and contractor personnel.
- Revise position descriptions for personnel with security administration responsibilities to include specific responsibilities, technical requirements, and appropriate performance measures in their annual performance plans.
- Ensure the use of OCIO-approved System Development Life Cycle standards and techniques for all new systems, system enhancements, and program changes.
- Perform quality control for all test plans and results for new systems, system enhancements, and program changes to ensure that results are documented, the system operates as intended, and test-support documentation is retained.
- Limit and monitor programmer access to operating systems, system utilities, application software, and production data.
- Assess critical system functions and access controls to identify incompatible duties and enforce SBA's "Rule of Two."
- Complete the agency's disaster recovery and business continuity plans and perform annual testing of major portions of the plans.
- Obtain approval by senior management and program officials of security plans and risk assessments.

SBA MANAGEMENT COMMENTS

SBA management agreed to address these recommendations and implement solutions to improve information systems controls. A copy of the response is provided as Attachment 2.

FY 1999 CFO AUDIT – INFORMATION SYSTEMS CONTROLS REVIEW	SYSTEM					
	LAS	ALCS	FFS	DFC	LANs & WAN	SBG
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES						
SECURITY PROGRAM, PLANNING AND MANAGEMENT						
Risks are periodically assessed.	2	2	2	2	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	2	4
User access and privileges are authorized.	2	2	2	2	2	4
Physical and logical controls prevent and detect unauthorized activities.	2	2	2	2	2	4
Apparent unauthorized activities are monitored and investigated.	3	3	2	2	2	4
APPLICATION SOFTWARE DEVELOPMENT AND CHANGE CONTROL						
Program modifications are documented, reviewed, tested, and approved.	1	1	2	2	4	2
Program changes are documented, reviewed, tested, and approved before releasing to production.	1	1	2	2	4	2
Movement of programs in and out of libraries is authorized.	2	2	2	2	4	2
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	3	3	2	2	2	2
System access is monitored.	3	3	3	2	2	2
Changes to system are authorized and documented.	2	2	2	2	1	2
SEGREGATION OF DUTIES CONTROLS						
Incompatible duties are identified.	2	2	2	2	2	2
Segregation of duties is enforced through access controls.	2	2	2	2	2	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	2	2	2	2	2	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.	2	2	2	2	2	2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	1	3	3	3	3	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.



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

DATE: APR 19 2000

TO: Robert G. Seabrooks, AIG / Auditing

FROM: Larry Barrett, Chief Information Officer [FOIA ex. 6]
Bernard Kulik, AA for Disaster Assistance [FOIA ex. 6]
Joseph Loddo, Chief Financial Officer [FOIA ex. 6]

SUBJECT: Response to Draft "Audit of SBA's Information System Controls"

We have reviewed the Independent Auditor's FY 1999 draft report on Information System Controls issued by Cotton & Co., LLP (Cotton) and we have worked together to provide this response to the audit. We are pleased to note that Cotton's report recognized the progress that was made by our three offices during FY 1999 on:

- 1) the OCIO Certification and Accreditation review program and disaster recovery tests,
- 2) OCFO review of FFS access privileges and a draft of system development and program change control procedures and a draft security plan; and
- 3) ODAs new procedures for inventories of existing systems and application programs, improved system development controls and a draft security plan.

We also note, however, that Cotton reported that further work is needed to meet federal requirements for information system controls. Specifically, Cotton provided the attached recommendations to improve SBA's information system controls. The SBA is committed to addressing these recommendations during FY 2000 to remove this material internal control weakness from Cotton's future audit reports.

The Information Systems Control Committee that was formed last year will continue to meet to address these recommendations and to implement solutions to improve our information systems controls. As one of its actions, the committee will review and approve the implementation of plans developed by our offices to attain these solutions. We continue to invite the Office of the Inspector General to participate along with us to find workable solutions.

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

Attachment

REPORT DISTRIBUTION

<u>Recipient</u>	<u>Copies</u>
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
General Counsel	2
General Accounting Office	2
