

**AUDIT OF SBA'S
INFORMATION SYSTEMS CONTROLS
FISCAL YEAR 2000
AUDIT REPORT NO. 1-12**

MARCH 27, 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**

AUDIT REPORT

Issue Date: March 27, 2001

Report Number: 1-12

TO: Lawrence E. Barrett
Chief Information Officer

Joseph P. Loddo
Chief Financial Officer

Herbert L. Mitchell
Associate Administrator for Disaster Assistance

Robert G. Seabrooks
FROM: Robert G. Seabrooks
Assistant Inspector General for Auditing

SUBJECT: Audit of SBA's Information Systems Controls – Fiscal Year 2000

Attached is the Independent Accountant's Audit Report on Information Systems Controls, issued by Cotton & Company LLP. As part of the audit of SBA's FY 2000 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 continued to make significant progress in implementing its information systems security program, but that improvements are still needed. The report describes areas where controls can be strengthened, such as (1) monitoring, assessing and measuring security program effectiveness; (2) physical access to network servers; (3) documenting application development; (4) changes to operating system configurations; (5) segregation of duties; and (6) disaster recovery plan testing. The report also provides recommendations for strengthening controls in these areas.

The findings included in this report are the conclusions of the independent auditor and 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) 205-7204.

Attachments

COTTON & COMPANY LLP

CERTIFIED PUBLIC ACCOUNTANTS

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

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

DAVID L. COTTON, CPA, CFE, CGFM
MICHAEL W. GILLESPIE, CPA, CFE
SAM HADLEY, CPA, CGFM

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

February 23, 2001

AREAS FOR IMPROVEMENT IN COMPUTER CONTROLS FISCAL YEAR 2000 FINANCIAL STATEMENT AUDIT U.S. SMALL BUSINESS ADMINISTRATION

Inspector General
U.S. Small Business Administration

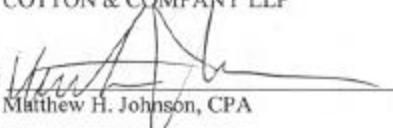
Cotton & Company LLP audited the U.S. Small Business Administration's (SBA) principal financial statements as of September 30, 2000, and 1999, and for the year then ended. The audit included a review of SBA's information system controls. The purpose of this letter is to communicate the audit results and recommendations for improvement.

This letter is intended solely for the information and use of 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: 
Matthew H. Johnson, CPA

**AREAS FOR IMPROVEMENT IN COMPUTER CONTROLS
FISCAL YEAR 2000 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION**

Cotton & Company LLP audited the Fiscal Year (FY) 2000 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 and make recommendations for improvements. Although weaknesses continue to exist, we commend the agency for the substantial progress it has made toward implementing an agency-wide information systems internal control program. Because of this progress, we no longer consider this area to be a material weakness.

BACKGROUND

General controls are the policies, procedures, and practices 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. GAO categorizes general controls as follows:

- **Entity-wide security program controls** 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 control computer hardware and 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 system environment is decentralized. It is comprised of six major components operated and maintained by all SBA offices and external contractors, as described below.

- **Loan Accounting System (LAS)**, a set of mainframe programs that processes and maintains accounting records and provides 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 tracks and processes 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 LAS.
- **Federal Financial System (FFS)**, a mainframe financial management system used by all SBA offices for administrative accounting functions. The Department of the 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 offices to share files and communicate electronically, (3) transfer data among systems, and (4) provide Internet access. 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.

In addition, SBA's financial management activities rely on systems developed, maintained, and operated by external parties such as Colson, Inc., ACS-GSG (formerly known as CDSI) and the National Finance Center, for processing and exchanging data related to functions such as loan servicing and payroll.

FY 2000 AUDIT RESULTS

During FY 2000, SBA significantly improved internal control over its information system environment. Specifically, it accomplished the following:

- For each major application, assigned a security manager knowledgeable in the program supported by the application.
- Conducted certification and accreditation reviews of each major application, the network, and mainframe computer.
- Implemented an online security awareness training program to instruct SBA employees and contractors on their information system security responsibilities; employees and contractors are required to complete this program annually.
- Developed procedures to notify security personnel of changes in employee status and system access requirements.
- Developed position descriptions for security administration personnel that include specific responsibilities and technical requirements.
- Adopted a System Development Methodology to improve control over new system development, system enhancements, and program changes.
- Developed quality control procedures and practices for documenting test plans and results for new systems, system enhancements, and program changes.
- Reduced programmer access to operating systems, system utilities, application software, and production data and implemented procedures to monitor programmer access.
- Developed and implemented procedures and practices to assess (1) critical system functions and (2) controls to identify incompatible duties and enforce SBA's "Rule of Two."
- Completed development of disaster recovery and business continuity plans.
- Developed procedures for reviewing and approving security plans and risk assessments as part of the certification and accreditation process.

These actions are essential elements for a sound information system control environment. Areas for improvements do, however, continue to exist in the six FISCAM categories. In the remainder of this report, we discuss these areas and present our recommendations for improvements.

Attachment 1 provides an overall summary of the audit results. Ratings were assigned to each of the six major system groups and general control techniques. For controls rated "1," SBA

has implemented adequate policies, procedures and practices. For controls rated “2*,” controls had been recently implemented, but insufficient time had passed for the controls’ effectiveness to be fully evaluated. For controls rated “2,” controls were in place, they but had not been fully implemented, e.g. personnel responsible for implementing the control did not possess the necessary knowledge or experience, the control’s effectiveness was reduced by weaknesses in other areas, or the control was only partially integrated into the related business processes.

1. Entity-Wide Security Program Controls

SBA has developed an entity-wide security program that provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls. SBA has not, however, achieved full implementation of this program. During our audit, we noted four conditions that weaken the overall information system control environment.

The most significant of those conditions involves security monitoring. OCIO has not fully implemented procedures and processes for carrying out security monitoring functions, activities, and responsibilities. This includes developing criteria for measuring security program effectiveness and reporting results to senior management. OCIO’s current procedures and processes do not comply with GAO’s Internal Control Standards for ongoing monitoring in the course of normal operations.

Further, the procedures do not ensure that identified deficiencies and recommendations are promptly reviewed, and corrective actions are implemented in a timely manner. For instance, control deficiencies identified in June 2000 accreditation and certification reviews had not been addressed as of December 2000.

The other three conditions related to the entity-wide security program are:

- Network and application security administrators are not knowledgeable of security controls necessary to assess user requests for privileges or perform routine housekeeping actions.
- OCIO’s strategic information resources management plan does not fully reflect the information technology initiatives currently underway or planned, and does not include a summary of the security plans as required by OMB Circular A-130.
- Roles and responsibilities between the OCIO, the Office of Human Resources and SBA program offices are not clearly defined as they relate to items such as (1) notifying security administrators of changes to SBA employee and contractor employment status, (2) identifying sensitive positions and the need to access sensitive information, and (3) obtaining confidentiality and conflict-of-interest statements.

Without full implementation of the entity-wide security program, the overall effectiveness of the program is diminished.

Recommendations:

We recommend that the Chief Information Officer, in conjunction with the appropriate program offices:

- 1A. Develop and implement procedures for monitoring, assessing, and measuring security program effectiveness.
- 1B. Provide training and annual retraining for network and application security administrators to enable them to understand security controls necessary to assess user requests and perform routine housekeeping actions.
- 1C. Ensure that SBA's strategic plan is updated annually to reflect the approved information technology plan and initiatives and include a summary of the security plans.
- 1D. Clearly define and document roles and responsibilities of OCIO, the Office of Human Resources and SBA program offices as they relate to notifying security administrators of changes to SBA employee and contractor employment status, identifying sensitive positions and the need to access sensitive information, and obtaining confidentiality and conflict-of-interest statements.

2. Access Controls

Physical and logical access controls are designed to protect an agency's assets against unauthorized modification, loss, and disclosure. SBA has made significant and important improvements in its controls to limit or detect access to its computer resources. We noted, however, three specific areas in which access controls could be improved:

- Although physical safeguards for the majority of SBA's network servers are adequate, for some servers these safeguards can be improved. For example, a number of network servers are located in a room with an electronic door lock; the locks are not, however, connected to a backup power supply and, as such, deactivate during power outages. Also, we noted other network servers left unattended and unsecured, and, at one location, the network server was located within the main work area of an office.
- Universal network accounts with both local and wide area network privileges were not properly secured with a password.
- User passwords were not always configured for the minimum length of 8 characters and were not changed every 90 days. In addition, some user accounts permitted an unlimited number of failed log-on attempts.

OMB A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Systems*, requires agencies to establish physical security commensurate with the risk and magnitude of the potential resulting harm. Further, SBA's

Standard Operating Procedure (SOP) 90-47, *Automated Information System Security Programs*, specifies controls applicable to user passwords and log-on attempts.

SBA has sound policies and procedures over access to its various systems; however, many of the individuals responsible for controlling access are not trained sufficiently to ensure that these policies and procedures are implemented and carried out as designed. As a result, SBA's ability to control or detect access to computer resources is limited.

Recommendations:

We recommend that the Chief Information Officer, in conjunction with appropriate program offices:

- 2A. Develop and implement procedures to ensure the physical security of network servers at all times including during power outages.
- 2B. Establish monitoring procedures for periodic tests of local networks and applications to ensure that user accounts are properly established and comply with SBA's standards.

3. Application Software Development and Program Change Control

SBA's application software development and program change controls need to be improved to prevent implementation of unauthorized programs or modifications to existing programs. We noted that documentation for system and program changes was outdated, and documentation supporting tests of program changes was inadequate. Specifically, we found that user and programmer test plans and results are not documented to demonstrate that programs are properly tested and approved prior to being placed in operation.

OCIO requires basic documents for all systems, including user requirements, design documents, test plans, implementation, and acceptance documents. It also requires retention of User Request Forms that detail program changes; these forms are required to be signed by the programmer and the user to acknowledge acceptance of the change. Compliance is not enforced, because control procedures do not exist to ensure that documentation is being updated and maintained.

Not properly documenting system and program changes increases the risk that SBA personnel using an application and relying upon the results will not be knowledgeable enough about the program to identify errors. Additionally, programmers may be relying upon outdated and inaccurate program information if documentation is incorrect.

Recommendation:

We recommend that the Chief Information Officer:

- 3A. Develop quality control program procedures to periodically review existing applications to assure that documentation is kept current and accurately reflects the cumulative affects of program changes made over time.

4. System Software Controls

Properly designed system software controls limit and monitor access to programs and files that control computer hardware and secure applications. SBA has adequate system software controls. We did, however, identify instances where controls need to be improved. For example, we found that SBA's local area network servers are not standardized, and monitoring procedures are not in place to ensure that changes to servers are approved, consistent among offices, and compatible with existing network protocols as required by Federal Information Processing Standards. Local area network administrators do not consult or seek approval prior to implementing changes to the network servers, thereby increasing the risk that inappropriate software changes are made, data are corrupted, and sensitive data are modified or released to unauthorized individuals.

Recommendations:

We recommend that the Chief Information Officer:

- 4A. Develop procedures to require review and approval of all proposed changes to server configurations.

5. Segregation-of-Duty Controls

SBA generally has appropriate segregation of duties throughout its information system environment; individuals generally do not have the ability to conduct unauthorized actions or gain unauthorized access to assets or records. We did, however, identify some instances of inadequate segregation of duties. For example, one individual at a field office was the security officer for LAS, a senior loan officer on LAS, and had supervisory privileges on the Field Cashiering System.

OMB Circular A-130, Appendix III, requires agencies to establish and implement controls within the general control environment and major applications that support the "Least Privilege" practice. Also, OMB requires establishing and implementing practices to divide steps of critical functions among different individuals and establishing practices to keep a single individual from subverting a critical process.

Inadequate segregation of duties resulted from workforce changes, which required reassignments without regard or knowledge of their impact. Where we did identify inappropriate segregation of duties, however, SBA management took immediate actions to eliminate the incompatible duties. Improper segregation of duties increases the risk of unauthorized activities and may result in a loss of funds.

Recommendation:

We recommend that the Chief Information Officer, in conjunction with the appropriate program offices:

- 5A. Continue its efforts to identify and eliminate incompatible duties, responsibilities, and functions.

6. Service Continuity Controls

Properly designed service continuity controls ensure that operations continue uninterrupted when unexpected events occur. We noted two conditions that, if improved, will enhance SBA's ability to ensure such uninterrupted operations:

- SBA has not tested its non-mainframe computer contingency plans.
- SBA does not properly store offsite its backup and recovery tapes for network data, files, and software.

OMB Circular A-130, Appendix III, requires agencies to develop, implement, and test contingency plans and to properly secure and protect backup and recovery tapes.

SBA has not completed its contingency plans and has not made arrangements for offsite storage of backup and recovery tapes. The agency is continuing to develop contingency plans and is reviewing a contract proposal for offsite storage.

Without contingency plan testing, SBA has reduced assurance that the plans adequately address contingencies and provide an orderly and reasonable recovery process. Improper storage of backup and recovery tapes may increase recovery time and increase the potential for improper release, theft, and destruction of information and tapes.

Recommendations:

We recommend that the Chief Information Officer, in conjunction with the appropriate program offices:

- 6A. Develop a contingency test plan and schedule.
- 6B. Expedite its review and establish standard procedures for storing backup and recovery tapes. As an interim procedure, permit offices to store backup and recovery tapes in a bank safety deposit box.

MANAGEMENT RESPONSE

In response to a draft of this report, SBA management generally agreed with the findings and recommendations, but expressed concern about the report's lack of support for our assessments of controls. Management also disagreed with several of the ratings in Attachment 1, and expressed concern that the ratings may give a false impression of the state of SBA's security program. A copy of management's response is provided as Attachment 2.

EVALUATION OF MANAGEMENT RESPONSE

We agree with management that the draft report did not contain details supporting all the ratings provided in Attachment 1. It was not our intention to provide such details in the report, but rather to communicate our overall assessment of controls and provide general information about areas for improvement – with details to be provided separately. Some of the details supporting our assessments are sensitive and inappropriate for inclusion in a report that will be made public.

We met with management representatives and provided them additional details to support the ratings in Attachment 1. We also modified the report to clarify our assessments and address other issues raised in management's response.

<i>FY 2000 CFO AUDIT – INFORMATION SYSTEMS CONTROL REVIEW</i>	SYSTEM					
	LAS	ALCS	FFS	DFC	LANs & WAN	SBG
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES						
ENTITY- WIDE SECURITY PROGRAM CONTROLS						
Risks are periodically assessed.	1	1	1	1	1	1
Security program is documented.	1	1	1	1	1	1
Security management structure is in place and responsibilities assigned.	1	1	1	1	2	2
A personnel security policy is established.	1	1	1	1	1	1
A security-monitoring program is established.	2	2	2	2	2	2
ACCESS CONTROLS						
Information is properly classified.	1	1	1	1	1	1
User access and privileges are authorized.	2	2*	2*	2*	2*	2*
Physical and logical controls prevent and detect unauthorized activities.	2	2	2*	2*	1	2
Apparent unauthorized activities are monitored and investigated.	2	2	2*	2*	1	2
APPLICATION SOFTWARE DEVELOPMENT AND PROGRAM CHANGE CONTROLS						
Program modifications are documented, reviewed, tested, and approved.	1	1	4	1	4	2
Program changes are documented, reviewed, tested, and approved before releasing to production.	1	1	4	1	4	2
Movement of programs in and out of libraries is authorized.	1	1	4	1	4	2*
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	2	2	4	1	1	1
System access is monitored.	2	2	4	1	1	1
Changes to system are authorized and documented.	1	1	1	1	1	1
SEGREGATION OF DUTIES CONTROLS						
Incompatible duties are identified.	1	1	1	1	1	1
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 are identified.	1	1	1	1	1	1
Procedures exist for effective backup and offsite storage of data and application and system software.	1	2	1	1	2	2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	1	2	2	2	2	2

LEGEND

1 – Control in place. 2 - Control in place, but not fully implemented. 2* - Recently implemented control, not fully evaluated.
3 – Control not in place. 4 - Control not applicable.



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

Attachment 2

Date: March 16, 2001

To: Robert G. Seabrooks, Assistant Inspector General for Audit

From: Lawrence E. Barrett, Chief Information Officer 

Subject: Audit of SBA's Information Systems Controls - FY 2000

The Office of the Chief Information Officer, Office of the Chief Financial Officer and the Office of Disaster Assistance have reviewed the draft audit report on SBA's Information Systems Controls issued by Cotton & Company LLP as part of the audit of SBA's FY 2000 financial statements. Although we generally agree with the findings and recommendations in the report, we do have several issues that are addressed in the attached responses.

One concern that we have is the lack of support for the ratings provided in Attachment I of the draft report. The chart should be supplemented by a discussion of the factors considered for the ratings assigned, that we could then use to improve our offices information system controls. We disagree with several of the ratings in the chart, as identified in the response narrative. We believe that the absence of criteria, an explanation, or supporting documentation for the ratings may give the reader a false impression of the state of SBA's IT security program.

Also, included in the attached responses are several issues related to the findings and recommendations. You will note that we partially agree in some cases to the recommendations in the report. Also, we disagree in one instance, to a finding on the lack of configuration standards, as the issue is really conformance with the existing standard.

Representatives from our three offices are available to discuss our comments at your convenience. We look forward to hearing from you.

If you require additional information, please contact me on 205-6708.

Attachment

cc: Joseph P. Loddo, Chief Financial Officer
Herbert L. Mitchell, Associate Administrator for Disaster Assistance
Kristine Marcy, Chief Operating Officer



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