REDACTED FOR FOIA

AUDIT OF SBA'S INFORMATION SYSTEMS CONTROLS FISCAL YEAR 2001 AUDIT REPORT NUMBER 2-18

MAY 6, 2002

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

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

AUDIT REPORT
Issue Date: May 6, 2002
Number: 2-18

To: Lloyd A. Blanchard, Chief Operating Officer

Lawrence E. Barrett, Chief Information Officer

Herbert L. Mitchell, Associate Administrator for Disaster Assistance

Robert G Seabrook

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

Subject: Audit of SBA's Information Systems Controls

Attached is the audit report on SBA's Information Systems Controls issued by Cotton & Company LLP as part of the audit of SBA's FY 2001 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. General controls 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 Circular A-130, Security of Federal Automated Information Resources and the Computer Security Act of 1987.

The auditors concluded that SBA continued to make 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) entity-wide security program controls, (2) access controls, (3) application software development and program change controls, (4) system software controls, (5) segregation of duty controls, (6) service continuity controls, and (7) review of mainframe operations. The report also provides recommendations for strengthening controls in these areas.

The findings in this report are based on the auditors' conclusions and the report recommendations are subject to review, management decision and action by your office, in accordance with existing Agency procedures for follow-up and resolution. Please provide us your proposed management decisions within 30 days on the attached SBA Forms 1824, Recommendation Action Sheet. If you disagree with the recommendations, please provide your reasons in writing.

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

Attachments

COTTON & COMPANY LLP

auditors ◆ advisors

David L. Cotton, CPA, CFE, CGFM ◆ Charles Hayward, CPA, CFE, CISA ◆ Michael W. Gillespie, CPA, CFE ◆ Catherine L. Nocera, CPA
Matthew H. Johnson, CPA, CGFM ◆ Sam Hadley, CPA, CGFM ◆ Colette Y. Wilson, CPA

February 20, 2002

AREAS FOR IMPROVEMENT IN COMPUTER CONTROLS
FISCAL YEAR 2001 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Inspector General
U.S. Small Business Administration

We have audited the Balance Sheets of the U.S. Small Business Administration (SBA) as of September 30, 2001, and 2000, and the related Statements of Net Cost for the years then ended; we have also audited the related Statements of Changes in Net Position, Budgetary Resources, and Financing for the year ended September 30, 2001. We have issued our report thereon dated February 20, 2002. The audits 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 2001 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Cotton & Company LLP audited the Fiscal Year (FY) 2001 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) *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. The control weaknesses discussed in this report have been reported in the SBA's FY 2001 financial statement audit as reportable conditions.

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** 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** 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** prevent implementation of unauthorized programs or modifications to existing programs.

- **System software controls** 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** 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** 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 SBA offices and external contractors, as described below.

1. **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 a third-party vendor at its Eagan, Minnesota, facility.

2. **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.

3. **Denver Finance Center (DFC) Systems**, a variety of specialized programs developed and maintained by the Office of the Chief Financial Officer (OCFO). These programs perform various functions such as exchanging data with SBA's business partners, processing and maintaining disbursement and collection records, and interfacing with LAS.

4. **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. On October 1, 2001, SBA discontinued use of FFS and implemented the Joint Administrative Accounting Management System ($JA^2 MS$). JA^2MS, an Oracle-based client-server system, will be the financial system for the agency starting in FY 2002.

5. **Local and Wide-Area Networks (LANs and WANs)**, communications systems maintained and operated by all the SBA offices. LANs and WANs provide gateways to LAS, ALCS, and FFS; allow offices to share files and communicate electronically; transfer data among systems; and provide Internet access. OCIO develops and disseminates guidance and procedures for the operation of these systems and periodically monitors to ensure compliance.

6. **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 Services Corporation; ACS-GSG; and the National Finance Center for processing and exchanging data related to functions such as loan servicing and payroll. SBA also has acquired lock-box banking services from Bank of America and other non-continental domestic banks for processing checks on borrowers' loan payments. This information is provided electronically to DFC.

FY 2001 AUDIT RESULTS

During FY 2001, SBA continued to improve internal control over its information system environment in certain areas. Specifically, it accomplished the following:

- Conducted certification and accreditation reviews for additional major applications.
- Continued implementation of an online security awareness-training program to instruct SBA employees in proper computer-security procedures.
- Continued implementation of a System Development Lifecycle Methodology to improve control over new system development, system enhancements, and program changes.

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. Audit results are summarized in Attachment 1.

1. Entity-Wide Security Program Controls

SBA's Standard Operating Procedure 90-47, *Automated Information Systems Security Program*, provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls. During our audit, however, we noted six conditions that weaken the overall information system control environment. The most significant of these, Item A below, involves security monitoring.

A. Controls are not in place to monitor the effectiveness of SBA's information system security program in meeting the established goals and objectives of safeguarding and securing the agency's assets and complying with federal laws and regulations. In FY 2001, OCIO established goals and performance measures for FY 2002 Information Technology (IT) projects; however, with the exception of developing a disaster resumption business plan, the goals, expectations, and performance factors were not in place to monitor and measure the security program's effectiveness and efficiency. The Chief Operating Officer (COO) has not developed processes and procedures to measure the effectiveness of OCIO's implementation of SBA's security program. On March 21, 2002, SBA released the Automated Information Systems Security Program Draft Security Program Evaluation Metrics. While this does address the goals and performance of the Security Program, it was not in place during FY 2001.

B. OCIO does not have a current information system strategic and operational plan. OCIO, however, did have an Information Technology Infrastructure and Architecture Plan that contains most of the requirements required by OMB A-130 Appendix III.

C. SBA has not developed an agency-wide integrated security plan for implementing and integrating SOP requirements into OCIO's security program as required by Section 5.8.1 of SBA's FY 2000 Information Technology Architecture Plan.

D. SBA does not obtain signed non-disclosure agreements from SBA and contractor personnel who handle sensitive data.

E. SBA's Office of Human Resources (OHR) has not defined personnel consequences for non-compliance with security policies and procedures and "rules of behavior."

F. OCIO has not developed and provided technical training for personnel performing security administration activities either at the network or application level. See Section 2, Access Controls, for further discussion and recommendations.

OMB Circular A-130, *Management of Federal Information Resources,* Section 8, requires agencies to develop an integrated information system plan for resource allocation and use, including budgeting, acquisition, and use of IT. Further, Section 9 requires agencies to develop and maintain an up-to-date 5-year strategic information resources management plan.

Furthermore, OMB Circular A-130, *Security of Federal Automated Information Resources*, Appendix III, requires agencies to implement a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Appendix III also requires agencies to develop and implement adequate management controls that monitor and measure the effectiveness and efficiency of the information system security program and ensure that established controls are commensurate with the acceptable level of risk for the system.

Without full implementation of the entity-wide security program, overall program effectiveness is diminished. In addition, without proper monitoring of the security program and functions within the agency, program effectiveness and assurance that all laws and regulations are being met is reduced.

Recommendations

We recommend that the Chief Operating Officer, in conjunction with OCIO, OHR, and appropriate program offices:

1A. Enhance:

- Performance measures for OCIO, to include specific security goals and objectives derived from SBA's Five Year Strategic Plan, Annual Performance Plan, and business plan.

- Procedures to monitor and measure OCIO accomplishments in achieving performance goals and objectives.

1B. Develop and implement procedures for:

- A 5-year Information Technology (IT) strategic and operational plan incorporating SBA's Information Technology Infrastructure Plan, to fully integrate and support SBA's business plan, objectives, and goals.

- Adequately identifying the financial requirements and commitment necessary to implement the agreed-upon information technology solution contained in the plan that supports SBA's business plan, objectives, and goals.

- Ensuring that the IT plan is updated annually.

1C. Develop an agency-wide security plan, as recommended in Section 5.8 of SBA's Information Technology Architecture Plan, to establish and implement the policies, procedures, and practices for the following:

- Full integration of the information security approach and implementation process, along with key milestones for implementing the program.

- Coordination among program offices to support their security needs.

- Guidance to the program office for effective implementation of information system security controls.

- Methods to monitor the effectiveness of each part of the IT security assigned to each program office.

We recommend that Chief Information Officer in conjunction with the Office of Human Resources:

1D. Develop personnel policies and procedures consistent with and in support of the defined "rules of behavior" for general support systems and major applications, to include the consequences for personnel non-compliance with the security policy and "rules of behavior." These consequences may include written reprimands, suspension, leave-without-pay, and termination. Additionally, SBA should incorporate these "rules of behavior" in SOP 90-47.

1E. Develop both a non-disclosure and a security awareness agreement that agency and contractor personnel will be required to sign. The non-disclosure agreement should include a statement such as:

> The individual acknowledges that as part of normal duties, SBA has granted the individual access to sensitive agency and personal information. The individual agrees not to disclose this information to any individual outside the agency without obtaining the SBA's written permission.

The security awareness agreement should include:

- A statement that an individual has been made aware of the security policy and the consequences for non-compliance with the policy.
- A statement that the individual understands the security policy and consequences.
- A requirement for personnel to sign the statement annually.

2. Access Controls

Physical and logical access controls are designed to protect an agency's assets against unauthorized modification, loss, destruction, and disclosure. During the FY 2001 controls review, the audit team performed external and internal intrusion testing to test the network and application access controls.

During the internal intrusion test, we were able to gain administrative access to several servers residing on the network, including one of the backup domain controllers, which allowed us to obtain network administrator capabilities. This was accomplished, because a network administrator had not password-protected a remote access path. This open path would allow an intruder to assume control of the network or install software for monitoring, capturing, and modifying information crossing through the network. By obtaining the network administrator's account privileges, we were able to obtain the network user account password file and de-encrypt user account passwords for all SBA headquarters (HQ) users. In conducting this test, we also found that many SBA and contractor personnel are using easily guessed passwords, such as "PASSWORD," and passwords that do not conform to requirements, such as "MMMMMMMM." The failure of personnel to use effective and appropriate passwords weakens security control effectiveness. OCIO states that with the implementation of Windows 2000 agency wide in August of 2002, proper security settings and administration will be performed more effectively and efficiently.

We noted the following additional conditions in the area of access controls:

A. System administrators (network and LAS) at SBA field offices are not effectively carrying out their duties and responsibilities. Additionally, OCIO had not established a method to monitor the field offices' security activities. For instance, at the field offices we visited during the audit, we found that:

- LAS security administrators at some offices are providing all users with the same privileges.
- Some LAS user account privileges are excessive.
- Server security settings are not always configured correctly.
- Network user accounts were not properly setup or monitored.
- Not all network accounts were required to use a password.
- Not all network accounts required that account passwords be changed once every 90 days.
- Administrators did not set all accounts to lock out or disable the accounts after three failed login attempts.

B. Although OCIO and OHR have developed undocumented procedures for informing security personnel of staff separations, we found the controls were not effective, because user accounts on HQ network servers, LAS, the Field Cashiering System, Sybase systems (SBG and Microloan processing), and the Sybase security module belonged to individuals no longer employed by or under contract to SBA.

C. LAS security software module continues to permit the field office LAS security officer to view each user's password in the clear, thereby violating the security requirement to ensure that only the user has knowledge of the password.

D. LAS screen SSDD04, which allows LAS users to change their own passwords, was not widely known or used by SBA employees.

E. SBA employees are not complying with security policy and standards that require unattended workstations to be properly secured by installing a password-protected screen-saver.

OMB Circular A-130, Appendix III, requires agencies to establish physical security commensurate with the risk and magnitude of the potential resulting harm. SBA's SOP 90-47 specifies controls applicable to user passwords and log-on attempts.

Furthermore, National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 112, *Password Usage*, provides guidance on proper password configuration. Minimum password length is eight alpha and numeric characters, and passwords must be stored in an encrypted format.

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 access to computer resources is limited. This can lead to unauthorized access, modification, release, or destruction of SBA mission-critical and sensitive information.

Recommendations

We recommend that the Chief Operating Officer:

2A. Provide adequate funding and resources to allow OCIO to develop and implement technical training for security staff and all network and application security administrators.

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

2B. Develop and implement standard operating procedures for network system and security administrators that provide adequate guidance, describe procedures for maintaining the network and other system accounts, and ensure that accounts belong only to authorized individuals. These procedures should:

- Provide guidance and technical training opportunities for all network and application security administrators describing expected duties and supporting successful performance of these duties.
- Require spot checks of field office servers for compliance with established rules.
- Conduct physical security reviews of workstations.

2C. Document and enhance procedures to ensure that:

- OHR provides OCIO with timely separation reports.
- Security administrators are reviewing separation listings and deleting/deactivating accounts immediately.
- Each COTR informs the security group and appropriate security administrators when contractors no longer require access to SBA applications and the network.

2D. Make necessary program changes to the LAS security module to:

- Prevent the LAS security administrator from viewing passwords in plain text.
- Enable the administrator to re-set user passwords.

2E. Re-issue a procedural notice that requires offices to have users change their own passwords through the use of security screen SSDD04.

2F. Obtain security software for periodically de-encrypting and testing user network passwords for compliance with SBA's password policy.

3. Application Software Development and Program Change Control

SBA's application software development and program change controls are designed 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 documented, reviewed, tested, and approved before being placed in operation. Specifically:

A. Although members of the OCIO security team were involved during JAAMS development, the security team was not involved throughout the entire process. The team did not participate in the planning phase of the project or the final user-acceptance testing and system implementation. Documentation of involvement consisted of e-mails and a limited number of memorandums. OCIO did not develop a plan to identify and guide its participation during the JAAMS development. Additionally, OCIO did not develop procedures to ensure that actions were taken in a timely manner. The Information Technology Architectural Plan, Section 4.4.1, Application Architecture Design Principles, and Section 5.4, Application Architecture, require that applications be designed and developed to incorporate IT security policies at the beginning and throughout the System Development Life Cycle (SDLC). We noted that OCIO did perform a Certification and Accreditation review during the implementation phase of the project.

B. Program changes to the SBG system were not recorded in the tracking list of program changes, even though individual documentation was available.

C. SBA Office of Disaster Assistance (ODA) programmers have unrestricted access to the Loan Officer Report (LOR) software and independently placed the software into production.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing IT,* provides guidance for developing procedures and processes to control system development and program changes. Additionally, GAO's *Standards for Internal Control In the Federal Government* requires agencies to adopt application controls to ensure that program changes are documented, reviewed, tested, and approved before a program is placed into production, thus obtaining assurance a program operates as intended.

Improper and inadequate system and program change documentation increases the risk that:

- Programming errors will not be detected, thus causing management to rely on erroneous accounting and financial information for decision-making purposes.
- Programmers may be relying upon outdated, inaccurate, or omitted programming information to properly maintain the system.

By failing to properly document, test, and approve program changes, management increases the risk that unwanted, erroneous, or malicious code might be introduced into the production environment, resulting in the unauthorized modification, destruction, or release of SBA data. Additionally, lack of involvement by the security team in all system development project phases may result in the incurrence of increased costs for additional software development to correct security controls.

Recommendations

We recommend that the Chief Information Officer:

3A. Enhance system development procedures to ensure that security personnel actively participate in all phases of system development for new systems and enhancements to existing systems, and require security personnel to sign off as having reviewed and approved security controls.

3B. Enhance configuration management procedures to modify the user request form to include a check-off block indicating that the program tracking system has been updated for the program change.

We recommend that the Associate Administrator for Disaster Assistance:

3C. Develop and implement software development and program change procedures and processes that incorporate OCIO standards.

3D. Restrict Disaster Area Office development programmer access to the production environment and preclude programmers from independently installing new software.

4. System Software Controls

Properly designed system software controls limit and monitor access to programs and files that control computer hardware and protect applications. Our analysis of SBA's network identified security control weaknesses with the network operating system that impact the adequacy of control to protect network operations from unauthorized activities from internal sources. For this audit, we have included the network and intrusion detection software (IDS) in the area of system software. We tested the IDS for its effectiveness to identify inappropriate and malicious activity.

Although OCIO has practices for the installation of recommended operating software and hardware fixes and patches for known security vulnerabilities, our tests showed that these practices were not being consistently carried out. Thus, an individual with malicious intent could have exploited known software security vulnerabilities to gain access to network administrator accounts and obtain powerful administrative privileges and tools. With these privileges and tools, an individual with malicious intent could have gained access to applications and software residing on network operating system software.

A. While conducting our internal and external tests over several weeks, OCIO's network intrusion detection software did identify scans coming from the internal CyberCop software. It did not, however, detect external CyberCop scans and common hacking activities originating from external and internal sources being used to conduct intrusion testing. Ineffective software monitoring tools impair the ability to detect unusual activities on the network and provide an intruder with opportunity and time to gain unauthorized access to sensitive and highly privileged accounts. The result could be unauthorized modification, destruction, or release of SBA data.

B. During our physical security test of SBA workstations, we identified a software glitch with the Windows 95 operating system and Outlook 97 that prevented the password-protected screen-saver from activating. This allowed the tester to gain access to a user's workstation hard drive, network account, and shared drives. Although screen-savers were installed to activate after 10 minutes of inactivity, the Windows Outlook email application interfered with screen-saver software. OCIO stated that the screen-saver glitch will be resolved through the full implementation of Windows 2000 on the network and workstations.

OMB Circular A-130, Appendix III, requires agencies to establish and implement adequate technical security controls to secure and safeguard data, software, and hardware from theft, misuse, alteration, and unauthorized access.

Recommendations

We recommend that the Chief Information Officer:

4A. Develop and implement policies and procedures to ensure that network administration personnel apply vendor operating system patches and fixes to network resources as soon as the vendor releases the patches.

4B. Develop procedures to review and assess the technical compatibility of new software with existing operating systems and other applications residing on the network and workstations.

4C. Enhance policies, procedures, and technical capabilities to monitor the network for suspicious activity.

5. Segregation-of-Duty Controls

SBA generally has established and implemented appropriate segregation-of-duty controls throughout its information system environment. We did, however, identify two instances in which control was inadequate.

A. Several district office and servicing center LAS security administrators have LAS user accounts for themselves in addition to their highly privileged administrator accounts. OCIO stated that, while some of the smaller offices have to operate in such a manner due to a lack of staffing, it agrees that administrators of larger offices should not have normal user accounts.

B. Although OCIO has established procedures for controlling emergency access to the source code residing on the mainframe in the current environment, the audit team found that mainframe computer console operators and programmers have access to both development and production environments on SBA's mainframe. As a result, programmers have access to production data.

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.

Improper segregation of duties increases the risk of unauthorized activities and may result in a loss of funds.

Recommendations

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

5A. Establish and implement specialized information security administrator training that provides the knowledge base sufficient to properly maintain the LAS security system and the integrity of the controls. This should also emphasize to all LAS security administrators that they are precluded from establishing individual user accounts for themselves.

5B. Direct the third-party mainframe service provider to partition the mainframe computer into two environments: (1) development environment for software development and testing, and (2) production environment for processing and maintaining loan accounting transactions and records.

5C. When recommendation 5B is implemented, update management controls for providing programmers with limited access to the production environment in a controlled manner for emergency fixes. This would include the creation and use of emergency accounts, and monitoring the activities of these accounts, when a programmer must make changes within the production area.

6. Service Continuity Controls

Properly designed service continuity controls increase the assurance that normal business operations can continue with minimal disruption when unexpected events occur. We noted areas for enhancing SBA's business continuity and disaster recovery ability and minimizing the impact upon its business operation resulting from unexpected events.

SBA has not developed a disaster recovery test plan for its network and has not entered into a support service arrangement to obtain off-site network hardware capabilities should HQ facilities become inoperable or uninhabitable.

A. The agency's mainframe computer operations disaster recovery hot-site test did not include a test of communication linkage between SBA's HQ and the hot-site facility.

B. SBA has not made arrangements for offsite storage of backup and recovery tapes. HQ and field offices network server backup tapes were being improperly stored and secured on building premises or, in some instances, at employee residences during FY 2001. In March of FY 2002, OCIO entered into a contract with Secure Vault for on-line, real-time backups to the contractor's storage devices.

OMB Circular A-130, Appendix III, requires agencies to establish and periodically test their capability to continue to provide services within a system based upon needs and priorities of system users. Furthermore, agencies are required to establish and periodically test the capability to perform agency functions supported by the application in the event of failure of its automated support.

Without adequate service continuity controls, SBA has reduced assurance that it can provide an orderly and reasonable recovery process.

Recommendations

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

6A. Revise current contractual agreements between SBA and its communication supplier to include setting up a temporary dedicated line between HQ or a major business center and the hot-site mainframe recovery facility in the event of a problem.

6B. Develop and test disaster recovery and business contingency plans on an annual basis. The tests would include:

- Actual communication changes that would be necessary to establish communication services between the hot-site and the test location.

- HQ communications hub and network facility recovery plans.

- Recovery of HQ and field offices using back-up capabilities.

7. Review of Mainframe Operations

We reviewed and assessed control over the mainframe service provider's operations and physical facilities. This audit activity was needed, because the contract between SBA and the service provider does not require the provider to undertake an independent third-party audit of its facility to provide assurance that it has instituted adequate security over data processing activities. We identified physical and management access control weaknesses with the mainframe computer data processing center and computer room. Specifically, we identified the following conditions:

- Facility management has not established internal controls to ensure that console logs are reviewed on a regular basis.

- Facility management has not established internal controls to ensure that only current employees have console user accounts.

- Facility management has not established internal controls to ensure that console account passwords comply with SOP 90-47.

- The transportation bins storing backup tapes of the mainframe operating system and loan accounting software and transactions were not properly secured before transport of tapes to the off-site storage location.

OMB Circular A-127 requires that agencies plan for and incorporate security controls in accordance with the Computer Security Act (CSA) of 1987 and requires agencies to ensure that the service provider incorporate adequate security.

Weak mainframe computer operation controls increase the risk of lost LAS data and data processing capability and hinder SBA's ability to carry out its day-to day functions.

Recommendations

We recommend that the Chief Information Officer:

7A. Enter into an agreement with the third-party mainframe service provider to correct identified weaknesses and allow periodic reviews of controls by SBA representatives.

7B. Continue to pursue with GSA a requirement for the third-party mainframe service provider to undergo an annual audit of its data processing facility and make audit results available to SBA.

ATTACHMENT 1: SUMMARY OF AUDIT RESULTS

FY 2001 CFO AUDIT *INFORMATION SYSTEMS CONTROL REVIEW*	SYSTEM					
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	**OCIO LAS**	**ALCS**	**FFS**	**DFC**	**LANs WANs**	**SBG**
ENTITY-WIDE SECURITY PROGRAM CONTROLS						
Risks are periodically assessed.	1	1	1	1	1	1
Security program is documented.	2	1	1	1	1	1
Security management structure is in place and responsibilities assigned.	2	1	1	1	2	2
A personnel security policy is established.	2	1	1	1	1	1
A security-monitoring program is established.		2	2	2		2
ACCESS CONTROLS						
Information is properly classified.	1	1	1	1	1	1
User access and privileges are authorized.	2	2	1	1	2	2
Physical and logical controls prevent and detect unauthorized activities.	2	2	1	1		2
Apparent unauthorized activities are monitored and investigated.	2	2	1	1		2
APPLICATION SOFTWARE DEVELOPMENT AND PROGRAM CHANGE CONTROLS						
Program modifications are documented, reviewed, tested, and approved.	2	1	4	1	4	2
Program changes are documented, reviewed, tested, and approved before releasing to production.	2	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	2	1
System access is monitored.	2	2	4	1	2	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	1	1	2	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	2	2	1	1	2	2
SERVICE CONTINUITY CONTROLS						
Critical data and resources for recovery and establishment of emergency processing procedures are identified.	1	1	1	1	2	1
Procedures exist for effective backup and offsite storage of data and application and system software.	2	2	1	1		2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	2	2	2	2		2

LEGEND

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

For controls rated "1," SBA has implemented adequate policies, procedures, and practices. For controls rated "2," controls were in place, but had not been fully implemented (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). For controls rated "3," controls were not in place or not effective.

ATTACHMENT 2: MANAGEMENT COMMENTS AND OUR EVALUATION

The Office of the Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO) provided joint comments to the draft report, and the Office of Disaster Assistance (ODA) provided separate comments.

OCIO and OCFO generally agreed with 15 of the 24 recommendations; they did, however, disagree with 8 recommendations and did not comment on one recommendation. An overriding concern was that the report did not give enough recognition to the progress SBA has made over the past several years toward achieving its goals of control and security over its information systems. Cotton & Company agrees that SBA has made significant improvements and has modified the report appropriately to reflect those improvements.

ODA agreed with the findings and provided comments on recommendations affecting its office.

We have incorporated comments in this report as appropriate and include full OCIO/OCFO and ODA comments and our responses on the following pages.

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

DATE: March 28, 2002

TO: Robert G. Seabrooks Assistant Inspector General for Auditing

FROM: Howard F. Bolden
Agency Computer Security Program Manager

SUBJECT: Response to Audit of SBA's Information Systems Controls

On behalf of the Office of the Chief Information Officer (OCIO), Office of the Chief Financial Officer (OCFO), and Office of Disaster Assistance (ODA) we appreciate the opportunity to respond to the report on the Audit of SBA's Information Systems Controls.

Attached please find the responses of OCIO and OCFO (combined) and ODA.

If you have any questions please contact me at 205-7173.

OCIO/OCFO Response to Audit of SBA's
Information Systems Controls
March 14, 2002

1. Entity-Wide Security Program Controls

1A - We partially agree with the recommendation. The Office of the Chief Information Officer (OCIO) has performance goals and measures that are linked to the SBA performance goals, the President Management Goals, and the Government Paperwork Elimination Act. These goals have been incorporated into the performance plans for the Chief Information Officer (CIO) and the senior OCIO staff (GS 14/15). OCIO is currently developing additional performance measures to improve our ability to monitor performance.

Cotton & Company Comments: Modified report to emphasize SBA progress in this area.

1B - We partially agree with this recommendation. The OCIO has focused on developing an enterprise architecture (EA) plan for the Agency in accordance with the guidance and requirements mandated by the Office of Management and Budget (OMB). The EA incorporates many of the items identified and needing to be included in a strategic IT plans such as linking business functions to data, systems, hardware and software including security. We plan to produce a strategic plan as a companion document to the EA.

Cotton & Company Comments: Modified report to emphasize SBA progress in this area.

1C - We partially agree with this recommendation. In terms of information technology security, the OCIO has developed, and is continuing to improve its Agency comprehensive security plan. It has been in progress for several years. We find it disconcerting that each time the auditors report on our progress they make it sound as though the Agency has done nothing. We have developed implementation milestones which we have shared with the auditors over several years. We will continue to enhance the program per the existing implementation schedule. We have developed, and will continue to develop, general security policies and procedures for the SBA's Program Offices. Per GISRA, it is the responsibility of the heads of the Program Offices to implement IT security policies and procedures. OCIO will monitor compliance with the program requirements through its normal reviews of Program Office systems. OCIO will not develop a separate program to "monitor effectiveness of each part of the information technology security assigned to each office'. We consider that redundant to the use of performance measures.

Cotton & Company Comments: Disagree with SBA's response. A comprehensive security plan would include oversight procedures to permit OCIO to monitor the effectiveness of each aspect of IT security assigned to each general support system or major application outside of periodic certification and accreditation reviews. Further, OCIO's response is in conflict with SOP 90-47 and OMB Circulars A-130, Appendix III. SOP 90-47 clearly assigns responsibility for the security program to OCIO.

1D - We agree with the recommendation. OCIO and the Office of Human Resources (OHR) are developing IT security rules of behavior.

lE - We agree with the recommendation. OCIO in coordination with OHR, the Office of Procurement and Grants Management and the Office of the General Counsel will determine the appropriate language of the agreement.

2. Access Controls

In the description of Access control issues the auditors have made statements that mislead the reader into believing that there are security issues that do not, in fact exist. Specifically Item B "Accounts belonged to people no longer employed..." When the contractors left, their user privileges were locked. Their ID are not removed because that would orphan all of the files that they created and, in fact, Sybase will not allow the

IDs to be removed without removing all associated files first. If the accounts are locked there is no security issue.

2A. - We disagree with the recommendations. We already provide information to security administrators and IRMs though the computer -based training courses, which all IRMs and system administrators are required to complete per SBA Notice We will be working with OHR to revise the position description of all agency personnel having security IT related duties, whether as a primary function or as collateral duties to reflect the new standard developed by the Office of Personnel Management (OPM) for personnel having duties in the IT series. CICR reviews already spot check desktop machines and HQ network administrators run security sweeps of LAN servers.

We have determined that 60 days is the appropriate interval for changing administrative passwords.

Cotton & Company Comments: Disagree with SBA's response. The finding states that security administrators run their systems (Network and LAS) differently without having a standard set of procedures or checklists for maintaining networks and other systems. The IRM security-training course is too basic to satisfy this finding and recommendation.

2B - We disagree with the recommendations. Local network administrators do not need to review their user lists monthly. They need to verify that their user lists are current and keep them current by promptly removing individuals when they leave - as they are required to do by current policy. IT security routinely receives a listing of separated employees from NFC within fifteen days of heir departure. We are working with OHR to obtain immediate notification when employees are separated.

Cotton & Company Comments: Agree with SBA's response and have modified the recommendation accordingly.

2C - We disagree with the recommendation. This is a closed issue. We are in the process of migrating applications from the mainframe to client-server systems. We have determined that it would be too costly and resource intensive to retrofit the security system when it will be going away. We have evaluated the risks and made a decision to accept the risk. This is the fourth time that we have told you the same thing. Our decision is final.

Security administrators have always had the ability to reset user passwords.

Cotton & Company Comments: Disagree with SBA's response. SBA relies on LAS to perform mission-critical operations relating to SBA loan activities and, as such, part of SBA's critical infrastructure. Allowing LAS security administrators to view user passwords in plain text does not provide adequate assurance that transactions processed are valid. While OCIO insists that LAS will be eliminated, further development of the new Loan Modernization System (LMS) was put on hold in 2001. As such, weaknesses in LAS must be addressed.

2D - We agree with the recommendation.

2E - We agree with the recommendation.

3. Application Software Development and Program Change Control

We believe the statements made by the string together a series of individual facts that may lead the reader to an inaccurate conclusion. Specifically Item A "individuals who approve financial transactions may modify transaction entered by others...". In fact budget approvers can modify transactions before they approve it. They have that authority. In any event, ALL transaction modifications are recorded in the audit log. There is no issue here of which we are aware.

Additionally, in reviewing the information a reader may conclude that the IT security staff was remiss in not 'participating fully in the design, development, etc., of JAAMS". In fact the security staff did have a person assigned to the development team. This individual attended meetings and provided input and guidance on security related issues. They became a regular meeting participant after they were trained in Oracle security features. Prior to that guidance was provided for baseline security requirements and guidelines via the information contained in the security SOP guidelines. The security staff is not the primary systems designer but rather has the role of providing guidance on baseline security requirements and reviewing the system during and after development. Those are exactly the functions that were performed for the JAAMS project.

3A - We disagree with the recommendation. Security personnel already participate in the development process. Specific security reviews are defined in the Agency's system development methodology. We will continue to perform pre and post certification reviews. Sign-offs at each step of development are not necessary.

Cotton & Company Comments: Disagree with SBA's response. We consider it important that OCIO security participate in the development process from the beginning. This ensures that security requirements meet SBA security standards rather than being retrofitted after the fact. Further, OCIO security needs to participate in all major phases of all major development projects, including sign-off at the end of critical phases.

3B - We agree with the recommendation.

3F- OCFO has no comment on this recommendation. They will provide comments on the 1824.

Cotton & Company Comments: Recommendation was withdrawn pending further audit work next year.

4. System Software Controls.

We do not believe the statement accurately reflect the situation--specifically item B. We have extensive intrusion detection capabilities of which the auditors are well aware. The auditors were briefed last year by Creative Technologies, a company commissioned by OCIO to perform penetration tests, in which they praised SBA's intrusion detection capabilities which blocked them from the system at the start of their tests.

We did, in fact, detect the auditors' attempts to penetrate the system. We contacted the auditors to verify that it was they who were attempting to gain information about the system. When they affirmed that it was, we ignored further attempts from those IP addresses. The auditors apparently thought that we should have repeatedly informed them that we observed their activity. The fact of the matter is that neither they, nor any other companies with whom we have contracted to perform penetration tests have succeeded in an external penetration attempts. We also continue to monitor internal penetration attempts.

The incident cited in paragraph A was caused by an administrator who knowingly violated standard operating procedure of which he was well aware. The issue cited in paragraph C was caused by an administrator who failed to make changes to the system and who violated long standing policy of which he was well aware. We have addressed this issue with the individuals involved and with the network staff in general. We disagree with the auditors on the gravity of this issue.

OCIO/OCFO Response to Audit of SBA's Information Systems Controls March 14, 2002

4A - We disagree with the recommendation. Policies are already in place to apply patches in a timely manner.

Cotton & Company Comments: Disagree with SBA's response. While SBA has practices that require timely installation of software patches, this is not being accomplished. OCIO needs to emphasize the importance of applying patches to operating system and applications in a timely manner.

4B - We disagree with the recommendation. OCIO tests all new software before installing it on the network.

Cotton & Company Comments: Agree with SBA's response and have modified the recommendation accordingly.

4C - We disagree with the recommendation. OCIO already has a successful intrusion detection program.

Cotton & Company Comments: Disagree with SBA's response. During the audit, OCIO did not detect the external CyberCop scans and common hacking activities originating from external and internal sources being used to conduct intrusion testing.

5. Segregation of Duty Controls.

We believe that Item B is misleading and combines two issues in one statement for additional impact. The mainframe facility uses a centralized control room in which the consoles of all systems in the facility are located. The consoles are restricted to operators and anyone approaching them is challenged. The security of the mainframe consoles is not an issue. We have reviewed the Unisys facility and find no security issues with the console area. We have made a management decision that security is adequate and any security issues are acceptable. We consider this matter closed.

5A - We partially agree with the recommendation. We have already developed training courses for system administrators and are in the process of upgrading the training courses. We will add some additional material pertaining to the mainframe security system. We will not preclude LAS administrators from having user account on the system as many of the administrators perform that task as a collateral duty and, in fact, need a user ID.

Cotton & Company Comments: We disagree with SBA. SBA can not maintain an adequate separation of duties where the security administrators are also users. SBA could geographically consolidate its LAS administrator functions to ensure that those who perform security duties do not also perform user duties.

5B - We agree with the recommendation. We are in the process of partitioning the production, development, and test environments.

5C - We partially agree with the recommendation. Procedures are already in place for emergency access to production systems by programmers on mainframe systems. We do not see the need for additional procedures.

Cotton & Company Comments: Disagree that SBA does not need to monitor programmer's emergency access and emergency changes in the production systems. This is a basic rule of computer security, and management should not accept this situation.

OCIO/OCFO Response to Audit of SBA's Information Systems Controls March 14, 2002

6. Service Continuity Controls.

6A - We partially agree with the recommendation. Our current agreement with our mainframe contractor requires the establishment of alternate connectivity in the event of an emergency.

Cotton & Company Comments: Disagree with SBA's response. SBA mainframe contractor is required to establish a communication line between its facility and the hotsite during testing. It is not, however, responsible for providing a direct communication line between SBA and the hotsite facility.

6B - We partially agree with the recommendation. We are near completion of the development of a comprehensive disaster recovery plan for the Agency. We will test the plan every year. Semi-annual testing would be too resource intensive and disruptive to the Agency. Testing once per year is sufficient. OCIO and Agency management will determine what areas require testing.

Cotton & Company Comments: Agree with SBA's response and have modified the recommendation accordingly.

6C,D - We disagree with the recommendations - OCIO has recently signed an agreement with Secure Vault to provide real time online backup and storage of Field Office LAN servers. The service will start on Monday for all offices which have been upgraded to Windows2000. As each office is upgraded, data will be automatically backed up by Secure Vault. This will be the Agencywide backup solution.

Cotton & Company Comments: Agree with SBA's response and have removed the recommendation accordingly.

7. Review of Mainframe Operations

7A. We agree with the recommendation

7B. We partially agree with the recommendation - As this contract is run by GSA fro the benefit of the Federal Government SBA is in no position to require an annual audit under the contract. We will, however, contact GSA yet again, to request that they require a SAS 70 audit to be performed. We had suggested in the past that the IG contact GSA's IG to see of they could assist in this effort.
If you have any questions please contact Howard Bolden, Agency Computer Security Program Manager, at
[ex. 6]

Cotton & Company Comments: We disagree with SBA. SBA management has primary responsibility for ensuring that required reviews of its contractors are performed and the integrity of SBA systems are maintained. OIG has stated, however, that it will determine if it can be of assistance to SBA management in securing the required reviews with GSA.

FOIA EX. 6

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

Date: MAR 27 2002

To: Robert G. Seabrook
Assistant Inspector General for Auditing

From: Associate Administrator for Disaster Assistance

Subject: Response to Audit of SBA's Information Systems Control

Regarding the draft audit report on SBA's Information Systems Controls issued by Cotton & Company LLP, as part of the audit of SBA's FY 2001 financial statements, we agree with findings of the report. However, it should be noted that several of the findings need clarification.
Specifically, the following recommendations for the Office of Disaster Assistance:

Develop and implement software development and program change procedures and processes that incorporate OCIO standards.

In 1999, ODA issued numbered memo 99-50 addressing computer software development, which established procedures for program changes. In 2000, OCIO released the Systems Development Methodology (SDM) for the Agency. ODA's objective is to fully comply with the Agency SDM.

Provide written authorization for the use of LOR modules with ALCS.

In 1997, ODA initiated the LOR project and subsequently piloted, demonstrated and implemented the LOR system. Numbered memos 97-56, *97-65* and 97-68, establish written authorization for the LOR initiative.

Restrict development programmer access to the production environment and preclude programmers from independently installing new software.

ODA is currently in the process of developing the new DCMS (Disaster Credit Management System). Therefore, the LOR system is deemed an interim solution and will require further analysis to determine if this capability can be incorporated into the LOR system. Costs and resources required need to be weighed against the risks and benefits derived from these controls.

If you have any questions or comments on this subject please contact [Ex. 6]

Herbert L. Mitchell

cc: Tom Dumaresq
Lawrence Barrett
Howard Bolden

Cotton & Company Comments: SBA did not specifically address the recommendations, but indicated that a new system would be replacing the LOR system. SBA stated that costs and resources required would be weighed against risks and benefits derived from recommended controls.

FOIA EX. 6, 5

ATTACHMENT 3

REPORT DISTRIBUTION

Recipient	**Copies**
Associate Deputy Administrator for Management & Administration	1
Associate Deputy Administrator for Capital Access	1
Associate Administrator for Field Operations	1
Assistant Administrator Office of Congressional & Legislative Affairs	1
Assistant Administrator for Human Resources	1
Chief Financial Officer	1
General Counsel	2
General Accounting Office	1
Office of the Chief Financial Officer Attention: Jeff Brown	1