AUDIT OF SBA'S
INFORMATION SYSTEMS CONTROLS
FISCAL YEAR 2003
AUDIT REPORT NUMBER 4-19

APRIL 29, 2004

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

AUDIT REPORT
Issue Date: April 29, 2004
Number: 4-19

To: Stephen D. Galvan
Chief Operating Officer
Chief Information Officer

Thomas A. Dumaresq
Chief Financial Officer

/S/
From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's Information Systems Controls for FY 2003

Attached is the audit report on SBA's Information Systems Controls for FY 2003 issued by Cotton & Company LLP as part of the audit of SBA's FY 2003 financial statements. The auditors reviewed the general and application 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. Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. Application controls help ensure that transactions are valid, properly authorized, and completely and accurately processed by the computer. Federal requirements for general and application 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, and (6) service continuity controls. The report also provides recommendations for strengthening controls in these areas.

SBA generally agreed with the auditor's findings and recommendations with the exception of finding 3B on SBA's Credit Reform Models. A determination as to the level of documentation required for the Credit Reform Models will be addressed in the audit resolution process.

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(s), 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 Jeffrey A. Brindle, Director, Information Technology and Financial Management Group at (202) 205-[FOIA Ex. 6].

Attachments

COTTON&COMPANY LLP

auditors • advisors

333 North Fairfax Street • Suite 401 • Alexandria, Virginia 22314 • 703/836/6701 • FAX 703/836/0941 • WWW.COTTONCPA.COM

January 29, 2004

AUDIT OF INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2003 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Inspector General
U.S. Small Business Administration

We were engaged to audit the financial statements of the U.S. Small Business Administration (SBA) as of and for the years ended September 30, 2003, and 2002, and have issued our report thereon dated January 28, 2004, in which we disclaimed an opinion on those financial statements. These financial statements are the responsibility of SBA's management.

In planning and performing our work, we considered SBA's internal control over financial reporting by obtaining an understanding of SBA's internal control, determining if internal control had been placed in operation, assessing control risk, and performing tests of control. We limited our internal control testing to those controls necessary to achieve objectives described in Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations. The objective of our work was not to provide assurance on internal control. Consequently, we do not provide an opinion on internal control.

Our consideration of internal control over financial reporting would not necessarily disclose all matters in internal control over financial reporting that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect SBA's ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements.

This report 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 work. They were always courteous, helpful, and professional.

Very truly yours,

COTTON & COMPANY LLP

/S/
Charles Hayward, CPA, CISA, CGFM

AUDIT OF INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2003 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Cotton & Company LLP was engaged to audit Fiscal Year (FY) 2003 and 2002 financial statements of the U.S. Small Business Administration (SBA). As part of that work, we reviewed general and application controls over SBA's information systems following guidance provided in the General Accounting Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM). FISCAM incorporates audit techniques and procedures to ensure adequate coverage of federal requirements and standards established by:

- Computer Security Act of 1987.
- Clinger Cohen Act.
- Federal Information Security Management Act (FISMA).
- Office of Management and Budget (OMB) Circulars A-127 *Financial Management Systems,* and A-130, *Management of Federal Information Resources,* Appendix III, *Security of Federal Automated Information Resources.*
- National Institute of Standards and Technology (NIST) standards and guidelines contained in NIST's Federal Information Processing Publications (FIP Pubs) and in its 800 series Special Publications.

This report contains the results of our review and recommendations for improvements. Control weaknesses discussed herein have been reported in SBA's FY 2003 financial statement internal control report as a reportable condition.

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 modification 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.

Application controls are the structure, policies, and procedures that apply to separate, individual application systems, such as accounts payable, inventory, payroll, grants, or loans. Application controls encompass both routines contained within the computer program code and policies and procedures associated with user activities, such as manual measures performed by the user to determine if the computer accurately processed data. GAO categorizes application controls as follows:

- **Authorization controls** are most closely aligned with the financial statement accounting assertion of existence or occurrence. This assertion, in part, concerns the validity of transactions and that they represent economic events that actually occurred during a given period.

- **Completeness controls** directly relate to the financial statement accounting assertion on completeness, which deals with whether all valid transactions are recorded and properly classified.

- **Accuracy controls** directly relate to the financial statement assertion on valuation or allocation. This assertion deals with whether transactions are recorded at correct amounts. The control category, however, is not limited to financial information, but also addresses the accuracy of other data elements.

- **Controls over integrity of processing and data files**, if deficient, could nullify each of the above control types and allow the occurrence of unauthorized transactions, as well as contribute to incomplete and inaccurate data.

SBA'S INFORMATION SYSTEMS ENVIRONMENT

SBA's financial management information system environment is decentralized. It is comprised of seven 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 and maintained under contract for SBA by UNISYS 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 data, and interfacing with LAS.

4. **Joint Accounting and Administrative Management System (JAAMS)**, a client-server financial management system used by all SBA offices for administrative accounting functions. The JAAMS server and database were operated and maintained under contract for SBA by UNISYS at its Eagan, Minnesota, facility during FY 2003. The JAAMS production server and database were relocated to a new third-party vendor, CORIO, Inc. in Tempe, Arizona, on September 1, 2003. CORIO has a second facility in California housing the JAAMS test environment.

5. **Local- and Wide-Area Networks (LANs and WANs)**, communications systems maintained and operated by all SBA offices. LANs and WANs provide gateways to LAS, ALCS, and JAAMS; allow offices to share files and communicate electronically; permit the transfer of data among systems; and provide Internet access. OCIO develops and disseminates guidance and procedures for 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. This system processes SBG program data and exchanges accounting information with JAAMS.

7. **Credit Reform and Subsidy Calculation System,** a series of SAS and JAVA programs and Microsoft Excel spreadsheets developed and maintained by OCFO used for calculating subsidy rates supporting SBA's various direct and guarantee loan programs consisting of the Section 7(a), Small Business Investment Company (SBIC) Program, Section 504, and Disaster assistance loans, and SBA's secondary market guarantee program for pooled business loans accounted for in the Master Reserve Fund (MRF).

In addition, SBA's financial management activities rely on systems developed, maintained, or operated by external parties, including CORIO, Inc., Colson Services Corporation, UNISYS, and the National Finance Center (NFC), for processing and exchanging data related to functions, such as loan servicing and payroll. SBA also has acquired lock-box banking services from the Bank of America and other non-continental domestic banks for processing checks on borrowers' loan payments; the banks provide this information electronically to DFC.

FY 2003 RESULTS

SBA continued to improve internal control over its information system environment in certain areas during FY 2003. Its major accomplishments this year include the following:

- Conducted certification and accreditation reviews for additional major applications.
- Continued roll out of the Windows 2000 operating system at various field locations.

These accomplishments were, however, overshadowed by:

- Delays by SBA's program offices in implementing corrective actions to resolve prior-year weaknesses.
- Inadequate allocation of resources to support OCIO's security program to:
    - Effectively monitor day-to-day security operations.
    - Promote compliance with established security policies throughout SBA.

In the remainder of this report, we discuss results of our FY 2003 review and the status of management actions to address prior-year recommendations and new weaknesses identified in FY 2003. We also present our recommendations for improvements. This report includes the following attachments:

Number	Title
1	FY 2003 Summary of Results
2	Status of Prior-Year Audit Recommendations
3	Management Comments
4	Network Analysis Results (Restricted Distribution and Use)

1. ENTITY-WIDE SECURITY PROGRAM CONTROLS

Entity-wide security program planning and management provides a framework for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer-related controls. SBA's information system security program planning and management continued to have areas of weakness. Without an effective management control structure, control weaknesses throughout the information system and security infrastructure will continue, and specific actions to address weaknesses will continue to be ineffective. The cause of most control weaknesses discussed in this report can be traced to the weaknesses discussed in this segment of the report.

We identified the following entity-wide security program control weaknesses during our FY2003 financial statement audit:

A. SBA's information system and security program did not provide assurance that the program complied with requirements established by federal laws, regulations, and standards. Control weaknesses identified in certification and accreditation reviews and audit reports were not resolved in a timely manner. Additionally, OCIO did not have procedures in place to ensure the effectiveness of controls to preclude reoccurrence of conditions. OCIO technical personnel were not provided technical training to enable personnel to successfully carry out their duties and responsibilities, and personnel technical training requirements were not strategically aligned with SBA's technology strategic plan.

   Further, OCIO was not effectively participating in developing new systems in a timely manner to ensure that system controls are properly designed and developed to provide adequate security; and data reliability, completeness, and accuracy. OCIO had not developed the procedures to fulfill its delegated responsibilities and provide technical leadership on system development efforts initiated by other SBA program offices such as OCFO and ODA to ensure system interrelationships and interfaces are properly and timely addressed to reduce manual transfer of financial information.

   OCIO had not fully resolved 15 conditions identified in prior year audits. This demonstrates that SBA is not assigning a high priority to resolving audit recommendations and implementing corrective actions, contrary to requirements stipulated in OMB Circular A-50, Audit Follow-up.

   Management claimed that insufficient resources and higher priorities have impeded its ability to implement all requirements established by the Computer Security Act, Clinger Cohen, FISMA, OMB Circulars A-127 and A-130; and NIST standards.

SBA received approval to reorganize OCIO effective December 31, 2003. The reorganization will create two new offices: E-commerce and Information Security. OCIO will be a direct-report to SBA's Administrator.

Recommendation 1A: We recommend that the SBA Administrator ensure that sufficient resources are provided to enable OCIO to meet its responsibilities under the Clinger Cohen Act, FISMA, and OMB Circulars A-50, A-127, and A-130.

Recommendation 1B: We recommend that the Chief Information Officer revise and enhance existing policies and procedures to:

- Ensure control weaknesses identified in certification and accreditation reviews and audit reports are resolved in a timely manner and ensure senior management is provided timely information regarding the progress towards implementing corrective actions,
- Ensure OCIO monitoring controls are effective to preclude reoccurrence of previously noted weaknesses,
- Ensure technical personnel are provided technical training to enable personnel to successfully carry out their duties and responsibilities,
- Assure that technical skills are sufficient to meet new technical requirements prior to implementing new hardware and software, and
- Ensure OCIO effectively participates in all phases of system development in a timely manner to ensure that system controls are properly designed and developed to provide adequate security; and data reliability, completeness, and accuracy for all significant system initiatives both within and outside of OCIO.

B. OCIO had not implemented procedures to monitor and report management's actions to address and resolve weaknesses identified during system certification and accreditation reviews, audits, and management reviews. OCIO did not monitor system owner implementation of corrective actions to ensure that program offices address weaknesses identified during certification and accreditation reviews in a timely manner. As a result, OCIO was not fully compliant with FISMA, OMB circulars, and NIST standards.

Recommendation 1C: We recommend the Chief Information Officer, in conjunction with system owners:

(1) Develop policies and procedures to require system owners to provide plans of action to OCIO for correcting weaknesses identified from audits, management reviews, and certification and accreditation reviews.

(2) Ensure that plans adequately address management actions to resolve or minimize weaknesses in the short term while implementing longer term system corrective actions. Develop reporting processes to follow-up on system owner corrective action plans.

(3) Ensure that sufficient resources are made available to monitor system owner corrective action plans.

2. ACCESS CONTROLS

Physical and logical access controls should be designed to protect an agency's assets against unauthorized modification, loss, destruction, and disclosure. During the FY 2003 controls review, we performed external and internal testing of the network and application access controls. We noted the following access controls weaknesses:

A. Controls over the administration of network and financial application accounts were not effective. OCIO developed and disseminated Procedural Notice 9000-1406 "Removal of Old Computer User Accounts" during FY2003 in response to our prior-year recommendation in this area however, this procedural notice is not being followed by all parties. We identified administrators not following established policies and procedures when adding or modifying accounts. Although OCIO did not have administrative responsibilities for all systems and the network, it was responsible for ensuring that all SBA program offices complied with OCIO security policy, standards, and requirements.

We identified the following issues during our review of account administration at SBA headquarters, DFC, Sacramento Disaster Area Office, and Fresno Commercial Loan Service Center:

[FOIA Ex. 2]

Recommendation 2A: We recommend that the Chief Information Officer:

(1) Implement procedures to ensure compliance with Procedural Notice 9000-1406 "Removal of Old Computer User Accounts"

(2) Require network security administrators to review all current network accounts to identify and eliminate unnecessary accounts and require periodic documented reviews of all generic network accounts to ensure that they are authorized and needed.

(3) Provide resources sufficient to monitor and assess network administration activities to ensure compliance with federal laws and regulations, SBA policies and procedures, NIST guidance, and industry best practices.

(4) In coordination with program directors, develop procedures for controlling contractor personnel access to the network and applications. Procedures should be established to:

- Require Contracting Officers' Technical Representatives (COTRs) to notify security administrators in writing of each contractor personnel needing a network and application account along with privileges to assign to the account.

- Require all network and application accounts established for contractor personnel to be established with a renewal or termination date not to exceed one year or the length of the contract, whichever is less.

(5) In coordination with OHCM, develop procedures for network and application security administrators to receive notification of termination of SBA employees.

B. [FOIA Ex. 2].

Recommendation 2B: We recommend that the Chief Financial Officer instruct the Director of DFC to establish adequate physical security for routers by either moving the routers to a restricted area where access is limited to only authorized individuals, such as the server room, or develop compensating controls, such as constructing a security cage.

C. [FOIA Ex. 2].

Recommendation 2C: We recommend that the Chief Information Officer:

(1) [FOIA Ex. 2]

(2) Create new network accounts for non-headquarter network administrators with limited domain administrative privileges to add and delete users and add, delete, and modify objects within office Organization Units.

(3) Develop and implement procedures to perform periodic reviews of highly-privileged accounts to assess the continuing need for accounts and privileges.

3. APPLICATION SOFTWARE DEVELOPMENT AND PROGRAM CHANGE CONTROLS

SBA's application software development and program change controls should be designed to prevent implementation of unauthorized programs or modifications to existing programs. We noted the following:

A. Change control policies and procedures for JAAMS and Financial Reporting Information System (FRIS) are not being properly followed at DFC, because required signatures on SBA's System Implementation Order/Change Control forms are missing.

Recommendation 3A: We recommend that the Chief Financial Officer require that OFM ensure that all change control forms are complete before changes are released in the production environment and signatures are present for all spaces provided.

B. OCFO's Credit Reform Models did not comply with change control policies, procedures and documentation requirements in FASAB Technical Releases No. 3 and No. 6 or SBA system development and program change control policies and procedures. This occurred because:

- Actual changes to the formulas within Credit Reform Models were not tracked,
- Change policies to the models were informal and were not rigorously followed,
- Computations could not be reperformed, and
- Documentation needed to support computations did not exist.

Federal Financial Accounting and Auditing Technical Release No. 3: Preparing and Auditing Direct Loan and Loan Guarantee Subsidies under the Federal Credit Reform Act of 1990 (FCRA), also broadly requires agencies to maintain internal controls over models in each of the following categories:

- Control environment
- Risk assessment
- Control activities
- Information and communication
- Monitoring

The OIG released Audit Report No. 3-39, Monitoring of SBA's Implementation of the Disaster Credit Management System in September 2003; this report identified OCIO's non-compliance with its SDLC policy and procedures relating to OCIO's lack of involvement with new systems being developed.

Recommendation 3B: We recommend that the Chief Financial Officer formalize the change control, testing, acceptance, documentation standards, and validation procedures for the Credit Reform Models to conform with FASAB Technical Release No. 3 and No. 6 and SBA system development and program change control policies and procedures.

Recommendation 3C: We recommend that the Chief Information Officer develop the means to actively participate in all phases of system development efforts within the agency.

4. SYSTEM SOFTWARE CONTROLS

Properly designed system software controls limit and monitor access to programs and files that control computer hardware and protect applications. We identified security control weaknesses with the network operating system that reduce the effectiveness of controls to protect network operations from unauthorized activities from internal sources.

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. Additionally, NIST and the National Security Agency (NSA) have developed standards for securing Windows 2000 environments.

A. We conducted a scan of SBA's network to identify and assess the level of risk using a vulnerability scanning tool to identify SANS (SysAdmin, Audit, Network, Security) Institute "Top 20" security vulnerabilities. Our scan assessed whether SBA network servers had been properly configured, and network operating system software had been updated with vendor patches designed to properly address known vulnerabilities. A detailed breakdown of specific weaknesses is in Attachment 4.

[FOIA Ex. 2]

Recommendations 4A and 4B:

We recommend Chief Information Officer develop and implement a corrective action plan with specific milestones to address network weaknesses identified in Attachment 4 in a timely manner.

C. In our FY 2002 FISCAM audit, we recommended that SBA enhance policies, procedures, and technical capabilities to monitor the network for suspicious activity. SBA agreed with this recommendation and initially projected a completion date of September 30, 2002. This date was later modified to February 28, 2003.

Although OCIO installed a network intrusion detection system (IDS) and contracted with a vendor to monitor IDS activities and maintain and review all IDS activity logs, OCIO had not developed written policies or procedures to establish requirements and ensure performance.

We commend OCIO for recognizing the need for installing additional server sensor devices on the network. OCIO plans to add another 20 sensors during FY 2004. OCIO has not, however, performed a security analysis to determine the most effective locations for the sensors.

Recommendation 4C: We recommend that the Chief Information Officer:

(1) Perform a security assessment to determine the most effective placement of the 20 new sensors.

(2) Revise the IDS vendor's contract as necessary for performance factors established in Recommendation No. 4A of this report.

D. The FY2002 FISCAM report recommended that OCIO develop the means to test for compliance with SBA's password configuration requirements.

[FOIA Ex. 2]

5. SEGREGATION-OF-DUTY CONTROLS

An appropriately designed organizational structure with well-designed roles and responsibilities will minimize the risk that unauthorized actions take place and are not detected.

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. Appendix III also requires establishing and implementing practices to divide steps of critical functions among individuals and establishing practices to keep a single individual from subverting a critical process.

GAO's FISCAM states:

> *Management should have analyzed operations and identified incompatible duties that are then segregated through policies and organizational division. Although incompatible duties may vary from one entity to another, the following functions are generally performed by different individuals: IS management, system design, application programming, systems programming, quality assurance/testing, library management/change management, computer operations, production control and scheduling, data security, data administration, and network administration.*

In addition, FISCAM states that:

> *...it is management's responsibility to ensure that segregation of duties is established, enforced, and institutionalized within the organization.*

A. Proper separation of duties for changes to JAAMS and FRIS had been identified on the System Implementation Change Control Form used at DFC; these separation-of-duties controls were not,

however, fully enforced by management. Individuals were completing more than one area of the form, thus subverting controls intended to ensure proper separation of duties. Inadequate separation of duties increases the potential for unauthorized code to be implemented and placed into production that could result in unauthorized activities.

Recommendation 5A: We recommend that the Chief Financial Officer instruct DFC management to take steps necessary to ensure that individuals are not allowed to complete incompatible areas during the system implementation and change process. In addition, management should review all change control forms to verify that proper separation is in place.

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.

OMB Circular A-130, Appendix III, requires an agency to establish and periodically test its capability to continue to provide services within a system based upon user needs and priorities. 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.

A. SBA cannot ensure that operations can be brought back within an acceptable period of time in the event of a disaster or disruption in service. We reviewed service continuity plans and procedures at SBA headquarters and field sites at DFC, Sacramento Disaster Area office, and Fresno Commercial Loan Service Center. We noted weaknesses in business resumption plans (BRP) and service continuity policies and procedures at all three field sites.

The following are specific exceptions noted by field site:

- DFC had not developed or documented a test plan for testing its BRP and had not established a target date for completing testing.
- The Sacramento Disaster Area Office did not have a documented BRP, its tape backup procedures did not meet SBA requirements, and it did not store tapes offsite.
- The Fresno Commercial Loan Service Center had not tested or updated its BRP since 2001 and did not have adequate off-site storage of the office's backup tapes.

The SBA Headquarters Continuity of Operations Plan (COOP) was successfully tested in March 2003. In September 2003, SBA moved the JAAMS general ledger system from Eagan, Minnesota, to a new data processing facility located in Tempe, Arizona. We understand the JAAMS COOP was tested after fieldwork ended.

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

Weaknesses with SBA's COOP were previously noted in OIG Audit Report No. OIG 02-18. In that report, we recommended that the Chief Operating Officer (COO) complete a formal business impact analysis in support of COOP and ensure the COOP properly addressed the required elements (Recommendation Nos. 6A and 6B). We consider the COO's actions to date as non-responsive. Additionally, at the exit meeting, the CIO stated that OCIO cannot take responsibility for all facets of SBA's disaster recovery and business contingency planning and tests.

Recommendation 6A: We recommend that the Chief Operating Officer develop an agency-wide business impact analysis that captures all identified needs within stated recovery times. At a minimum, the analysis would identify:

- Critical SBA business processes.
- General support systems and major applications that would be needed in a recovery process to support critical SBA business processes.
- Required recovery time periods.

Recommendation 6B: We recommend that the Chief Operating Officer finalize the draft COOP. The final COOP should include the following items:

- List of personnel and other resources related to the critical system that would be needed in a recovery process.
- Provisions for plan testing by each field office, disaster office, and headquarters at least every 3 years.
- Provisions for annual training on plan execution.
- Requirements for distribution of the plan to appropriate individuals.
- Identification of established contracts with external vendors as necessary to support the business continuity plan and disaster recovery plan.
- Assurance that all field sites have current, documented, and tested business resumption plans in place.
- Provisions to inform all field sites of their responsibilities for keeping the business resumption plans current and tested.
- Provisions to ensure that all field sites adhere to SBA policy requiring backup tapes to be stored offsite.
- Provisions to ensure that BRPs include procedures for safekeeping critical business documents, such as loan files, to ensure their availability.

ATTACHMENT 1A

SUMMARY OF RESULTS

FY 2003 CFO AUDIT INFORMATION SYSTEMS CONTROL REVIEW	SYSTEM					
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	OCIO LAS	ALCS	JAAMS	DFC	LANs WANs	Credit Reform Models
ENTITY-WIDE SECURITY PROGRAM CONTROLS						
Risks are periodically assessed.	1	1	2	1	1	4
Security program is documented.	2	1	2	1	1	4
Security management structure is in place and responsibilities assigned.	2	1	2	1	2	4
A personnel security policy is established.	2	1	2	1	1	4
A security-monitoring program is established.	3	2	2	2	3	4
ACCESS CONTROLS						
Information is properly classified.	1	1	1	1	1	3
User access and privileges are authorized.	2	2	2	1	2	2
Physical and logical controls prevent and detect unauthorized activities.	2	2	2	1	3	2
Apparent unauthorized activities are monitored and investigated.	2	2	2	1	3	2
APPLICATION SOFTWARE DEVELOPMENT AND PROGRAM CHANGE CONTROLS						
Program modifications are documented, reviewed, tested, and approved.	2	1	2	1	4	3
Program changes are documented, reviewed, tested, and approved before releasing to production.	2	1	2	1	4	3
Movement of programs in and out of libraries is authorized.	1	1	2	1	4	3
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	2	2	2	1	2	3
System access is monitored.	2	2	2	1	2	3
Changes to system are authorized and documented.	1	1	2	1	1	2
SEGREGATION-OF-DUTIES CONTROLS						
Incompatible duties are identified.	1	1	2	1	1	3
Segregation of duties is enforced through access controls.	2	2	2	1	2	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	2	2	2	1	2	2
SERVICE CONTINUITY CONTROLS						
Critical data and resources for recovery and establishment of emergency processing procedures are identified.	1	1	2	1	2	1
Procedures exist for effective backup and offsite storage of data and application and system software.	2	2	1	1	2	2
Business contingency and continuity and disaster recovery plans with hot-site facilities and annual testing are established.	2	2	2	2	2	2

LEGEND

1 – Based on our testing, controls appear to be in place. 2 – Based on our testing, controls appear to be in place, but not fully implemented. 3 – Based on our testing, controls appear to not be in place. 4 - Control not applicable.

ATTACHMENT 1B

APPLICATION CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	JAAMS	DCLS	FRIS
AUTHORIZATOIN CONTROLS			
All data are authorized before entering the application system.	1	1	1
Restrict data entry terminals to authorized users for authorized purposes.	4	4	4
Master files and exception reporting help ensure all data processed are authorized	2	1	1
COMPLETENESS CONTROLS			
All authorized transactions are entered into and processed by the computer.	2	2	2
Reconciliations are performed to verify data completeness.	1	1	1
ACCURACY CONTROLS			
Data entry design features contribute to data accuracy.	1	1	1
Data validation and editing are performed to identify erroneous data.	2	2	2
Erroneous data are captured, reported, investigated, and corrected.	3	2	2
Review of output reports helps maintain data accuracy and validity.	2	2	2
CONTROLS OVER INTEGRITY OF PROCESSING AND DATA FILES			
Procedures ensure that the current versions of production programs and data files are used during processing.	2	2	4
Programs include routines to verify that the proper version of the computer file is used during processing.	1	2	4
Programs include routines for checking internal file header labels before processing.	1	2	4
The application protects against concurrent file updates.	1	2	4

LEGEND

1 – Based on our testing, controls appear to be in place. 2 – Based on our testing, controls appear to be in place, but not fully implemented. 3 – Based on our testing, controls appear to not be in place. 4 - Control not applicable.

ATTACHMENT 2

AUDIT OF INFORMATION SYSTEM CONTROLS
FOR FY 2003
STATUS OF PRIOR-YEAR AUDIT RECOMMENDATIONS

Condition	Recommendation	Status as of 9/30/03
1 A: SBA has not recognized the NFC payroll/personnel system as a major agency application and therefore has not established a system security plan, risk assessment, and accreditation or approval for system use.	**Recommendation 1A:** We recommend that the Chief Human Capital Officer in conjunction with OCIO designate the NFC payroll/personnel system as a critical system and then proceed to develop an application systems security plan, risk assessment, and accreditation plan for the system.	Partially Complete
B: 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.	**Recommendation 1B:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA develop an agency-wide security plan, in accordance with Section 5.8 of the Information Technology Architecture Plan. SBA agreed with this recommendation and projected a completion date of September 30, 2003.	Closed
C: The Office of Human Capital Management (OHCM) has not defined personnel consequences for non-compliance with security policies and procedures and rules of behavior.	**Recommendation 1C:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA develop personnel policies and procedures consistent with and in support of defined rules of behavior for general support systems and major applications. SBA agreed with this recommendation and initially projected a completion date of December 1, 2002. This date was later modified to January 31, 2003.	Open
D: SBA does not obtain signed non-disclosure agreements from SBA and contractor personnel who handle sensitive data.	**Recommendation 1D:** We recommended in our Information Systems Controls Report for FY 2001 (OIG 02-18) that SBA develop non-disclosure and security awareness agreements that agency and contractor personnel will be required to sign. SBA agreed with this recommendation and initially projected a completion date of December 1, 2002. This date was later modified to February 28, 2003.	Closed
[FOIA Ex. 2]	[FOIA Ex. 2]	Open
B: OCIO and OHCM have undocumented procedures for informing security personnel of staff separations. By using informal separation procedures, the risk of an unauthorized user having access to a	**Recommendation 2B:** We recommended in our Information Systems Controls Report for FY 2001 (OIG 02-18) that OCIO and OHCM formally document staff separation procedures. SBA agreed with this recommendation and initially projected a completion date of November 1, 2002. This date was	Open

Condition	Recommendation	Status as of 9/30/03
system is increased.	later modified to February 20, 2003.	
C: OCIO has not adequately developed and provided technical training for personnel performing security administration activities either at the network or application level.	**Recommendation 2C:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA develop and implement technical training for security staff and all network and application security administrators. SBA agreed with this recommendation and initially projected a completion date of November 1, 2002. This date was later modified to December 1, 2003.	Open
[FOIA Ex. 2]	[FOIA Ex. 2]	Partially Complete
E: The LAS security software module continues to permit field office LAS security officers to view each user's password in the clear, thereby violating the security requirement that only the user has knowledge of the password. LAS screen SSDD04, which allows LAS users to change their own passwords, was not widely known or used by SBA employees. Furthermore, LAS security officers are unable to re-set user passwords.	**Recommendation 2E:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA change the LAS security module to prevent the LAS security administrator from viewing passwords in plain text and to enable the administrator to re-set user passwords. On January 31, 2003 SBA reported full corrective action had been completed.	Closed
3 A: As noted in the prior-year, although members of the OCIO security team were involved during JAAMS development, the security team was not involved throughout the entire process. 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	**Recommendation 3A:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that the CIO enhance system development procedures to ensure that security personnel actively participate in all phases of system development. SBA agreed with this recommendation and projected a completion date of May 30, 2003.	**Partially Complete**

Condition	Recommendation	Status as of 9/30/03
policies at the beginning and throughout the System Development Life Cycle (SDLC).		
3 B: As noted in the prior-year, program changes to the SBG system were not recorded in the tracking list of program changes, even though individual documentation was available.	**Recommendation 3B:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that the CIO enhance configuration management procedures to modify the user request form to include a check-off and identification block. SBA agreed with this recommendation and initially projected a completion date of August 1, 2002. This date was later modified to March 31, 2003.	**Closed**
4 A: In our previous audit, we recommended that SBA enhance policies, procedures and technical capabilities to monitor the network for suspicious activity. SBA agreed with this recommendation and initially projected a completion date of September 30, 2002. This date was later modified to February 28, 2003. [FOIA Ex. 2] Ineffective software monitoring tools and escalation procedures 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. In our previous-year audit, we recommended that SBA enhance policies, procedures, and technical capabilities to monitor the network for suspicious activity.	**Recommendation 4A:** We recommend that the Chief Information Officer fully implement the planned upgraded intrusion detection system and reporting/monitoring tools. Additionally, we recommend that the Chief Information Officer develop a rule base and procedures for monitoring network activity and create and document escalation procedures and timelines for reporting suspicious activity to OCIO security. Further, we recommend that Chief Information Officer test escalation procedures to ensure that responsible personnel report questionable activities in a timely manner.	Partially completed
[FOIA Ex. 2]	[FOIA Ex. 2]	Open
[FOIA Ex. 2]	[FOIA Ex. 2]	Open
[FOIA Ex. 2]	[FOIA Ex. 2]	Open

Condition	Recommendation	Status as of 9/30/03
E: OCIO has not completed an interim certification and accreditation prior to implementation of Windows 2000.	**Recommendation 4E:** We recommend that the Chief Information Officer develop and implement procedures to require that an interim certification be completed for operating systems and applications before implementation. Further, we recommend that the Chief Information Officer complete a full certification and accreditation of Windows 2000.	**Closed**
F: The OCIO has not applied the most recent relevant patches to the Windows 2000 operating system. While OCIO has developed procedures related to obtaining, testing and applying software patches as they are released, these procedures are not being consistently followed	**Recommendation 4F:** We recommend that the Chief Information Officer adhere to the policies previously developed and apply all relevant appropriate patches necessary to bring Windows 2000 up to the current patch version as recommended by the vendor.	**Open**
G: Administrators and security personnel are not adequately trained to allow them to fully understand their responsibilities and handle possible security violations.	**Recommendation 4G** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that OCIO provide appropriate training and periodic retraining to security personnel and administrators to allow them to perform security responsibilities effectively. SBA agreed with this recommendation and projected a completion date of March 31, 2003. Therefore, we are making no recommendation at this time.	**Open**
A: We noted an instance in which system programmers have access to the development environment as well as the production environment. Specifically, we noted the SBA Office of Financial Systems (OFS) programmers have access to the JAAMS production environment. Furthermore, we did not note any compensating control to this segregation-of-duty issue.	**Recommendation 5A:** We recommend that the Chief Financial Officer either restrict programmer access to the production environment and preclude programmers from independently installing new software or develop alternative control procedures to manage the risk of developers having access to the production environment.	**Closed**
B: Several district office and servicing center LAS security administrators continue to have LAS user accounts for themselves in addition to their highly privileged administrator accounts.	**Recommendation 5B:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA preclude LAS security administrators from establishing individual user accounts for themselves. SBA responded that certain LAS security administrators cannot be precluded from establishing individual user accounts for themselves due to the size of the offices where they work and that performing security administrator functions are a collateral duty. SBA implemented LAS program edits to prevent the same user ID from performing multiple functions on the same loan. Therefore, SBA has accepted the risk of allowing certain users to perform inherently conflicting duties.	**Closed**

Condition	Recommendation	Status as of 9/30/03
A: SBA has not completed a formal business impact analysis in support of its COOP. Additionally, the COOP is still in draft stage.	**Recommendation 6A:** We recommend that the Chief Operating Officer develop an agency-wide business impact analysis that captures all identified needs within stated recovery times. At a minimum, the analysis would identify: • Critical SBA business processes. • General support systems and major applications that would be needed in a recovery process to support critical SBA business processes. • Required recovery time periods.	Open
6 B: SBA's current draft COOP does not contain other critical elements of a COOP.	**Recommendation 6B:** We recommend that the Chief Operating Officer follow the formal process outlined above, make changes to the current COOP as necessary, and finalize the draft COOP. The final COOP should include the following items: • List of personnel and other resources related to the critical system that would be needed in a recovery process. • Provisions for annual plan testing. • Provisions for annual training on plan execution. • Distribution of the plan to appropriate individuals. • Identification of established contracts with external vendors as necessary to support the business continuity plan and disaster recovery plan.	Open
7 A: SBA's mainframe computer operations disaster recovery hot-site test did not include a test of the communication linkage between headquarters and the hot-site facility.	**Recommendation 7A**: We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that OCIO revise current contractual agreements with its communication supplier to include setting up a temporary dedicated line between headquarters or a major business center and the hot-site mainframe recovery facility in the event of a problem. OCIO agreed with this recommendation and projected a completion date of July 1, 2003.	Open
7 B: Weak mainframe computer operation control increases the risk of lost LAS data and data processing capability and hinders SBA's ability to carry out its daily functions. We identified physical and management access control weaknesses with the mainframe computer data processing center and computer room. Specifically, we identified the following conditions:	**Recommendation 7B:** We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA enter into an agreement with the third-party mainframe service provider to correct identified weaknesses and allow periodic reviews of controls by SBA representatives. SBA agreed with this recommendation and projected a completion date of March 31, 2003. We also recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA continue to pursue with the General Services Administration a requirement for the third-party	Open

Condition	Recommendation	Status as of 9/30/03
Facility management has not established internal control to ensure that: • Console logs are reviewed on a regular basis. • Only current employees have console user accounts. • Console account passwords comply with SOP 90-47.	mainframe service provider to undergo an annual SAS 70 type of audit of its data processing facility and make audit results available to SBA. SBA agreed with this recommendation and projected a completion date of August 31, 2005.	
8 A: Only authorized transactions should be entered into the application system and processed by the computer. A written authorization (certification and accreditation) to operate JAAMS was not completed until December 2002. Also, application-specific rules of behavior do not exist. The JAAMS security plan, written during development, has not been updated.	**Recommendation 8A:** We recommend that the Chief Financial Officer in conjunction with OCIO develop rules of behavior for JAAMS and update the application security plan.	**Closed**
B: A formal business recovery plan for JAAMS does not exist.	**Recommendation 8B:** We recommend that the Chief Financial Officer in conjunction with OCIO develop a JAAMS-specific business continuity plan, communicate plan requirements to all impacted employees, contractors, and vendors and update underlying service-level agreements to reflect those requirements.	**Closed**
D: All authorized transactions should be entered into and completely processed by the computer. Three suspense files have unresolved transactions over 30 days old. The most significant of these was the accounts payable suspense file with over 1,000 unresolved transactions worth over $1 million.	**Recommendation 8J:** We recommend that the Chief Financial Officer create and implement policies and procedures to research and resolve all items outstanding in suspense, rejection, and error accounts older than 60 days.	**Closed**
E: SBA inadvertently issued four duplicate payments to grant recipients. The funds were later identified and retrieved. The duplicate payments appear to have been caused by a lack of documented procedures relating to a specific occurrence in the accounts payable daily close process. During the close process, SBA attempted to cancel a	**Recommendation 8K:** We recommend that the Chief Financial Officer ensure that formal documented procedures exist to eliminate the re-occurrence of duplicate payments.	**Closed**

Condition	Recommendation	Status as of 9/30/03
batch accounts payable submission. When the submission was canceled, four payments were still processed. SBA personnel were unaware that these four payments were processed. This error could have been immediately identified with documented procedures instructing the employee to verify that no payments were processed. SBA does not, however, have documented procedures on how or what to do when a batch submission is cancelled in the accounts payable module. We have been informed that procedures have been verbally updated to ensure that duplicate payments are not processed again through the accounts payable close process.		
F: Funds availability in the JAAMS budget module is erroneously fluctuating when end users input incorrect transaction codes. This error appears to be partially caused by inadequate end-user training and incomplete edit and validation checks.	**Recommendation 8L:** We recommend that the Chief Financial Officer provide training and strengthen edits and validations related to funds availability and related procurement and accounts payable transaction codes to prevent the "movement" of funds availability.	**Closed**
G: Cancellation or final closure of a document is designed to cause the related commitment or obligation to reverse, and funds to become available once again. This does not, however, always happen. Therefore, in such cases, the general ledger must be fully researched and corrected.	**Recommendation 8M:** We recommend that the Chief Financial Officer follow up with Oracle to resolve the issue of funds not being released when a document is cancelled.	**Closed**
H: The OCFO has not applied the most recent patches to JAAMS . While OCIO has developed procedures related to obtaining, testing and applying software patches as they are released, these procedures are not being consistently followed.	**Recommendation 8N:** We recommend that the Chief Financial Officer adhere to the policy developed by OCIO and apply all patches necessary to bring JAAMS up to the current patch version as recommended by the vendor.	**Closed**

ATTACHMENT 3: MANAGEMENT COMMENTS AND OUR EVALUATION

The Chief Operating Officer, Chief Information Officer, Chief Financial Officer, and Chief Human Capital Officer provided a consolidated response to the draft report. SBA management generally agreed with recommendations except for recommendations 3B. We have incorporated their comments in this report as appropriate and included their comments and our evaluation of the comments on the following pages.

ATTACHMENT 3A

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

Date: April 8, 2004

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Stephen D. Galvan /S/
Chief Operating Officer/Chief Information Officer

Subject: Response to Draft Audit of SBA's Information Systems Controls

Attached is SBA's response to the draft audit report titled, "Audit of SBA's Information System Controls," which recommends way to improve Agency information system general and application controls. Based on GAO's categorization of information system controls, the draft report reviews and discusses the following areas:

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, and
6. Service Continuity Controls.

In general, SBA agrees with the majority of the recommendations, though not necessarily the specific recommended corrective action(s) identified in response to cited deficiencies. Once the OIG publishes the final report, we will include projected timelines for completing the corrective actions as part of the Agency's response. In the attached response, we have summarized the essence of each audit recommendation, followed by our response.

Attachment a/s

Attachment 3A

OIG Recommendations and SBA Responses

Entity Wide Program Controls – SBA should assign higher priority to resolving audit recommendations, implementing corrective actions, and providing CIO with sufficient resources to minimize entity-wide security program weaknesses as required in statute.

Recommendation 1A: (1) SBA's Administrator should ensure that sufficient resources are provided to OCIO to meet its responsibilities under statute and OMB circulars, and (2) CIO should revise and enhance existing policies and procedures to ensure that proper control weaknesses are resolved, monitoring is effective, technical training made available, existing skill sets sufficient to the tasks, and Office of Chief Information Officer (OCIO) participating in all phases of system development.

Response: SBA agrees with the two recommendations and has already begun to implement them. For example, the SBA Administrator has reorganized the OCIO to report directly to him, assigned the security functions to a separate division within the OCIO raising its visibility, increased the priority assigned to information technology and systems control by designating the Chief Operating Officer (COO) the dual responsibility of COO and CIO, and supported increases in staff and budget for CIO security functions. Assigning the dual responsibility of COO and CIO to one person serves to integrate the IT and security functions more fully into Agency line programs. Furthermore, the COO co-directs the performance monitoring process within the Agency (i.e.. Execution Scorecard), which ensures that we place sufficient priority on resolving control weaknesses and execution of sound internal management principles.

OCIO is also currently revising its policies and procedures that relate to its certification and accreditation reviews and establishing monitoring systems to track implementation of corrective actions, offer project management training to all Agency project managers, and negotiate partnership agreements to define OCIO involvement and commitment with program “owners” at the earliest phases of system development.

Recommendation 1B: CIO should (1) develop policies and procedures to ensure system owners fix weaknesses (2) ensure that plans resolve weaknesses and that effective follow up procedures are developed for corrective action plans, and (3) ensure that sufficient resources are made available to monitor system owner corrective action plans.

Response: We agree with recommendation 1B and will develop appropriate policies and procedures. For major weaknesses, we are including corrective actions into the Agency Scorecard to enable senior management to monitor progress and to ensure corrective actions and execute them in a timely and effective manner. The COO has assigned a senior staff member to track OIG and GAO management weaknesses and execution of corrective actions. Together with implementation of the monthly Scorecard monitoring process, SBA will significantly improve its internal management processes.

2. <u>Access Controls</u>—ineffective controls over the network administration and financial application accounts make SBA vulnerable to unauthorized modification, loss, destruction and disclosure.

<u>Recommendation 2A:</u> [FOIA Ex. 2]

<u>Response:</u> [FOIA Ex. 2].

<u>Recommendation 2B:</u> CFO should ensure that the Director of DFC establishes adequate physical security for routers.

<u>Response:</u> As included in separate response to the draft audit, CFO agrees with the recommendation and OCIO and DFC will determine the best way to improve the physical security for the routers.

<u>Recommendation 2C:</u> CIO should (1) [FOIA Ex. 2], (2) create new network accounts for non-HQ network administrators, and (3) perform periodic reviews of highly-privileged accounts.

<u>Response:</u> CIO agrees with the recommendation to exercise close scrutiny over who continues to have "domain admin" privileges and special accounts and to continue to review the need. It should be noted, however, that at this time senior management has determined that the current 59 accounts are necessary to execute required job functions.

3. <u>Application Software Development & Program Change Controls</u>—change control policies and procedures are not being followed, which makes SBA vulnerable to unauthorized programs or modifications (JAAMS and FRIS)

<u>Recommendation 3A:</u> CFO should require OFM to ensure that all change control forms are complete before changes are released in the production environment.

<u>Response:</u> CFO agrees with this recommendation.

<u>Recommendation 3B:</u> CFO should comply with change control test, acceptance, and validation procedures in SBA's SDM for all credit reform models.

<u>Response:</u> As described in separate response to this draft audit, CFO disagrees with this recommendation for three reasons; namely, (1) OMB has determined that credit subsidy models are not systems, (2) SBA has a Business Technology Investment Council (BTIC) process to determine what is a system and what is reported on Exhibit 300s and 53s, and (3) other credit agencies do not subject their subsidy models to these "systems" requirements.
<u>Recommendation 3C:</u> CIO should develop the means to actively participate in all phases of system development in the Agency.

Response: CIO agrees with this recommendation and has taken the following steps: (1) Reinvigorated the BTIC process (chaired by the Deputy CIO), where the Agency can prioritize and approve development of its systems and ensure that the appropriate offices are collaborating in the development, (2) Ensured that Information Technology efforts are included in the Execution Scorecard monitoring process, and (3) Developed a partnership modeling process whereby program offices sign performance agreements with OCIO to establish performance goals and commitment levels from the onset of systems design efforts.

4. **System Software Controls — Security weaknesses with the network, vendor patches, and improperly configured servers make SBA vulnerable to unauthorized activities from internal sources.**

Recommendation 4A and 4B: CIO should implement corrective actions to address weaknesses identified in Attachment 4 (separate document) and develop policies for monitoring the network for suspicious activity.

Response: CIO agrees with the recommendations.

Recommendation 4C: CIO should perform a security analysis to determine the most effective location for server sensors and revise the IDS vendor's contract to comply with recommendations in this report.

Response: CIO agrees with the need to perform a security analysis, but will determine appropriate performance and metrics for security related activities, including and needed contract modifications.

Recommendation 4D: [FOIA Ex. 2].

5. Segregation of Duty Controls – SBAA has not fully implemented separation-of-duty controls for changes to JAAMS and FRIS used at DFC.

Recommendation 5A: CFO should instruct DFC management to ensure that appropriate procedures are followed in change processes and that management should review all change control forms.

Response: CFO agrees with this recommendation and will respond in detail to the OIG upon receipt of the final FISCAM report.

6. Service Continuity Controls—SBA cannot ensure that disruption in service is minimized in event of disaster and has weaknesses in its continuity of operations plan.

Recommendation 6A: COO should develop a business impact analysis that captures all identified needs within stated recovery times for the Continuity of Operations Plan (COOP) and finalize the draft COOP.

Response: COO agrees with the recommendation and will do a business impact assessment that defines SBA critical business processes, identifies general support systems that need recovery processes, and stipulate required recovery time periods. We will also work with GSA, other federal agencies, and the OIG to determine the appropriate components of the COOP and to ensure effective implementation based on guidelines developed in the ongoing OIG audit of our COOP.

ATTACHMENT 3B

U.S. Small Business Administration
Office of the Chief Financial Officer
Washington, D.C. 20416

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Thomas Dumaresq /S/
Chief Financial Officer

Date: April 5, 2004

Re: Response to Fiscal Year 2003 Federal Information Systems Controls Audit Manual (FISCAM) report

---

This is a response to the draft report issued by the Office of the Inspector General (OIG) "Areas for Improvement in Information System Controls - Fiscal Year 2003 Financial Statement Audit".

The Office of the Chief Financial Officer received three recommendations related to Denver based financial systems (recommendations 2B, 3A and 5A). These recommendations relate to the physical security, change control, and access to these systems. Generally, we agree with these recommendations and we will respond in detail upon the receipt of the final FISCAM report.

Recommendation 3B on SBA's credit subsidy models was for the Chief Financial Officer to comply with change control test, acceptance, and validation procedures in SBA's Systems Development Manual for all credit reform models that have been rebuilt or have undergone significant change. We disagree with this recommendation for three reasons. 1) The Office of Management and Budget (OMB) recently determined that credit subsidy models are not "systems" for the purpose of the systems requirements governing change control test, acceptance, and validation procedure. We agree with OMB's position and think it inappropriate to classify SBA's subsidy models as a system. 2) SBA has an established Business Technology Investment Council (BTIC) composed of senior management and board members; the council is led by the Chief Information Officer/Chief Operating Officer. Through the activities of the BTIC, SBA determines the classifications of systems which are ultimately reported on SBA's Exhibit 53 and Exhibit 300 submissions to OMB. The classification of systems is internal to the agency. 3) Finally, based on our research, other Federal credit agencies do not subject their subsidy models to these "system" requirements.

We have also reviewed Attachments 1A and 1B that use the green/yellow/red color scheme to depict the FISCAM audit results. As agreed upon, all the red-colored boxes under the JAAMS column will be changed to yellow. We have had positive discussions with Cotton & Company and OIG on the attachments and believe that we should strive for a clearer representation of the summary results and its associated colors based on the findings in the FISCAM report.

I thank you for the opportunity to respond to the audit report. We are looking forward to continuing to work with the Office of the Inspector General on future audits.

Audit of SBA's Information System Controls
April 15, 2004
COO/OCIO/OHCM/OCFO Response
(Certain Recommendations were renumbered from the Draft Report)

1. Entity-Wide Security Program Controls

Recommendation 1A: SBA agrees with the two recommendations and has already begun to implement them. For example, the SBA administrator has reorganized the OCIO to report directly to him, assigned the security functions to a separate division within the OCIO raising its visibility, increased the priority assigned to information technology and systems control by designating the Chief Operating Officer (COO) the dual responsibility of COO and CIO, and supported increases in staff and budget for CIO security functions. Assigning the dual responsibility of COO and CIO to one person serves to integrate the IT and security functions more fully into Agency line programs. Furthermore, the COO co-directs the performance monitoring process within the Agency (i.e., Execution Scoreboard), which ensures that we place sufficient priority on resolving control weaknesses and execution of sound internal management principles.

Recommendation 1B: OCIO is also currently revising its policies and procedures that relate to its certification and accreditation reviews and establishing monitoring systems to track implementation of corrective actions, offer project management training to all Agency project managers, and negotiate partnership agreements to define OCIO involvement and commitment with program "owners" at the earliest phases of system development.

Recommendation 1C: We agree with recommendation 1B [1C] and will develop appropriate policies and procedures. For major weaknesses, we are including corrective actions into the Agency Scorecard to enable senior management to monitor progress and to ensure corrective action. The COO meets regularly with each senior manager to discuss OIG suggested corrective actions and execute them in a timely and effective manner. The COO has assigned a senior staff member to track OIG and GAO management weaknesses and execution of corrective actions. Together with implementation of the monthly Scorecard monitoring process, SBA will significantly improve its internal management processes.

2. Access Controls

Recommendation 2A: CIO agrees with each of the elements in the above recommendation and will determine the most cost effective, systematic, and ongoing way for implementing them without jeopardizing daily operations.

Recommendation 2B: As included in a separate response to the draft audit, CFO agrees with the recommendation and OCIO and DFC will determine the best way to improve the physical security for the routers.

Recommendation 2C: [FOIA Ex. 2]

3. Application Software Development and Program Change Controls

Recommendation 3A: CFO agrees with this recommendation.

Recommendation 3B: We disagree with this recommendation for three reasons. 1) The Office of

Management and Budget (OMB) recently determined that credit subsidy models are not "systems" for the purpose of the systems requirements governing change control test, acceptance, and validation procedure. We agree with OMB's position and think it inappropriate to classify SBA's subsidy models as a system. 2) SBA has an established Business Technology Investment Council (BTIC) composed of senior management and board members; the council is led by the Chief Information Officer/Chief Operating Officer. Through the activities of the BTIC, SBA determines the classification of systems which are ultimately reported on SBA's Exhibit 53 and Exhibit 300 submissions to OMB. The classification of systems is integral to the agency. 3) Finally, based on our research, other federal credit agencies do not subject their subsidy models to these "systems" requirements.

Cotton & Company Comments to SBA Response

Cotton & Company does not agree with the CFO response to recommendation 3B in the Draft Report. However, Cotton & Company along with OIG modified finding 3B to reflect only the issues of non-conformance in SBA's Credit Reform Models identified in FASAB Technical Release 3 and 6. Cotton & Company removed its characterization of SBA's credit models as a "financial system" because such characterization was not essential to support our recommendation. We do, however, consider SBA's credit models to fit clearly within OMB's "financial system" definition (see Circular A-127).

Recommendation 3C: CIO agrees with this recommendation and has taken the following steps: (1) Re-invigorated the BTIC process (chaired by the Deputy CIO), where the Agency can prioritize and approve development of its systems and ensure that the appropriate offices are collaborating in the development, (2) Ensured that Information Technology efforts are included in the Execution Scorecard monitoring process, and (3) Developed a partnership modeling process whereby program offices sign performance agreements with OCIO to establish performance goals and commitment levels from the onset of systems design efforts.

4. System Software Controls

Recommendation 4A and 4B: CIO agrees with the recommendations.

Recommendation 4C: CIO agrees with the need to perform a security analysis, but will determine appropriate performance and metrics for security related activities, including any needed contract modifications.

Recommendation 4D and 4E: [FOIA Ex. 2]

Recommendation 4F: CIO partially agrees with this recommendation. We note for the OIG, however, that NIB currently does not have the skill set or tools to administer this task on our network. CIO will review the option of assigning the Security Branch to conduct the network test on SBA's environment. Subsequently, NIB will address any identified vulnerabilities.

5. Segregation-of-Duty Controls

Recommendation 5A: CFO agrees with this recommendation and will respond in detail to the OIG upon receipt of the final FISCAM report.

6. Service Continuity Controls

Recommendation 6A: COO agrees with the recommendation and will do a business impact assessment that defines SBA critical business processes, identifies general support systems that need recovery processes, and stipulates required recovery time periods.

Recommendation 6B: We will also work with GSA, other federal agencies, and the OIG to determine the appropriate components of the COOP and to ensure effective implementation based on guidelines developed in the ongoing OIG audit of our COOP.

ATTACHMENT 5

REPORT DISTRIBUTION

Recipient	**Copies**
Associate Deputy Administrator for Management & Administration	1
General Counsel	3
General Accounting Office	1
Office of the Chief Financial Officer Attention: Jeff Brown	1