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

AUDIT REPORT
Issue Date: March 31, 2003
Number: 3-20

To: Lloyd A. Blanchard, Chief Operating Officer

Lawrence E. Barrett, Chief Information Officer

Thomas A. Dumaresq, Chief Financial Officer

Monika Edwards Harrison, Chief Human Capital Officer

/s/ Original signed

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

Subject: Audit of SBA's Information System Controls for FY 2002

Attached is the audit report on SBA's Information System Controls for FY 2002 issued by Cotton & Company LLP as part of the audit of SBA's FY 2002 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, (6) service continuity controls, (7) review of mainframe operations, and (8) JAAMS applications controls. 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

AUDIT OF SBA'S
INFORMATION SYSTEMS CONTROLS
FOR FISCAL YEAR 2002

AUDIT REPORT NUMBER 3-20

MARCH 31, 2003

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.

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, CISA
MATTHEW H. JOHNSON, CPA, CGFM • SAM HADLEY, CPA, CGFM • COLETTE Y. WILSON, CPA • ALAN ROSENTHAL, CPA

January 29, 2003

AREAS FOR IMPROVEMENT IN INFORMATION SYSTEM CONTROLS FISCAL YEAR 2002 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, 2002, and 2001, and have issued our report thereon dated January 29, 2003, 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 for the period October 1, 2001 through September 30, 2002, 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 further limited our testing to the period under review and therefore did not extend our procedures beyond September 30, 2002. 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 audit included a review of SBA's information system controls. We noted a number of control weaknesses that, taken as a whole, we consider to be a reportable condition. The purpose of this report is to communicate the results of that review and recommendations for improvement.

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.

C&C

established 1981

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

Very truly yours,

COTTON & COMPANY LLP

Charles Hayward, CPA, CISA, CGFM

AREAS FOR IMPROVEMENT IN INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2002 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Cotton & Company LLP was engaged to audit Fiscal Year (FY) 2002 and 2001 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). Below, we communicate results of that review and make recommendations for improvements. Control weaknesses discussed below have been reported in SBA's FY 2002 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 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.

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 that data were processed accurately by the computer. 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 with 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 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 and maintained under contract for 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 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 are operated and maintained under contract for SBA by a third-party vendor at its Eagan, Minnesota, facility. SBA discontinued use of the mainframe-based Federal Financial System and implemented JAAMS on October 1, 2001.

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.

In addition, SBA's financial management activities rely on systems developed, maintained, and operated by external parties, including Colson Services Corporation, Affiliated Computer Services, Inc. – Government Services Group, 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 2002 RESULTS

During FY 2002, SBA continued to improve internal control over its information system environment in certain areas. Additionally, SBA implemented a new accounting and financial management system and a new operating system. These two tasks resulted in new risks for SBA. SBA's major accomplishments this year include the following:

- Conducted certification and accreditation reviews for additional major applications.
- Rolled out the Windows 2000 operating system.
- Implemented a new online data back up system.
- Implemented a new intrusion-detection tool.

These actions are essential elements for a sound information system control environment. Areas for improvements do, however, continue to exist in the six FISCAM general control categories and in all four of the FISCAM application control categories for JAAMS. In the remainder of this report, we discuss these areas and present our recommendations for improvements. Results are summarized in Attachment 1. Management comments and our evaluation are presented in Attachment 2.

1. Entity-Wide Security Program Controls

SBA's Standard Operating Procedure (SOP) 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. We noted four conditions that weaken the overall information system control environment. The most significant of these, Item A below, involves developing an agency-wide integrated security plan.

Office of Management and Budget (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, acquiring, and using information technology. Section 9 requires agencies to develop and maintain an up-to-date 5-year strategic information resources management plan.

Furthermore, OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, 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.

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.

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.

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. Therefore, we are making no recommendation at this time.

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.

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. Therefore, we are making no recommendation at this time.

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

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. Therefore, we are making no recommendation at this time.

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 2002 controls review, the audit team performed external and internal intrusion testing of the network and application access controls.

FOIA Ex. 2

FOIA Ex. 2

FOIA Ex. 2

[redacted]

OMB Circular A-130, Appendix III, requires agencies to establish physical security commensurate with the risk and magnitude of the potential resulting harm. 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 policies and procedures over access to its various systems. Many of the individuals responsible for controlling access are not, however, 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.

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

A. Excessive privileges have been granted to the payroll/personnel systems. Additionally, over 30 different security profiles have been established for the payroll/personnel system. Most of these profiles are for one individual. The combination of these two issues weakens application security controls.

Recommendation 2A: We recommend that the Chief Human Capital Officer review duties and eliminate excessive access granted to the NFC payroll/personnel system. We also recommend that OHCM review its current security profiles and reduce the number of profiles commensurate to job responsibilities.

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 system is increased.

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 later modified to February 20, 2003. Therefore, we are making no recommendation at this time.

C. OCIO has not adequately developed and provided technical training for personnel performing security administration activities either at the network or application level.

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. Therefore, we are making no recommendation at this time.

D. System administrators (network and LAS) at SBA field offices are not effectively carrying out their duties and responsibilities. Additionally, OCIO has not established a method to monitor field office security activities. For instance, we observed the following during field office visits:

- 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.

- Not all network user accounts are properly set up or monitored, require passwords, or require passwords to be changed every 90 days.

- System administrators do not always set all accounts to lock out or become disabled after three failed login attempts.

We recommended in our Information System Controls Report for FY 2001 (OIG 02-18) that SBA 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. SBA agreed with this recommendation and initially projected a completion date of November 1, 2002. This projected completion date was later modified to December 1, 2003. Therefore, we are making no recommendation at this time.

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.

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. We did not validate that corrective action had been successfully completed as corrective action occurred after the end of audit fieldwork. Therefore, we are making no recommendation at this time.

3. Application Software Development and Program Change Controls

SBA's application software development and program change controls are designed to prevent implementation of unauthorized programs or modifications to existing programs. As noted in the prior year, documentation for system and program changes is outdated, and documentation supporting tests of program changes is inadequate. 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.

NIST Special Publication 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* 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 that a program will operate 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 increased costs for additional software development to correct unwanted, erroneous code.

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 policies at the beginning and throughout the System Development Life Cycle (SDLC).

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. Therefore, we are making no recommendation at this time.

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.

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. Therefore, we are making no recommendation at this time.

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 impact the adequacy of control to protect network operations from unauthorized activities from internal sources.

Although OCIO has practices for installing recommended operating software and hardware fixes and patches for known security vulnerabilities, these practices are 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 permitting access to applications and software.

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. 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.

B. OCIO has not developed the means to test user password configurations to enforce SBA's password configuration requirements. Also, OCIO has not identified and removed invalid or unnecessary group accounts shared by a number of individuals.

Recommendation 4B: We recommend that the Chief Information Officer develop and implement policies and procedures to require:

- All network administration accounts to be password-protected and require passwords on those accounts to be changed every 30 days.

- Periodic review of all administrative-level accounts and a limit placed on the number of individuals granted this access.

- SBA to annually review its use of group accounts for only those group accounts that are valid and necessary for sound network management and SBA to prohibit the use of generic accounts.

- All system users to use more robust passwords, to include the combination of alpha, numeric and special characters.

C. We noted instances where personnel were using unauthorized remote access software. Recently, OCIO has not developed and implemented written procedures for the proper use of remote access software.

Recommendation 4C: We recommend that the Chief Information Officer enforce the procedures currently in place and remove all unauthorized remote desktop software from workstations.

D. The configuration of Windows 2000 on SBA workstations and servers is not adequate to ensure security over SBA data and network operations.

Recommendation 4D: We recommend that the Chief Information Officer provide a standard configuration for Windows 2000 consistent with NIST and NSA guidelines. We further recommend that the Chief Information Officer complete the implementation of Windows 2000, including the Exchange servers, so that Windows 2000 can run in Native mode, and security features can be properly and fully utilized.

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.

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.

G. Administrators and security personnel are not adequately trained to allow them to fully understand their responsibilities and handle possible security violations.

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.

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. We noted two instances where segregation of duties was inadequate.

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, Appendix III 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 theft, malfeasance, and/or a loss of funds.

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.

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.

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. As a result, we are making no recommendation at this time.

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.

SBA has developed a draft Continuity of Operations Plan (COOP). However, these efforts have not been driven by the operational groups of SBA but rather by the Chief Information Officer. The goal of a COOP is to allow an organization to continue its business operations in the event of a disaster. Therefore, it is the responsibility of the operational groups headed by the Chief Operations Officer within an organization to determine what business requirements are necessary in the event of a disaster to continue operations. These requirements should be based on the critical business processes that an organization executes. These requirements should include the information resources, space resources, and other tools which will be needed to continue operations. Additionally, the operations group should determine the time frames necessary to recover these resources.

Typically this process referred to above is initiated by identifying the critical processes an organization performs and determining what length of time the organization could go without executing these processes. This will assist the organization in making recovery time frame decisions.

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.

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

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.

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.

C. 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.

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. Therefore, we are making no recommendation at this time.

7. Review of Mainframe Operations

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. Thus, we reviewed and assessed control over the mainframe service provider's operations and physical facilities.

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

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:

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.

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. Therefore, we are making no recommendation at this time.

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 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. Therefore, we are making no recommendation at this time.

8. Application Control Review of JAAMS

JAAMS was implemented in October 2001. SBA moved JAAMS from the software developer's facilities in December of 2001 to SBA's regular out sourcing provider data processing facility.

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. Appendix III also requires agencies to implement programs to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Finally, SOP 90-47 specifies controls applicable to user passwords and log-on attempts.

We identified the following application control deficiencies while performing our review of JAAMS.

Authorization Controls

Only authorized transactions should be entered into the application system and processed by the computer.

A. 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.

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.

C. We noted the following application security deficiencies within JAAMS:

- Auditing functionality of individuals, events, or transactions has not been established, and audit logs have not been enabled within Oracle.
- System administrator or UNIX root passwords are not forced to be changed every 60 days.
- JAAMS does not support maintaining a password history, disable a user after a failed number of log-in attempts, or prevent concurrent log in by the same user ID.
- Several users have excessive access privileges, and several have access differing from their access request forms. Procedures for periodically reviewing user access do not exist.
- We noted 199 inactive user accounts (not been logged into for over 90 days).
- The JAAMS security administrator is not signing access request forms, and an access request form was missing in one instance.
- The current responsibility matrix used by OCIO security does not contain all user profiles. Also, OCIO security has granted access inconsistent with the responsibility matrix, which resulted in excessive privileges.
- Security officers within OCIO do not have the requisite functional knowledge and have not received the appropriate training to adequately administer JAAMS security.

Recommendation 8C: We recommend that the Chief Financial Officer in conjunction with OCIO determine what critical security events are to be logged, enable Oracle auditing to log those events, and identify an appropriate individual to monitor audit logs daily.

Recommendation 8D: We recommend that the Chief Financial Officer in conjunction with the Chief Information Officer require that the third party outsourcer ensure that system administrator or UNIX root passwords be changed every 60 days.

Recommendation 8E: We recommend that the Chief Financial Officer in conjunction with OCIO update systematic password and log-in controls in JAAMS to be consistent with SBA standard password policy. These controls should include creation of a password history log to prevent repeat use of passwords, systematic controls to lock out users after a number of failed log-in attempts, and systematic controls to prevent concurrent logins from the same user ID.

Recommendation 8F: We recommend that the Chief Information Officer ensure that all users are approved before being granted access to JAAMS. We further recommend that the Chief Information Officer enforce procedures to ensure that the JAAMS security administrator sign and retain all user access forms before access is granted to a new user.

Recommendation 8G: We recommend that the Chief Information Officer in conjunction with OCFO require the JAAMS security administrator to perform an annual review of JAAMS users to ensure that no user has excessive access, and that all users are current, authorized JAAMS users.

Recommendation 8H: We recommend that the Chief Information Officer in conjunction with OCFO require the JAAMS security administrator to use a responsibility matrix to determine if requested access should be granted to a user. This JAAMS responsibility matrix should be updated and reviewed to reflect all current profiles and incompatible duties.

Recommendation 8I: We recommend that the Chief Information Officer provide adequate Oracle security administration training and periodic retraining to enable JAAMS security administrators to effectively perform their duties.

Completeness Controls

All authorized transactions should be entered into and completely processed by the computer.

D. 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.

Accuracy Controls

The recording of valid and accurate data into an application system is essential to provide for an effective system that produces reliable results.

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 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.

Recommendation 8K: We recommend that the Chief Financial Officer ensure that formal documented procedures exist to eliminate the re-occurrence of duplicate payments.

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.

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.

Controls Over the Integrity of Processing and Data Files

These controls include procedures ensure that the current version of production programs and data files are used during processing and that application security processes data as intended.

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.

ATTACHMENT 1: SUMMARY OF RESULTS

FY 2002 CFO AUDIT INFORMATION SYSTEMS CONTROL REVIEW	SYSTEM					
GENERAL CONTROL CATEGORIES AND SPECIFIC CONTROL TECHNIQUES	**OCIO LAS**	**ALCS**	**JAAMS**	**DFC**	**LANs WANs**	**SBG**
ENTITY-WIDE SECURITY PROGRAM CONTROLS						
Risks are periodically assessed.	1	1		1	1	1
Security program is documented.	2	1		1	1	1
Security management structure is in place and responsibilities assigned.	2	1		1	2	2
A personnel security policy is established.	2	1		1	1	1
A security-monitoring program is established.		2		2		2
ACCESS CONTROLS						
Information is properly classified.	1	1	1	1	1	1
User access and privileges are authorized.	2	2	2	1	2	2
Physical and logical controls prevent and detect unauthorized activities.	2	2		1		2
Apparent unauthorized activities are monitored and investigated.	2	2		1		2
APPLICATION SOFTWARE DEVELOPMENT AND PROGRAM CHANGE CONTROLS						
Program modifications are documented, reviewed, tested, and approved.	2	1	2	1	4	2
Program changes are documented, reviewed, tested, and approved before releasing to production.	2	1	2	1	4	2
Movement of programs in and out of libraries is authorized.	1	1	2	1	4	2
SYSTEM SOFTWARE CONTROLS						
Access to system software is limited.	2	2		1	2	1
System access is monitored.	2	2		1	2	1
Changes to system are authorized and documented.	1	1	2	1	1	1
SEGREGATION-OF-DUTIES CONTROLS						
Incompatible duties are identified.	1	1		1	1	1
Segregation of duties is enforced through access controls.	2	2		1	2	2
Segregation of duties is enforced through formal operating procedures and supervisory review.	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

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.

FY 2002 CFO AUDIT
INFORMATION SYSTEMS CONTROL REVIEW

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

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. Note that we performed application controls work specific to JAAMS for the FY 2002 audit. We have reviewed application control procedures for other significant applications in the past, however the GAO guidance related to application controls was not available at that time and therefore we do not present analysis as they relate to these standards.

ATTACHMENT 2: 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 agreed with 19 of the 25 recommendations and partially agreed with the remaining 6 recommendations. We have incorporated their comments in this report as appropriate and their comments and our evaluation of the comments are included on the following pages.

Date: March 25, 2003

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Lloyd A. Blanchard
Chief Operating Officer

Lawrence E. Barrett
Chief Information Officer

Thomas A. Dumaresq
Chief Financial Officer

Monika Edwards Harrison
Chief Human Capital Officer

Subject: Audit of SBA's Information System Controls for FY 2002

The draft audit report for the FY 2002 audit of SBA's Information Systems Controls dated February 20, 2003 provides the SBA with recommendations to four offices. Coordination with the COO, OCIO, OCFO and OHC has been completed and the responses addressing the recommendations are enclosed. In addition, comments are included with the responses.

Thank you for the opportunity to provide comments to the draft Information Systems Control letter.

Audit of SBA's Information System Controls
February 20, 2003
COO/OCIO/OHCM/OCFO Response

1. Entity-Wide Security Program Controls

Recommendation 1A: We agree with the recommendation. The Office of Human Capital Management will designate the system a major Agency application. OCIO and OHCM will perform a C&A review of **SBA's component** of the NFC payroll/personnel system and develop associated plans for the system.

2. Access Controls

Recommendation 2A: We agree with the recommendation. Our staff has reviewed the access granted to 56 SBA employees and found that some have system-wide access or access to portions of the system that they don't need to perform their current duties. We have been in touch with NFC to remedy this situation, and expect that changes to their access will be effective by the end of this month.

4. System Software Controls

Recommendation 4A: We agree with the recommendation.

Recommendation 4B: We partially agree with the recommendations. There are certain instances where group passwords are both necessary and appropriate. In those instances we will continue to use them and accept any associated risks. As of the completion of the windows rollout, all workstation users are forced by the system to adhere to Agency password policy which mandates inclusion of alphanumerics, multi case, and special characters. Where appropriate we will reiterate and enforce Agency password composition policy.

Cotton & Company Comments: We partially agree with SBA's response and have modified our recommendation accordingly. As SBA pointed out in its response, certain group passwords are a necessary component of good network management even though these accounts have increased risk. However, SBA had 742 group accounts when we performed our audit work. SBA should annually review its group accounts and ensure that only valid and necessary accounts are defined to the network.

Recommendation 4C: We agree with the recommendation.

Recommendation 4D: We agree with the recommendation.

Recommendation 4E: We agree with the recommendation. We already require a preliminary certification and accreditation review be performed on systems before implementation.

Recommendation 4F: We partially agree with the recommendation. OCIO applies patches to its systems which are appropriate to the services being run. In many cases Microsoft releases patches for components of the operating system that are not installed within the Agency. We suggest rewording this recommendation to install all **relevant appropriate** patches to the system.

Cotton & Company Comments: Agree with SBA's response and have modified the recommendation accordingly. However, we must point out that SBA must be very diligent and ensure that relevant and appropriate patches are timely implemented. Testing of the Windows 2000 network has identified that relevant and appropriate patches have not always been timely implemented.

Segregation-of-Duty Controls

Recommendation 5A: We agree with the recommendation but recommend redirection to the OCFO. In consultation with OCIO, OCFO will address this finding.

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

Service Continuity Controls

Recommendation 6A: We partially agree with the recommendation. OCIO is developing a comprehensive COOP plan which includes the recommended recovery timelines. We see the Chief Operating Officer's role as emphasizing the importance of the COOP plan to senior executives and assisting in moving the process forward through the program offices.

Cotton & Company Comments: Partially agree with SBA's response. We have reworded the finding to better describe the Chief Operating Officer's role in service continuity as requested in follow-up meetings to the draft FISCAM audit report.

Recommendation 6B: We partially agree with the recommendation. OCIO is already following the afore-mentioned process in its COOP development. Again we see the Chief Operating Officer's role as that of an advocate.

Cotton & Company Comments: Partially agree with SBA's response. A timeline for completion of the final COOP should be estimated. Additionally, all items identified in finding 6B are recommended for inclusion in the final COOP.

Review of JAAMS

Cotton & Company Comments: The review of JAAMS was reordered from the draft report to be more in the order of the U.S. General Accounting Office's Federal Information System Controls Audit Manual for Application Controls. The original recommendations and responses from SBA have also been reordered to reflect this change. There has been no change in report content unless it was requested by SBA.

Authorization Controls

Recommendation 8A: We partially agree with the recommendation. OCIO has developed generic rules of behavior that are applicable to all major applications at the SBA, including JA^{2}MS. The procedural notice was implemented and in effect on January 2nd, 2003. We believe that a well-crafted set of rules of behavior should be generic in nature and should be applicable to all systems.

Cotton & Company Comments: Partially agree with SBA's response. A well-crafted generic set of rules of behavior are a good beginning to drill-down into specific SBA systems and identify the individual control features in each application. Identification of these internal control features with incorporation into application specific rules of behavior will ensure that there is an internal control system which appropriately utilizes those features.

Recommendation 8B: We agree with the recommendation. OCIO in conjunction with OCFO has developed a Disaster Recovery test plan with a test date set of March 20, 2003. The full

Disaster Recovery test was conducted in Roseville, Minnesota and included contractors and employees. Service level agreements are already in place in the SBA contract for JAAMS support with Unisys.

Recommendation 8C (Draft Report 8H): We agree with this recommendation.

Recommendation 8D (Draft Report 8I): We agree with the recommendation but recommend redirection to OCFO. In consultation with OCIO, OCFO will request this change from Unisys.

Recommendation 8E (Draft Report 8J): We agree with the recommendation but recommend redirection to OCFO. In consultation with OCIO, OCFO will work on the controls.

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

Recommendation 8F (Draft Report 8K): We partially agree with the recommendation. OCIO already requires a completed ID request form signed by a responsible official. Security officers currently retain all application documents. (During this review apparently the security officer could not find 1 document which generated this part of the recommendation).

Cotton & Company Comments: Agree with SBA's response.

Recommendation 8G (Draft Report 8L): We agree with the recommendation but recommend redirection to OCIO and OCFO. The CFO's office will assist OCIO with an annual, not quarterly, review.

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

Recommendation 8H (Draft Report 8M): We agree with the recommendation but recommend redirection to OCIO and OCFO. The OCFO office has full responsibility for maintaining the JA^{2}MS responsibility matrix to reflect ongoing changes to application roles and permissions. OCIO will utilize the responsibility matrix for security administration.

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

Recommendation 8I (Draft Report 8N): The CFO's office will provide internal training to the JA^{2}MS security administrators. OCIO will provide travel funds.

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

<u>Completeness Controls</u>

Recommendation 8J (Draft Report 8F): We agree with this recommendation except we believe 60 days is more realistic timeframe to implement a correction.

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

Accuracy Controls

Recommendation 8K (Draft Report 8C): We agree with this recommendation.

Recommendation 8L (Draft Report 8D): We agree with this recommendation.

Recommendation 8M (Draft Report 8E): We agree with this recommendation.

Controls Over the Integrity of Processing and Data Files

Recommendation 8N (Draft Report 8G): We agree with this recommendation.

Attachment 3

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