AUDIT OF SBA'S
INFORMATION SYSTEMS CONTROLS
FISCAL YEAR 2004
AUDIT REPORT NUMBER 5-12

FEBRUARY 24, 2005

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

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

AUDIT REPORT
Issue Date: February 24, 2005
Number: 5-12

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

Jerry E. Williams
Acting Chief Information Officer

Thomas A. Dumaresq
Chief Financial Officer

Richard Brechbiel
Chief Human Capital Officer

/S/ Original Signed

From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's Information Systems Controls for FY 2004

Attached is the audit report on SBA's Information Systems Controls for FY 2004 issued by Cotton & Company LLP as part of the audit of SBA's FY 2004 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.

Responses from the Chief Financial Officer, Chief Human Capital Officer, and Acting Chief Information Officer (CIO) are included as attachments to this report. However, the response from the Acting CIO was condensed and the attachments (A-D) that accompanied the response from the Acting CIO were not included in the final report. The attachments from the Acting CIO were reviewed and considered as part of our final report.

SBA generally agreed with the auditor's findings and recommendations with the exception of finding 3A on application software development and program change control, and finding 5A on segregation of duty controls for the Loan Accounting System (LAS). Finding 3A and recommendation 3A were modified to more reflect what was found during audit fieldwork. Finding 5A and recommendation 5B were not changed or modified as the CIO must adequately ensure that security is enforced in LAS Agency-wide.

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 R Brindle, Director, Information Technology and Financial Management Group at (202) 205-[FOIA Ex. 2].

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

November 15, 2004

AUDIT OF INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2004 FINANCIAL STATEMENT AUDIT

Inspector General
U.S. Small Business Administration

We audited the financial statements of the U.S. Small Business Administration (SBA) as of and for the years ended September 30, 2004, and 2003, and have issued our report thereon dated November 15, 2004. In that report, we issued an unqualified opinion on the Fiscal Year (FY) 2004 combined statement of budgetary resources and the FY 2003 consolidated balance sheet (as restated); issued a qualified opinion on the FY 2004 consolidated balance sheet and statements of net costs, changes in net position, and financing; and disclaimed an opinion on the FY 2003 consolidated statements of net cost, changes in net position, and financing and the combined statement of budgetary resources. 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/ Original Signed
Charles Hayward, CPA, CISA

C&C
established 1981

AUDIT OF INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2004 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Cotton & Company LLP was engaged to audit Fiscal Year (FY) 2004 and 2003 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 Government Accountability 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.
- Government Information Security Review Act (GISRA), now the 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 our recommendations for improvements. Control weaknesses discussed herein have been reported in SBA's FY 2004 financial statement internal control report as a reportable condition.

BACKGROUND

General controls are the policies, procedures, and practices that apply to all or to a large segment of an entity's information systems to help ensure their proper operation. General controls affect 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 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 a third-party vendor, Corio, Inc., in Tempe, Arizona. Corio has a second facility in California housing the JAAMS test environment. The California facility also serves as the alternate computing facility for JAAMS in the event that the Tempe, Arizona facility becomes inoperable.

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 Subsidy Calculator and Monster Databases,** a series of SAS and JAVA programs and Microsoft Excel spreadsheets developed and maintained by OCFO 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 USDA 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 2004 RESULTS

SBA continued to improve internal control over its information system environment during FY 2004 in certain areas. Specifically, SBA:

- Conducted certification and accreditation (C&A) reviews for additional major applications.
- Continued to implement the Windows 2000 operating system at various field locations.
- Conducted a disaster recovery exercise.

These accomplishments were, however, overshadowed by the following identified weaknesses:

- SBA does not have an adequate information technology training program in place.
- SBA has not initiated prompt action to correct known deficiencies. Specifically, out of the 26 recommendations for 13 findings noted in FY 2003, 14 recommendations were not adequately addressed.

- Duties within financial applications are not adequately segregated. JAAMS security administration and user account administration privileges have been granted to several individuals. In addition, one user was identified as having both financial and Information Technology (IT) incompatible duties within JAAMS.
- Policies and procedures for the administration of the network operating system (Windows 2000 O/S) have not been developed.
- No minimally acceptable baseline configuration exists for the Sun Solaris (UNIX) operating system housing JAAMS, the Windows 2000 domain controllers, the Sybase database management system (DBMS), and the Oracle DBMS that support JAAMS. In addition, we found several weaknesses within the configuration of these platforms when compared with federal guidance and industry best practices as promulgated by the Center for Internet Security on properly securing the relative platforms.
- Access authorizations to the SBA Network, JAAMS, LAS, and the Sybase general support systems are not adequate. Access authorization forms are not required for the network, Sybase, and LAS. Access authorization forms are required for JAAMS; however, not all forms could be located for review.
- Emergency access authorizations to SBA's Network, JAAMS, LAS, and the Sybase general support system are not adequate.
- Network, JAAMS, and LAS password controls are weak.
- Review of inactive accounts is not being performed on the network, LAS, or the Sybase general support system.
- Logging and monitoring of SBA general support systems and JAAMS is not adequate.
- Business Resumption plans have not been completed and fully incorporated into SBA's Continuity of Operations Plan (COOP).

In the remainder of this report, we discuss results of our FY 2004 review and the status of management actions to address prior-year recommendations and new weaknesses identified in FY 2004. We also present our recommendations for improvements. This report includes the following attachments:

Number	Title
1	FY 2004 Summary of Results
2	Status of Prior-Year Audit Recommendations
3	Management Comments and Our Evaluation A – Response from Acting Chief Information Officer B – Response from Chief Financial Officer C – Response from Chief Human Capital Officer D – OCIO/OHCM/OCFO Response with Auditor Comment
4	Network Analysis Results (Limited Official Use and Restricted Distribution)
5	Windows 2000 Configuration Review Results (Limited Official Use and Restricted Distribution)
6	Oracle Database Configuration Review Results (Limited Official Use and Restricted Distribution)
7	Sybase Database Configuration Review Results (Limited Official Use and Restricted Distribution)
8	UNIX Configuration Review Results (Limited Official Use and Restricted Distribution)

ATTACHMENT 1

FY 2004 SUMMARY OF RESULTS

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.

We identified the following entity-wide security program control weaknesses during our FY 2004 financial statement audit:

A. A policy requiring mandatory vacation or job rotation for employees in sensitive positions has not been developed, and sensitive positions have not been formally identified and documented by OCIO. NIST Special Publication (SP) 800-14 "Generally Accepted Principles and Practices for Security Information Technology System" states that mechanisms besides auditing and analysis of audit trails should be used to detect unauthorized and illegal acts. Rotating employees in sensitive positions, which could expose fraudulent activities that required an employee's presence, is one method that can be used.

Recommendation 1A: We recommend that the Chief Human Capital Officer develop a policy requiring:

- Periodic job rotations and/or mandatory annual vacations for employees in sensitive Information Technology positions, or
- Temporary re-assignment of work of employees in sensitive Information Technology positions to other employees.

Recommendation 1B: We recommend that the Chief Information Officer include job shift and mandatory vacation requirements in the Security Program Plan SOP 90-47-1 and develop procedures to comply with the new policy.

B. An information technology training program has not been developed, and training and professional development are not documented and monitored for SBA system administration staff. This is especially significant for those personnel who operate SBA general support systems and major applications. Federal agencies cannot protect the confidentiality, integrity, and availability of information without ensuring that each person involved understands his or her role and responsibilities and is adequately trained to perform them. OCIO has not identified and requested the necessary resources to implement an effective employee training program.

Audit report (OIG 2-18) issued on May 6, 2002 recommended that the Chief Operating Officer provide adequate funding and resources to allow OCIO to develop and implement technical training for security staff and all network and application security administrators. Additionally, audit report (OIG 4-19) issued on April 29, 2004 recommended that the Chief Information Officer ensure that adequate technical training for SBA personnel including network and system personnel in accordance with NSA, NIST and Windows 2000 best practices. SBA responded to the initial recommendation in report (OIG 2-18) that adequate funding for technical training would be implemented by March 1, 2003. This recommendation remains open and documentation of adequate funding has not been provided. SBA responded to one of the two recommendations in audit report (OIG 4-19) that adequate technical training would be provided by March 31, 2005. SBA did not respond to the other recommendation which was due to OIG on May 29, 2004. Therefore, we are making no new recommendations at this time.

C. SBA does not initiate prompt action to correct known deficiencies, and corrective actions are not monitored on a continuing basis. OCIO developed a database for tracking recommendations identified in prior audits; however, this database is not being adequately maintained. Out of 26 recommendations for 13 findings noted in our FY2003 FISCAM report, 14 recommendations were not adequately addressed. In addition, we noted 40 recommendations in SBA's Plan of Action and Milestone (POA&M) document that remained unresolved past their scheduled completion dates. Of these 40 recommendations, 20 were more than 200 days past their scheduled completion date. OCIO responded in the initial exit meeting that they did not have adequate resources to oversee and ensure that audit recommendations were timely adjudicated.

Audit report (OIG 4-19) issued on April 29, 2004 recommended that the 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. SBA has not provided a response to the recommendation in audit report (OIG 4-19) which was due to OIG on May 29, 2004. Therefore, we are making no new recommendations at this time.

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 2004 controls review, we performed access control testing at the network, application, database, and operating system level. We noted the following access controls weaknesses:

A. Controls are not adequate to ensure that access authorizations are documented on standard forms, maintained on file, approved by senior managers, securely transferred to security managers, and that owners periodically review access authorizations to determine their appropriateness.

NIST SP 800-14, *Generally Accepted Principles and Practices for Security Information Technology System*, states that organizations should have a process for requesting, establishing, issuing, and closing user accounts, and for tracking users and their respective access authorizations. NIST also states that it is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, the conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth.

Access requests to SBA's network, LAS, and Sybase general support systems (Sybase) do not require documentation on standard forms that are retained. Access requests are submitted verbally or by e-mail to system administrators. In addition, because access requests are not being retained, owners are unable to periodically verify that the access users currently have was authorized.

The OCFO does require that access requests to JAAMS be documented on the Computer Access Security Request Form (Form 2200) and retained; however, our review determined that controls over the retention of access request forms need improvement. Out of 45 active accounts sampled, we identified six that could not be traced to access request forms.

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

- Develop policies and procedures requiring that access requests be documented on standard access request forms and retained.
- Develop a policy requiring that access request forms be periodically traced to active users to ensure user's access agrees with the authorization on the access request forms.

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

- Ensure access to JAAMS is granted only when requested via Form 2200.
- Ensure all access request forms are maintained on file for future reference. Access request forms should be periodically traced to active user accounts to make sure access in JAAMS agrees with the access that was requested and approved.

B. Controls are not adequate to ensure that emergency access authorizations are documented on standard forms, are approved by appropriate managers, are securely communicated to the security function, and are automatically terminated after a predetermined period of time.

Policies and procedures for granting emergency or temporary access to the network, LAS, JAAMS, and Sybase have not been developed and documented.

OCIO and OFS stated that normal procedures for granting access to the network and financial applications would be followed in an emergency; however, the request would be prioritized and pushed through the normal channels more rapidly.

In an emergency, excessive or inappropriate access may be granted. Accounts created for temporary access may remain active after the period of intended use, increasing the risk of unauthorized or malicious activities.

Recommendation 2C: We recommend that the Chief Information Officer in conjunction with OCFO:

- Develop and document policies and procedures for granting emergency and temporary access to the network, JAAMS, LAS, and Sybase.
- Require that emergency and temporary access request be documented on a standard form and retained for future reference.

C. Controls are not adequate to ensure that passwords for the network, LAS, and JAAMS are changed periodically, are at least eight alphanumeric characters in length, are prohibited from reuse for at least eight generations, and that attempts to log on with an invalid password are limited to three to five attempts. SBA's SOP 90-47-1, *Automated Information System Security Program*, states that passwords must be at least eight characters, must be set to automatically expire every 90 days, and should contain a history of the last eight passwords. In addition, NIST SP 800-14, *Generally Accepted Principles and Practices for Security Information Technology System*, states that organizations should limit the number of failed-login attempts.

[FOIA Ex. 2]

[FOIA Ex. 2]

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

- Develop procedures to ensure all network accounts are created in accordance with SBA policy.
- Periodically review network accounts to ensure compliance with policy.

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

- Develop and implement program changes for LAS to force users to change their password every 90 days, in accordance with SBA policy
- Develop and implement program changes to force LAS accounts to lock after three to five failed attempts at logging in. Accounts should be locked until reset by the system administrator.

Recommendation 2F: We recommend that the Chief Financial Officer continue with the planned upgrade of the Oracle application and database for JAAMS. Security settings should be enabled to enforce strong password controls, including password history and automatic lock-out after a set number of failed login attempts.

D. Controls are not adequate to ensure that inactive user accounts are monitored and removed when no longer needed. Periodic reviews of network, LAS, and Sybase accounts are not being performed. OCIO has a process in place in which they are notified by HR when employees leave so their accounts can be disabled or deleted; however, this process does not include contractors and does not identify unused accounts. If an employee's account is not disabled or deleted during the exit process, it will remain active. SBA policy and NIST SP 800-14, *Generally Accepted Principles and Practices for Security Information Technology Systems*, require that accounts be periodically reviewed to ensure access is appropriate.

As noted in our FY2003 report, OCIO is not performing periodic reviews of network accounts to remove inactive accounts in accordance with SOP 90-47-1, which states that network accounts should be reviewed monthly to determine continuing need. In addition, OCIO stated that they cannot readily identify which accounts on the network are active vs. inactive. Of the 1,483 accounts we reviewed for inactivity, 472 accounts had not been used in more than three months. Responsibility for reviewing SBA's network accounts was assigned during FY2003; however, the individual assigned with responsibility for this task transferred within SBA, and OCIO did not reassign responsibility.

In addition to the network, OCIO is not performing periodic reviews of LAS and Sybase accounts to identify and remove inactive accounts. Although SBA does have a policy stating that network accounts should be reviewed on a periodic basis, no such policy or procedures exists for the periodic review of other system accounts. Without a policy and procedures for the periodic review of network and application accounts, the likelihood of unauthorized individuals gaining access to SBA's network or financial application is increased. Inactive accounts could potentially be used by unauthorized individuals to perform malicious activities on the network.

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

- Conduct monthly reviews of network accounts, as required by SOP 90-47-1, to include identifying inactive accounts. These accounts should be reviewed to determine if they are still necessary.
- Investigate acquiring an automated tool to aid in differentiating active vs. disabled accounts on the network.

Recommendation 2H: We recommend that the Chief Information Officer develop a policy and procedures requiring the periodic review of all SBA accounts (General Support System and Major Application). Assign responsibility for executing these new procedures.

E. Logging and monitoring controls at the network and application level are weak. SBA has no policies and procedures identifying which activities should be logged and how to determine these activities, and has not specified who should review logs and how often. SBA briefly discusses logging in their Procedural Notice 9000-1407 and SOP 90-47-1; however, not at a level sufficient to ensure that individuals know what to log, who should review the logs, what the logs should be reviewed for, and how often they should be reviewed.

From our review of the network, LAS, Sybase, and JAAMS, we determined that logging and monitoring activities are not occurring on SBA's general support systems and major applications.

Specifically:

- Activities on SBA's network are being logged; however, these logs are not being reviewed on a regular basis. When the logs are reviewed, it is by the Network Integration Branch (NIB) and not OCIO security. In addition, we determined that logs are only retained for two weeks before they are overwritten due to limited storage capacity.
- Database administration activities in the Oracle database supporting JAAMS are not logged. The only logging enabled at the database level is for the tracking of two SBA employees with powerful access rights. In addition, although OCFO claimed they are using forms-level auditing on the JAAMS application, they could not provide sufficient information to detail what activities were logged, who reviewed these logs, what the logs were reviewed for, and how often they were reviewed.
- Logging was not enabled in Sybase, therefore Sybase activity was not being adequately monitored.
- Logging and monitoring of activities within LAS is not taking place. LAS does log activities such as failed logons however no individual in OCIO is currently assigned with responsibility for reviewing these logs.

Recommendation 2I: We recommend that the Chief Information Officer for all SBA internal and contractor supported general support systems and major applications e.g. Egan Mainframe; SBA and Corio UNIX; Network and Windows 2000; Loan Accounting System, Sybase, Mainframe; JAAMS Oracle, and related application functions:

- Develop and document policies and procedures clearly outlining what activities should be logged, who should be responsible for reviewing logs, what the logs should be reviewed for, how often logs should be reviewed, and how long logs should be retained.
- Assign responsibility within OCIO Security for the review of application and general support system security logs.
- Retain audit logs for a sufficient period of time (at least 90 days).

Recommendation 2J: We recommend that the Chief Financial Officer:

- Require that all activities by Oracle database administrators be logged.
- Require periodic review of database logs by someone outside of Corio, preferably an individual within OFS or OCIO Security with an understanding of the production Oracle database. Audit logs should not be reviewed by the individuals being audited.
- Take steps necessary to ensure all activity in JAAMS involving access to and modifications of sensitive or critical files at the application level are logged.
- Assign responsibility for the periodic review of JAAMS application logs.

F. Controls over the Oracle database supporting JAAMS are weak. [FOIA Ex. 2]

Our review identified system configuration and logical access control vulnerabilities. The specific security related conditions are detailed in Attachment 6 (Limited Official Use and Restricted Distribution).

We identified 42 vulnerabilities, of which 4 were considered high risk, 16 medium risk, and 22 low risk. The following conditions contributed to the high-risk vulnerabilities.

Recommendation 2K: We recommend that the Chief Information Officer in conjunction with OCFO:

- Use the CIS benchmark to ensure that adequate security is incorporated into the planned Oracle upgrade.

- Develop a minimally accepted security baseline configuration for the Oracle database platform which would be utilized for all SBA Oracle database management systems.

G. Controls over SBA's Sybase database are weak. Our review identified system configuration and logical access vulnerabilities. Specific security related conditions are detailed in Attachment 7 (Limited Official Use and Restricted Distribution).

Of the 23 vulnerabilities identified one was considered high risk, 13 medium risk, and the remaining nine were considered low risk.

[FOIA Ex. 2]

Recommendation 2L: We recommend that the Chief Information Officer develop and implement a corrective action plan with specific milestones to address the database weaknesses identified in Attachment 7 (Limited Official Use and Restricted Distribution) in a timely manner. In addition, we recommend that OCIO develop a minimally accepted security baseline configuration for the Sybase platform which would be utilized for all SBA Sybase database management systems

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 and modifications to existing programs, and should ensure that security is adequately incorporated into the development and change of programs. Our review of change controls for JAAMS and LAS identified the following weaknesses:

A. Change controls for LAS need improvement. Through our change control testing for LAS, we determined that OCIO personnel responsible for maintaining LAS were not aware of documented change control procedures for LAS, nor SDM configuration management procedures Agency-wide.

In addition, we determined that:

- Test plan standards for LAS have not been developed for all levels of testing that define responsibilities for each party,
- Documentation standards have not been developed that defines a sufficient amount of documentation on changes to code and operational procedures,
- LAS data center supervisors and/or security officers do not periodically review production program changes to determine whether access controls and change controls have been followed.

When documented change control policies and procedures are not adequately communicated and enforced, SBA has less assurance that changes introduced into production have gone through necessary controls. Changes introduced into production may contain malicious or harmful code or can potentially have a negative impact on the functionality of the application.

Recommendation 3A: We recommend that the Chief Information Officer:

- Provide software developers, testers, and IT management with ongoing training in software development, testing and acceptance procedures,
- Define sufficient documentation standards for LAS, and
- Define sufficient test standards and procedures for LAS.

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. In addition, we identified weaknesses with the UNIX operating system supporting JAAMS.

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, CIS, and the National Security Agency (NSA) have developed standards for securing Windows 2000 and UNIX 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 list of the most frequent vulnerabilities found within the SBA network is included in Attachment 4 (Limited Official Use and Restricted Distribution). Full details of vulnerabilities found are provided in separate reports that have been provided to OCIO and OIG.

The scan disclosed significant exposures on network resources residing on the SBA network. These exposures were primarily the result of the following:

- Vendor patches and security hot-fixes were not installed in a timely manner.
- Network servers, routers, and workstations were not properly configured.

Although OCIO developed procedures to ensure patches and security hot-fixes were implemented in a timely manner and to ensure network servers are properly configured, the procedures were inconsistently applied.

Audit report (OIG 4-19) Attachment 4 (Limited Official Use and Restricted Distribution) issued on April 29, 2004 in recommendation 4A(1), recommended that the Chief Information Officer develop and implement a corrective action plan to address the vulnerabilities identified in that report. SBA responded that a corrective action plan would be completed by March 31, 2005. We are augmenting that recommendation to included the vulnerabilities identified in this year's Attachment 4 (Limited Official Use and Restricted Distribution), which identify the vulnerabilities our current years' Network scan.

Recommendation 4A: We recommend that the Chief Information Officer develop and implement a corrective action plan with specific milestones to address network weaknesses identified in Attachment 4 (Limited Official Use and Restricted Distribution) of this years' report and the detailed vulnerability assessment reports in a timely manner.

B. 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 2005.

Audit report (OIG 4-19) issued on April 29, 2004 recommended that the Chief Information Officer perform a security assessment for the placement of the initial 20 network sensors. SBA responded that the analysis would be completed by February 28, 2005. Therefore, we are making no new recommendation at this time.

Additionally, audit report (OIG 4-19) issued on April 29, 2004 recommended that the Chief Information Officer revise the IDS vendor's contract as necessary for performance factors established in Recommendation No. 4A of this report. SBA responded that the IDS vendor's contract would be revised by February 28, 2005. Therefore, we are making no new recommendation in at this time.

C. The FY 2002 FISCAM report recommended that OCIO develop the means to test for compliance with SBA's password configuration requirements. In FY 2003, OCIO obtained password-cracking software to periodically test user password configurations for compliance with SBA's password configuration requirements and to determine if users were using easily guessed passwords. Although OCIO's test process achieved the stated goals, the test process was neither effective nor efficient and created potential security exposures if cracked passwords were inadvertently or intentionally released to unauthorized individuals. OCIO cracks all user password files and assesses the time required to crack as an indicator of complexity. For passwords that crack quickly, OCIO determines what caused the password to crack and advises the user of corrective action.

We found that password strength of SBA user passwords is weak. We identified the following:

- 173 passwords were cracked using only alpha characters,
- 13 passwords were cracked using only numeric characters, and
- 255 passwords were the same as the associated user ID.

All of these instances are violations of the SBA password policy. Some of the cracked passwords were for accounts that have administrative permissions to the domain and to all workstations.

Audit report (OIG 4-19) issued on April 29, 2004 recommended that the Chief Information Officer enhance password test procedures to screen all passwords for compliance with password configuration policy. SBA has not provided a response to the recommendation in audit report (OIG 4-19) which was due to OIG on May 29, 2004. Therefore, we are making no new recommendations at this time.

Audit report (OIG 4-19) issued on April 29, 2004 recommended that the Chief Information Officer in consultation with OHCM, develop procedures for escalating administrative consequences for personnel identified as not compliant, such as:

- Advise first-time offenders to immediately change their passwords to conform to the policy.

- Temporarily disable accounts for a second offense and notify the account owner and his or her supervisor.

- Suspend accounts for a third offense and send a request for adverse personnel action to the office director of OCHM and to the account holder.

SBA has not provided a response to the recommendation in audit report (OIG 4-19) which was due to OIG on May 29, 2004. Therefore, we are making no new recommendations at this time.

D. [FOIA Ex. 2]

Recommendation 4B: We recommend the Chief Information Officer develop minimally acceptable baseline configurations based on guidance from NSA, NIST, CIS, SANS, and industry best practices for Windows 2000 Domain Controllers. In addition, these baseline configurations should address all the issues identified above based on the source used for developing the baselines and the settings and policies should be put into place.

E. Policies and procedures for the administration of system software (Windows O/S) have not been developed and documented. OCIO has not identified and documented what administrative functions for the administration of Windows should be segregated and what access each administrator should have. Individuals within the NIB are granted similar access for administering the network operating system.

Conversion from Windows NT to Windows 2000 has not been completed. Without documented policies and procedures for identifying, selecting, installing, and modifying system software, SBA cannot be sure of system integrity. In addition, controls over sensitive functions within the operating system are weakened, and individuals with administrative access could intentionally or unintentionally change system settings in an unauthorized manner, adversely affecting the performance or security of the operating system.

Audit report (OIG 2-18) issued on May 6, 2002 recommended that the Chief Information Officer 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 responded that standard operation procedures for network and system accounts would be implemented by December 1, 2003. However, this recommendation remains open at this time. Since this recommendation remains open, we are augmenting this recommendation at follows:

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

- Develop policies and procedures for the administration of and restriction of access to system software.
- Develop policies and procedures for identifying, selecting, and modifying system software.
- Identify and document appropriate administrative access to system software.
- Ensure individuals with administrative access to system software require such access. Individuals should be granted the minimum level necessary to perform their assigned responsibilities.

F. We identified weaknesses in the UNIX operating system supporting JAAMS. Our analysis of the standard configuration documentation and operating system installation identified several issues and are included in Attachment 8 (Limited Official Use and Restricted Distribution). FISMA requires agencies to develop baselines for their systems to ensure security is adequately addressed.

Audit report (OIG 4-41) issued on September 10, 2004 recommended that the Chief Information Officer:

- Develop a standard baseline configuration that outlines security configurations for all UNIX operating systems at SBA. Best practice documents such as the CIS Solaris Benchmark, Sun Microsystem's Blueprint documents, and NSA's Guide to Securing Solaris should be used to develop these documents to ensure compliance with best practice standards.

- Implement the standard baseline configuration on all UNIX servers which support all major SBA applications including those servers owned and operated by SBA as well as those under contract to the various SBA offices.

- Ensure that the standard baseline configuration for all UNIX servers is enforced by the SBA Certification and Accreditation (C&A) process.

SBA responded that a standard baseline configuration UNIX servers would be developed by September 30, 2005. Additionally, SBA responded that this baseline would be implemented on all UNIX servers Agency-wide by September 30, 2005. Finally, SBA responded that the standard baseline for all UNIX servers would be enforced by the C&A process by September 30, 2005. Therefore, we are making no new recommendations 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 undetected.

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.

A. SBA does not ensure that separation of duty principles are established, enforced, and institutionalized within the organization. Controls are not adequate to ensure that no individual has complete control over incompatible administrative and transaction processing functions.

Our audit identified two individuals with excessive or incompatible responsibilities assigned to their account in JAAMS. Incompatible or excessive duties identified include:

- Security administration of JAAMS has been assigned to an individual within OCIO. We noted that this individual's account was assigned System Administrator and Security Manager Responsibilities. Separation of duty principles suggest that security administration and user account administration functions should be separated. Individuals assigned to review system access should not have the ability to add, modify, or delete accounts within production.

- OCFO has assigned the following excessive responsibilities in production to one of their programmers; SBA System Administrator, SBA Maintenance, SBA NFC Payroll Processing, SBA Credit Card, Alert Manager, Federal Administrator, Application Developer, SBA Translation Manager, and General Ledger Super User.

Our audit of LAS identified 57 users with Terminal User and Agency/Regional/District Security Officer responsibilities. These 57 individuals have the ability to add, modify, and delete user accounts under their security officer accounts and are normal users within their terminal user accounts. Separation of duty principles suggest that system or security administration and data entry functions should not be performed by the same individuals. Administration of LAS is not centralized. Field locations are assigning system administrator duties to individuals who also perform financial activities within LAS.

Without sufficient controls to ensure proper separation of duties, individuals may have complete control over incompatible transaction processing functions that could permit fraudulent activities. Fraudulent activities could include creating fictitious user accounts and permitting unauthorized access.

Recommendation 5A: We recommend that the Chief Financial Officer identify individuals with incompatible or excessive responsibilities within JAAMS. These include the following privileges:

- Alert Manager,
- Application Developer,
- Federal Administrator,
- General Ledger Super User,
- SBA Credit Card,
- SBA NFC Payroll Processing,
- Systems Administration,
- Systems Maintenance, and
- Translation Manager.

Incompatible or excess responsibilities should be removed or management should document the reason for granting these responsibilities and ensure compensating controls are in place to monitor activities by these individuals. Review of activities by individuals with excessive or incompatible duties should be documented and signed off by management.

Recommendation 5B: We recommend that the Chief Information Officer:

- Centralize the administration of LAS or putting compensating controls in place for the 57 individuals identified as having incompatible duties.
- Periodically review access to LAS to ensure proper separation of duties exist.

B. Day-to-day operating procedures for the headquarters data center are not adequately documented and prohibited actions are not identified. Resources have not been allocated to develop and document day-to-day operating procedures for the data center. Data center staff may not follow proper procedures, which can lead to problems with SBA information technology services.

Recommendation 5C: We recommend Chief Information Officer develop and document day-to-day operating procedures for the headquarters data center.

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 resumed within an acceptable period of time in the event of a disaster or disruption in service. SBA's Continuity of Operations Program (COOP) consists of detailed Business Resumption Plans (BRPs) for the various offices and field sites within SBA. OCIO is in the process of collecting these plans from the various offices for review and comment. Once all plans have been completed and submitted to OCIO, OCIO intend to help the offices test their plans. SBA has performed some testing on their COOP; however, testing was limited to selected portions of the COOP.

Our review of nine headquarters BRPs determined that many of the plans were incomplete. The following information was missing from all or some of the plans we reviewed:

- A list of critical operations and data has not been documented that prioritizes data and operations. Six out of the nine headquarter BRPs we reviewed did not have a prioritized list of data and operations. We did note that SBA does have an entity-wide prioritized list of critical data and operations in Attachment III of the HQ COOP.

- Resources supporting critical operations have not been identified and documented. Types of resources identified should include:
  - computer hardware
  - computer software
  - computer supplies
  - system documentation
  - telecommunications
  - office facilities and supplies
  - human resources

- Emergency processing priorities have not been documented and approved by appropriate program and data processing managers.

- A system disaster recovery plan for the LAS has not been fully documented that identifies critical data files and restoration procedures between the Egan mainframe and the SBA Sybase server systems to ensure that both systems adequately interface and operate in the event of an emergency.

- SBA has not tested all BRPs, and a deadline for completion of BRPs has not been set.

In the event of a disaster or disruption in service, SBA may not be able to resume operations within an acceptable period of time. In addition, in the event of a disaster, SBA may not know which processes to recover first, what offices are involved in recovery, who is responsible, and what supporting or other resources will be needed.

Recommendation 6A: We recommend that the Chief Operating Officer**:**

- Establish a deadline for the completion of all BRPs,
- Ensure all BRPs submitted are complete. In addition, information from the various BRPs should be used to update SBA's COOP where necessary,
- Comply with SBA policy which requires a prioritized list of critical data and operations be established and documented in agency BRPs,
- Work with the various offices to identify resources supporting mission critical functions. Resources should be documented and included in SBA's COOP,

- Identify and document emergency processing priorities in the HQ COOP and work with each office to establish a set of emergency processing priorities. Emergency processing priorities should be documented in BRPs and updated on a periodic basis,
- Work with the various offices within SBA to ensure all BRPs are tested, and
- Results from testing should be used to update or modify the plan where necessary.

Recommendation 6B: We recommend that the Chief Information Officer develop a system disaster recovery plan for LAS (both Egan mainframe and SBA's Sybase servers) to ensure that all facets of LAS can recover if both or either aspects of the system are disabled during an emergency.

ATTACHMENT 2

AUDIT OF INFORMATION SYSTEM CONTROLS FOR FY 2004
STATUS OF PRIOR-YEAR AUDIT RECOMMENDATIONS

Condition	Recommendation	Status as of 9/30/04
ENTITY-WIDE SECURITY PROGRAM CONTROLS:		
OIG Report 4-19, Finding 1A: SBA's information system and security program did not provide assurance that the program complied with requirements established by federal laws, regulations, and standards.	**Recommendation 1A:** 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.	**OPEN** Sufficient resources have not been provided to enable OCIO to meet its responsibilities.
OIG Report 4-19, Finding 1A: SBA's information system and security program did not provide assurance that the program complied with requirements established by federal laws, regulations, and standards.	**Recommendation 1B:** The Chief Information Officer revise and enhance existing policies and procedures to ensure that: • Chief Information Officer (CIO) revise and enhance existing policies and procedures to ensure that: • Control weaknesses identified in certification and accreditation reviews and audit reports are resolved in a timely manner and senior management is provided timely information regarding the progress towards implementing corrective actions. • OCIO monitoring controls are effective to preclude reoccurrence of previously noted weaknesses. • Technical personnel are provided technical training to enable personnel to successfully carry out their duties and responsibilities. • Technical skills are sufficient to meet new technical requirements prior to implementing new hardware and software. • 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.	**Open** Control weaknesses identified from prior year reports have not been corrected and a technical training program has not been implemented and provided to OCIO staff. See finding 1C in Attachment 1.

ATTACHMENT 2

Condition	Recommendation	Status as of 9/30/04
OIG Report 4-19, Finding 1B: 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 that 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.	**Partially Complete** Plans of action and milestones have been identified and developed from audits, management reviews and certification and accreditation reviews. However, they are not always complete. Monitoring of system owner corrective action plans does not take place. OCIO currently attempts to follow up with weaknesses in the POA&M in the next certification and accreditation which is generally three years later.
OIG Report 2-18, Finding 1C: 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 1C:** Develop an agency-wide security plan, as recommended in Section 5.8 of SBA's Information Technology Architecture Plan, to establish and implement the policies, procedures, and practices for the following: • Full integration of the information security approach and implementation process, along with key milestones for implementing the program. • Coordination among program offices to support their security needs. • Guidance to the program office for effective implementation of information system security controls.	**Open**

Condition	Recommendation	Status as of 9/30/04
	- Methods to monitor the effectiveness of each part of the information technology security assigned to each program office.	
ACCESS CONTROLS:		
OIG Report 4-19, Finding 2A: 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.	**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 Office of Human Capital Management (OHCM), develop procedures for network and application security administrators to receive notification of termination of SBA employees.	**Open** Weaknesses in network and financial system account administration were identified during the FY2004 audit. See finding 2D in Attachment 1.
OIG Report 4-19, Finding 2B: Physical controls over hardware at DFC were weak. Routers connected to the DFC	**Recommendation 2B:** We recommend that the Chief Financial Officer instruct the Director of DFC	**Closed** DFC has

Condition	Recommendation	Status as of 9/30/04
network were located in an unsecured area of the building. Anyone entering the building, after passing through security, could potentially gain access to these routers and disconnect the wires connected to them, thus bringing down portions of the network.	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.	enclosed the switches and limited access to them using a padlock.
OIG Report 4-19, Finding 2C: [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.	**Open**
OIG Report 2-18, Finding 2A: 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	**Recommendation 2B:** 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. These procedures should: • Provide guidance and technical training opportunities for all network and application security administrators describing expected duties and supporting successful performance of these duties. • Require spot checks of field office servers for compliance with established rules. • Conduct physical security reviews of workstations.	**Open** **See finding 4E in Attachment 1.**

Condition	Recommendation	Status as of 9/30/04
disabled after three failed login attempts.	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.	
OIG Report 3-20, Finding 2A: 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 on 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.	**Closed**
OIG Report 3-20, Finding 2B: 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.	**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 later modified to February 20, 2003.	**Closed**
OIG Report 2-18, Finding 2A: and OIG Report 3-20, Finding 2C: 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** See finding 1B Attachment 1.
APPLICATION DEVELOPMENT AND SOFTWARE CHANGE CONTROLS:		
OIG Report 4-19, Finding 3A: 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.	**Closed**
OIG Report 4-19, Finding 3B: OCFO's Credit Reform Models did not comply with change control policies, procedures and documentation requirements in Federal Accounting Standards Advisory Board (FASAB) Technical Releases No. 3 and No. 6 or SBA system development	**Recommendation 3B:** We recommend that the: (1) 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	**Closed**

Condition	Recommendation	Status as of 9/30/04
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 Office of Inspector General (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 System Development Life Cycle (SDLC) policy and procedures relating to OCIO's lack of involvement with new systems being developed.	system development and program change control policies and procedures. (2) Chief Information Officer develop the means to actively participate in all phases of system development efforts within the agency.	
OIG Report 4-19, Finding 4C: 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 3C:** We recommend that the Chief Information Officer develop the means to actively participate in all phases of system development efforts within the agency.	**Open**
OIG Report 1-12, Finding 3: Documentation for system and program changes was outdated, and documentation supporting tests of program changes was inadequate. Specifically, we found that user and programmer test plans and	**Recommendation 3A:** We recommend that the Chief Information Officer develop quality control program procedures to periodically review existing applications to assure that documentation is kept current and accurately reflects the cumulative affects of program changes made over time.	**Open**

Condition	Recommendation	Status as of 9/30/04
results are not documented to demonstrate that programs are properly tested and approved prior to being placed in operation. OCIO requires basic documents for all systems, including user requirements, design documents, test plans, implementation, and acceptance documents. It also requires retention of User Request Forms that detail program changes; these forms are required to be signed by the programmer and the user to acknowledge acceptance of the change. Compliance is not enforced, because control procedures do not exist to ensure that documentation is being updated and maintained.		
SYSTEM SOFTWARE CONTROLS:		
OIG Report 4-19, Finding 4A: Limited Official Use and Restricted Distribution	**Recommendation 4A:** Limited Official Use and Restricted Distribution	**Partially completed**
OIG Report 4-19, Finding 4B: Limited Official Use and Restricted Distribution	**Recommendation 4B:** Limited Official Use and Restricted Distribution	**Open**
OIG Report 4-19, Finding 4C: 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.	**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.	**Partially complete** OCIO recognized 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. See finding 4B in Attachment 1.

Condition	Recommendation	Status as of 9/30/04
OIG Report 4-19, Finding 4D: In FY 2003, OCIO obtained password-cracking software to periodically test user password configurations for compliance with SBA's password configuration requirements and to determine if users were using easily guessed passwords. Although OCIO's test process achieved the stated goals, the test process was neither effective nor efficient and created potential security exposures if cracked passwords were inadvertently or intentionally released to unauthorized individuals. OCIO cracks all user password files and assesses the time required to crack as an indicator of complexity. For passwords that crack quickly, OCIO determines what caused the password to crack and advises the user of corrective action. This two-stage test approach is time consuming and unnecessary to determine compliance with password configuration requirements.	**Recommendation 4D:** We recommend that the Chief Information Officer enhance its password test procedures to screen all passwords for compliance with password configuration policy. **Recommendation 4E:** We recommend that the Chief Information Officer in consultation with OHCM, develop procedures for escalating administrative consequences for personnel identified as not compliant, such as: • Advise first-time offenders to immediately change their passwords to conform to the policy. • Temporarily disable accounts for a second offense, and notify the account owner and immediate supervisor. • Suspend accounts for a third offense, and send a request for adverse personnel action to the office director, OHCM, and the account holder.	**Open** **See finding 4C in Attachment 1.**
OIG Report 4-19, Finding 4E: Our network analysis and tests identified significant numbers of security weaknesses with the Windows 2000 configuration for SBA workstations and servers residing on the network. Additionally, OCIO had not completed the Windows 2000 implementation project; thus certain security and administrative controls found in the Native Mode could not be installed. These weaknesses substantially reduce the level of assurance that management can place on the adequacy of security controls to properly secure SBA data and network operations from unauthorized activities and safeguard SBA information technology assets from harm. See Attachment 4 for a complete description of the specific weaknesses identified.	**Recommendation 4F:** We recommend that the Chief Information Officer conduct periodic network tests to ensure that security features are properly and fully utilized.	**Open**
OIG Report 3-20, Finding 4A: In our previous audit, we recommended that SBA enhance policies, procedures and technical capabilities to monitor the	**Recommendation 4A:** We recommend that the Chief Information Officer fully implement the planned upgraded intrusion detection system and reporting/monitoring tools. Additionally, we	**Partially completed** See finding 4B in

Condition	Recommendation	Status as of 9/30/04
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]	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.	Attachment 1.
OIG Report 3-20, Finding 4B: 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.	**Partially Complete** Although OCIO's test process achieved the stated goals, the test process was neither effective nor efficient and created potential security exposures if cracked passwords were inadvertently or intentionally released to unauthorized individuals. **See finding 4C in Attachment 1.**
OIG Report 3-20, Finding 4C: We	**Recommendation 4C:** We recommend that the	**Open**

Condition	Recommendation	Status as of 9/30/04
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.	Chief Information Officer enforce the procedures currently in place and remove all unauthorized remote desktop software from workstations.	
OIG Report 3-20, Finding 4D: 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.	**Open**
OIG Report 3-20, Finding 4F: 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** For audit tracking purposes, OIG Report 3-20, Finding Recommendation 4F was closed. OIG Report 4-19, Finding 4B, Recommendation 4B(1) is open. Although SBA asserts that it timely installs patches and fixes to its general support systems, audit testing contradicts this assertion.
OIG Report 3-20, Finding 4G: 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** For audit tracking purposes, OIG Report 3-20, Finding Recommendation 4G was closed. However, the finding remains

Condition	Recommendation	Status as of 9/30/04
		open. See finding 1C in Attachment 1.
SEGREGATION OF DUTY CONTROLS:		
OIG Report 4-19, Finding 5A: 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.	**Closed**
OIG Report 1-12, Finding 5A: SBA generally has appropriate segregation of duties throughout its information system environment; individuals generally do not have the ability to conduct unauthorized actions or gain unauthorized access to assets or records. However, some instances of inadequate segregation of duties were identified. For example, one individual at a field office was the security officer for LAS, a senior loan officer on LAS, and had supervisory privileges on the Field Cashiering System.	**Recommendation 5A:** We recommend that the Chief Information Officer, in conjunction with the appropriate program offices continue its efforts to identify and eliminate incompatible duties, responsibilities, and functions.	**Open**
SERVICE CONTINUITY CONTROLS:		
OIG Reports 3-20, and 4-19, Finding 6: 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	**(Findings were repeated from audit 3-20 to audit 4-19)** **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.	**Open** Business Resumption plans remain incomplete and untested.

ATTACHMENT 2

Condition	Recommendation	Status as of 9/30/04
(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.	• 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, to 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.	

Condition	Recommendation	Status as of 9/30/04
7A: 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**
7B: 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.	**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 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.	**Open**
Application Controls:		
OIG Report 3-20, Finding 8C: We noted that 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.	**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.	**Open** **See finding 2E in Attachment 1.**
OIG Report 3-20, Finding 8C: We noted that 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.	**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,	**Partially Complete** While the procedures were implemented to

Condition	Recommendation	Status as of 9/30/04
	authorized JAAMS users.	perform an annual review, documentation did not exist to ensure that the review was performed annually.
OIG Report 3-20, Finding 8C: We noted that security officers within OCIO do not have the requisite functional knowledge and have not received the appropriate training to adequately administer JAAMS security.	**Recommendation 8I**: We recommend the CIO provide adequate training and periodic retraining to enable JAAMS security administrators to effectively perform their duties	**Partially Complete** While initial training was provided to JAAM security personnel, documentation did not exist to ensure that training was performed periodically.

ATTACHMENT 3-A

U.S. Small Business Administration
Washington, D.C.

January 28,2005

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

/S/ Original Signed
From: Jerry E. Williams
Acting Chief Information Officer

Subject: Comments on Draft Audit of SBA's Information System Controls

Attached please find the response and comments from the Office of the Chief Information Officer to the subject audit. We appreciated the opportunity to review this report and we look forward to the improvements that should result from acting on many of its recommendations.

Our response and comments are attached within the body of the draft report and accompanied by four additional Attachments A - D. We are of course available to discuss the details and background of our comments at your request. If you have any questions please contact Dan Vellucci of my staff by telephone on 202-205-[FOIA Ex. 2].

Attachments

Page 4, FY 2004 Results:
OCIO Response and Comments (bullet 5 above, underlined): OCIO can neither agree nor disagree with this assessment because its meaning is unclear. OCIO requests that OIG modify this language to make the following distinction: Is the assertion that the Sun Solaris OS baseline configuration itself is not acceptable or that the baseline configuration is not adequately documented? If the issue is related to documentation, OCIO would request that the report language clarify this fact and provide specific recommendations with respect to completing or improving deficient areas of system documentation. If the issue is related to the system's actual configuration, OCIO would request that the report language list specific system configuration deficiencies, so that developers can be assigned to correct these areas immediately.

Recommendation 1B: OCIO Response: Partially Agree. We agree with the intent of the recommendation, which is aimed at assuring adequate human resource coverage for IT operations and systems management. We will develop internal procedures and recommended practices, such as cross-training and job shifts planning, for responsible managers to consider using. However, we do not intend to formulate or suggest personnel polices with regard to mandatory annual leave scheduling, which we believe to be a substantive matter directed by the Office of Human Capital Management and implemented by individual managers.

Recommendation 2A: OCIO Response: Partially Agree. OMB has directed OCIO to selectively automate SBA's paper forms and associated work processes. Using Metastorm eWORKS electronic forms and workflow software, OCIO will include these access requests within that effort.

Recommendation 2C: OCIO Response: Agree. As stated in response to Recommendation 2A OCIO is currently automating SBA's paper forms, utilizing Metastorm eWORKS workflow software and recommends using electronic forms for the IT systems and network access process. We note that in the case of temporary or emergency access a manual process may be necessary as an alternative.

Recommendation 2D: OCIO Response: Agree. We agree with the recommendation but note that considerable effort and cost would be involved in implementing these modifications, which would be applied to a Loan Accounting System that is aged and due for re-engineering Our estimate for making LAS changes alone would be approximately $1.5 - 2.0 million. That amount is not available within the budget at this time.

Recommendation 2F: OCIO Response: Agree. We note that some open network accounts have been extended for previous SBA executives. We have requested policy guidance from the Office of General Counsel on this matter to establish appropriate account de-activation deadlines for certain executives.

Recommendation 2G: OCIO Response: OCIO will define minimum requirements for MA and GSS audit logs addressing each platform and including retention requirements; assign responsibility for review and retention of GSS audit logs; work with system owners to assure the review and retention of MA audit logs. The system owner for the MAs will be responsible for assigning responsibility for review and retention of MA audit logs. During Certification and Accreditation, IT Security will validate the implementation. The response to Sybase issues is covered in our reply to Recommendation 2-J below.

Note: Considerable effort and cost would be involved in implementing these modifications, which would be applied to a Loan Accounting System that is aged and due for re-engineering. Our estimate for making LAS changes with audit log capabilities would be approximately $6.0 million. That amount is not available within the budget at this time.

<u>Recommendation 2I: OCIO Response: Agree.</u> OCIO will review the CIS benchmark for Oracle and set the minimum standards for SBA Oracle database management systems. OCIO will work with ODA and CFO to implement these standards. During Certification and Accreditation, IT Security will validate the implementation.

<u>Recommendation 2J: OCIO Response; Partially Agree.</u> An initial workplan for FISCAM Attachment 7 tasks is enclosed at <u>Attachment A.</u>

<u>Recommendation 3A: OCIO Response and Comments: Disagree.</u> OCIO agrees with the recommendation to inform SBA personnel about use of the SDM and we believe we are already doing that. OCIO is currently improving and expanding existing routine communications to inform SBA personnel of the SDM and the requirement to follow its methodology. Additionally, OCIO already conducts periodic audits or project reviews to ensure compliance with the SDM, as part of the Agency-wide Project Health Check process that the OCIO organization manages. <u>(Examples at Attachment B.)</u> Accordingly, OCIO requests that this recommendation be removed from the report, because OCIO has completed action on both parts of this recommendation and does not consider them outstanding issues. OCIO views these recommendations as best practices that the organization has already implemented.

<u>OCIO Response and Comments (para 1 above).</u> OCIO disagrees with the statement regarding SDM standards as applied to LAS, and requests that it be deleted. OCIO has documented the change control process for all mainframe applications, including LAS, and this change control process is fully consistent with and based upon the SBA SDM. <u>Attached at C.</u> are: (1) Mainframe Change Control Process Policy; (2) Mainframe Change Control Process Flow Diagrams; and (3) Mainframe Change Control Form. These documents are institutionalized parts of OCIO's change control procedures and detail the requirements for mainframe configuration changes.
See <u>Attachment D.</u>

1. Mainframe Development to Production Software Release Process
2. Mainframe Change Control Process Flowchart
3. Mainframe Change Control Form

OCIO Response and Comments; (para. 3 above). OCIO disagrees with the statement regarding periodic audits to verify SDM usage, and requests that the statement be deleted. OCIO periodically conducts Project Health Checks with all major projects (those documented in Exhibits 300) to monitor project performance and compliance with the SDM. There is a standard format/Health Check Evaluation Form and standard criteria that are used for all Health Checks, including compliance with the SDM, to evaluate the health of a project. OCIO has conducted and documented Health Checks for all major projects except LAS. Attached at B. are three out-briefs from completed Health Checks, covering the Disaster Credit Management System (DCMS), the Entrepreneurial Development Management Information System (EDMIS), and the Office of General Contracting and Business Development's 8(a) and SDB Electronic Application. If the concern is a Health Check for LAS itself, OCIO requests that the report be amended to state only that "periodic reviews of LAS applications have not been completed." The current report language appears to be overly broad and does not accurately depict OCIO's agency-wide SDM compliance monitoring activities as supported by standard tools and processes. We are enclosing a copy of several completed Health Checks as examples. (Attachment A.)

Recommendation 4A: OCIO Response: Agree

Recommendation 4C: OCIO Response: Agree. OCIO's Network Integration Branch (NIB) will assess the current Windows 2000 Server standard configuration. Once complete, NIB will research NIST and NSA Windows 2000 Server guidelines and evaluate each recommended item for its necessity and affect on SBA servers, then comply as deemed necessary.

Recommendation 5B: OCIO Response: Disagree. OCIO believes this responsibility lies with the system owner (CFO) since they alone have the specific knowledge required to determine whether appropriate segregation of duties and responsibilities are being maintained based upon access permissions granted to users.

Recommendation 5C: OCIO Response: Agree.

Recommendation 6A: OCIO Response: Agree. We agree with this recommendation but believe that all COOP related activities, except those directly related to critical IT systems, should be managed at the Chief Operating Officer level within the Agency.

ATTACHMENT 3-B

U.S. Small Business Administration
Office of the Chief Financial Officer
Washington DC 20416

To: Robert G. Seabrooks
Assistant Inspector General for Audit

/S/ Original Signed
From: Thomas Dumaresq
Chief Financial Officer

CC: Jennifer Main
Deputy Chief Financial Officer

Jerry Williams
Acting Chief Information Officer

Date: January 25, 2005

Re: Response to Audit of SBA's Information System Controls for Fiscal Year 2004

This is a response to the report issued by the Office of the Inspector General titled "Audit of SBA's Information System Controls".

The Office of the Chief Financial Officer has received four recommendations that are related to the administrative accounting system. Our response to each recommendation is stated below.

- Recommendation 2B: We recommend that the Chief Financial Officer:

  - Ensure access to JAAMS is granted only when requested via Form 2200;

  - Ensure all access request forms are maintained on file for future reference. Access request forms should be periodically traced to active user accounts to make sure access in JAAMS agrees with the access that was requested and approved.

- Response to 2B: Based on our discussion and Ethel Mathews agreement, this recommendation will be re-directed to the Office of the Chief Information Officer.

- Recommendation 2E: We recommend that the Chief Financial Officer continue with the planned upgrade of the Oracle application and database for JAAMS. Security settings should be enabled to enforce strong password controls, including password history and automatic lock-out after a set number of failed login attempts.

- Response to 2E: We agree. We have completed the Upgrade to Oracle Federal Financials 11.5.9, and have implemented the appropriate password complexity enforcement and history. Patchset FND-H implements lockout after a number of failed attempts, and will be implemented prior to the end of the second quarter. All non-application database accounts have been assigned to appropriate profiles that enforce complexity, history, and lockout. Application database accounts remain with the default profile, however compensating controls are being developed to ensure the use of FNDCPASS on a periodic basis consistent with best practices and SOP 90-47.

- Recommendation 2H: We recommend that the Office of the Chief Financial Officer:

  - Require that all activities by Oracle database administrators be logged

  - Require periodic review of database logs by someone outside of Corio, preferably an individual within OFS or OCIO Security with an understanding of the production Oracle database. Audit logs should not be reviewed by the individuals being audited.

  - Take steps necessary to ensure all activity in JAAMS involving access to and modifications of sensitive or critical files at the application level are logged

  - Assign responsibility for periodic review of JAAMS application logs

- Response to 2H: We agree. We will work with our ASP to extend auditing to all accounts assigned to ASPUSER, SBAUSER, and ASPSYS profiles. Furthermore, we will establish procedures for weekly emailing and review of the activity in both the Form level auditing logs as well as the database level logs. Target completion is the end of the second quarter.

- Recommendation 5A: We recommend that the Chief Financial Officer identify individuals with incompatible or excessive responsibilities within JAAMS. These include the following privileges: Alert Manager, Application Developer, Federal Administrator, General Ledger Super User, SBA Credit Card, SBA NFC Payroll Processing, Systems Administration, Systems Maintenance, and Translation Manager.

- Response to 5A: We agree with this recommendation.

The report also assigns recommendations for 2C and 2I to the Office of the Chief Information Officer in conjunction with the Office of the Chief Financial Officer. We will work with the OCIO on the two recommendations.

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.

ATTACHMENT 3-C

From: Brechbiel, Richard
Sent: Monday, January 31, 2005 3:27 PM
To: Harai, Richard K.
Cc: Gates, M. Catherine; Stoehr, Melissa A.
Subject: RE: Issuance of Audit Report on SBA Information System Controls

With regard to the Recommendation 1A I am not comfortable having a policy that requires mandatory vacations for employees. Annual leave is earned and employees are allowed to used it at their discretion. For example, if an employee is attempting to build their balance to the 240 hour carry over limit I do not believe that we can require them to use annual leave in lieu of that effort. It might be possible to have periodic job rotations for employees in such positions. However, this would assume there was sufficient staff with the requisite clearances to allow such temporary assignments. While assignment of work is a traditional right of management, we may have to involve the Union as it could be viewed as a change in working conditions.

ATTACHMENT 3-D

Audit of SBA's Information System Controls
January 28, 2005
OCIO/OHCM/OCFO Response with Auditor Comments
(Certain Recommendations were changed and renumbered from the Draft Report)

1. Entity-Wide Security Program Controls

Recommendation 1A: Partially Agree – SBA is not comfortable having a policy that requires mandatory vacations for employees. Annual leave is earned and employees are allowed to used it at their discretion. For example, if an employee is attempting to build their balance to the 240 hour carry over limit, SBA believes it cannot require them to use annual leave in lieu of that effort. It might be possible to have periodic job rotations for employees in such positions. However, this would assume there was sufficient staff with the requisite clearances to allow such temporary assignments. While assignment of work is a traditional right of management, we may have to involve the Union as it could be viewed as a change in working conditions.

Auditor Response: Some method of periodic job rotations for employees in sensitive IT positions will be needed. Adjudication of the recommendation will occur in the audit follow-up process.

Recommendation 1B: Partially Agree – SBA agrees with the intent of the recommendation, which is aimed at assuring adequate human resource coverage for IT operations and systems management. We will develop internal procedures and recommended practices, such as cross-training and job shifts planning, for responsible managers to consider using. However, we do not intend to formulate or suggest personnel polices with regard to mandatory annual leave scheduling, which we believe to be a substantive matter directed by the Office of Human Capital Management and implemented by individual managers.

Auditor Response: SBA will need to adopt a formal policy between the Office of Human Capital Management and the Office of Chief Information Officer to enact periodic job rotations for employees in sensitive IT positions. The policy should be part of an updated SOP 90-47. Adjudication of the recommendation will occur in the audit follow-up process.

2. Access Controls

Recommendation 2A: Partially Agree – OMB has directed OCIO to selectively automate SBA's paper forms and associated work processes. Using Metastorm eWORKS electronic forms and workflow software, OCIO will include these access requests within that effort.

Auditor Response: Some method of tracing or annually reviewing access request forms to determine if access requests are documented will need to be incorporated into this process.

Recommendation 2B: Based on our discussion and Ethel Mathews agreement, this recommendation will be re-directed to the Office of the Chief Information Officer.

Auditor Response: The recommendation was redirected to the SBA Computer Security Officer within the Office of Chief Information Officer.

Recommendation 2C: Agree – As stated in response to Recommendation 2A OCIO is currently automating SBA's paper forms, utilizing Metastorm eWORKS workflow software and recommends using electronic forms for the IT systems and network access process. We note that in the case of temporary or emergency access a manual process may be necessary as an alternative.

Recommendation 2D: Auditor Response – Original recommendation 2D was separated into 2D for the Network and 2E for LAS for the final report. SBA only responded to the LAS portion [2E] of the recommendation.

Recommendation 2E (Original 2D): Agree – We agree with the recommendation but note that considerable effort and cost would be involved in implementing these modifications, which would be applied to a Loan Accounting System that is aged and due for re-engineering Our estimate for making LAS changes alone would be approximately $1.5 - 2.0 million. That amount is not available within the budget at this time.

Auditor Response: Because of the information within LAS and its importance to the Agency, SBA must decide whether to implement the corrective actions necessary to ensure that LAS meets its security requirements as defined by OMB Circular A-130 and NIST 800 series publications or, SBA must decide that implementing such security requirements is not cost-effective and begin the process of replacing LAS with a system which can meet the security requirements. SBA cannot agree with the recommendation and at the same time state that it is not going to implement the recommendation and thus properly secure its information.

Recommendation 2F (Original 2E): We agree. We have completed the Upgrade to Oracle Federal Financials 11.5.9, and have implemented the appropriate password complexity enforcement and history. Patchset FND-H implements lockout after a number of failed attempts, and will be implemented prior to the end of the second quarter. All non-application database accounts have been assigned to appropriate profiles that enforce complexity, history, and lockout. Application database accounts remain with the default profile, however compensating controls are being developed to ensure the use of FNDCPASS on a periodic basis consistent with best practices and SOP 90-47.

Recommendation 2G (Original 2F): Agree. We note that some open network accounts have been extended for previous SBA executives. We have requested policy guidance from the Office of General Counsel on this matter to establish appropriate account de-activation deadlines for certain executives.

Recommendation 2H (Original 2F): Auditor Response – Original recommendation 2F was separated into 2G for the Network and 2H for periodically reviewing all General Support Systems and Major Applications for the final report.

Recommendation 2I (Original 2G): OCIO will define minimum requirements for MA and GSS audit logs addressing each platform and including retention requirements; assign responsibility for review and retention of GSS audit logs; work with system owners to assure the review and retention of MA audit logs. The system owner for the MAs will be responsible for assigning responsibility for review and retention of MA audit logs. During Certification and Accreditation, IT Security will validate the implementation. The response to Sybase issues is covered in our reply to Recommendation 2-J [2-L] below.

Note: Considerable effort and cost would be involved in implementing these modifications, which would be applied to a Loan Accounting System that is aged and due for re-engineering. Our estimate for making LAS changes with audit log capabilities would be approximately $6.0 million. That amount is not available within the budget at this time.

Auditor Response: Because of the information within LAS and its importance to the Agency, SBA must decide whether to implement the corrective actions necessary to ensure that LAS meets its security requirements as defined by OMB Circular A-130 and NIST 800 series publications, or, SBA must decide that implementing such security requirements is not cost-effective and begin the process of replacing LAS with a system which can meet the security requirements. SBA cannot agree with the recommendation and at the same time state that it is not going to implement the recommendation and thus properly secure its information.

Recommendation 2J (Original 2H): We agree. We will work with our ASP to extend auditing to all accounts assigned to ASPUSER, SBAUSER, and ASPSYS profiles. Furthermore, we will establish procedures for weekly emailing and review of the activity in both the Form level auditing logs as well as the database level logs. Target completion is the end of the second quarter.

Recommendation 2K (Original 2I): Agree. OCIO will review the CIS benchmark for Oracle and set the minimum standards for SBA Oracle database management systems. OCIO will work with ODA and CFO to implement these standards. During Certification and Accreditation, IT Security will validate the implementation.

Recommendation 2L (Original 2J): Partially Agree. An initial workplan for FISCAM Attachment 7 tasks is enclosed at Attachment A.

Auditor Response: We acknowledge management's plan, however, the plan does not address all critical areas in an adequate manner (i.e., adequate logging does not only include failed login attempts). Management should take corrective actions for all identified discrepancies. We will evaluate remediation efforts during the FY05 audit.

3. Application Software Development and Program Change Controls

Recommendation 3A: Disagree. OCIO agrees with the recommendation to inform SBA personnel about use of the SDM and we believe we are already doing that. OCIO is currently improving and expanding existing routine communications to inform SBA personnel of the SDM and the requirement to follow its methodology. Additionally, OCIO already conducts periodic audits or project reviews to ensure compliance with the SDM, as part of the Agency-wide Project Health Check process that the OCIO organization manages. (Examples at Attachment B.) Accordingly, OCIO requests that this recommendation be removed from the report, because OCIO has completed action on both parts of this recommendation and does not consider them outstanding issues. OCIO views these recommendations as best practices that the organization has already implemented.

OCIO Response and Comments (para 1 above). OCIO disagrees with the statement regarding SDM standards as applied to LAS, and requests that it be deleted. OCIO has documented the change control process for all mainframe applications, including LAS, and this change control process is fully consistent with and based upon the SBA SDM. Attached at C. are: (1) Mainframe Change Control Process Policy; (2) Mainframe Change Control Process Flow Diagrams; and (3) Mainframe Change Control Form. These documents are institutionalized parts of OCIO's change control procedures and detail the requirements for mainframe configuration changes.

See Attachment D.

1. Mainframe Development to Production Software Release Process
2. Mainframe Change Control Process Flowchart

3. Mainframe Change Control Form

OCIO Response and Comments; (para. 3 above). OCIO disagrees with the statement regarding periodic audits to verify SDM usage, and requests that the statement be deleted. OCIO periodically conducts Project Health Checks with all major projects (those documented in Exhibits 300) to monitor project performance and compliance with the SDM. There is a standard format/Health Check Evaluation Form and standard criteria that are used for all Health Checks, including compliance with the SDM, to evaluate the health of a project. OCIO has conducted and documented Health Checks for all major projects except LAS. Attached at B. are three out-briefs from completed Health Checks, covering the Disaster Credit Management System (DCMS), the Entrepreneurial Development Management Information System (EDMIS), and the Office of General Contracting and Business Development's 8(a) and SDB Electronic Application. If the concern is a Health Check for LAS itself, OCIO requests that the report be amended to state only that "periodic reviews of LAS applications have not been completed." The current report language appears to be overly broad and does not accurately depict OCIO's agency-wide SDM compliance monitoring activities as supported by standard tools and processes. We are enclosing a copy of several completed Health Checks as examples. (Attachment A.)

Auditor Response: The audit finding and recommendation were reworded to be more exactly what was identified during fieldwork. LAS programmers were unaware of SBA's SDM and proper change control procedures that should have been in effect for making changes to code, testing and acceptance of software. Therefore, we believe that better training in configuration management is warranted along with more defined procedures for programming, testing, and acceptance.

4. System Software Controls

Recommendation 4A: Agree

Recommendation 4B: SBA did not respond to recommendation 4B.

Recommendation 4C: Agree. OCIO's Network Integration Branch (NIB) will assess the current Windows 2000 Server standard configuration. Once complete, NIB will research NIST and NSA Windows 2000 Server guidelines and evaluate each recommended item for its necessity and affect on SBA servers, then comply as deemed necessary.

5. Segregation of Duty Controls

Recommendation 5A: We agree with this recommendation.

Recommendation 5B: Disagree. OCIO believes this responsibility lies with the system owner (CFO) since they alone have the specific knowledge required to determine whether appropriate segregation of duties and responsibilities are being maintained based upon access permissions granted to users.

Auditors Response: While we believe this is true for JAAMS (to an extent as OCIO is still responsible for aspects of security administration for JAAMS), the responsibility for LAS resides entirely with OCIO. Since this entire recommendation discusses the problems with LAS, then this response is not adequate to address this recommendation. Given that OCIO Security has the responsibility for security for systems that cross SBA Office boundaries, OCIO is responsible for

ensuring the LAS security officers are not also acting as users of the system.
6. Service Continuity Controls
Recommendation 6A: Agree. We agree with this recommendation but believe that all COOP related activities, except those directly related to critical IT systems, should be managed at the Chief Operating Officer level within the Agency. **Recommendation 6B:** Auditor Response – Original recommendation 6A was separated into two recommendations to separate the IT aspects of the recommendation from the operational aspects of SBA's COOP program.

ATTACHMENT 9

REPORT DISTRIBUTION

Recipient	**Copies**
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	3
U.S. Government Accountability Office	1