AUDIT OF SBA'S INFORMATION SYSTEMS CONTROLS FOR FISCAL YEAR 2005 AUDIT REPORT NUMBER 06-08

DECEMBER 22, 2005

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

AUDIT REPORT
Issue Date: December 22, 2005
Number: 06-08

To: Charles T. McClam
Acting Chief Information Officer

Herbert L. Mitchell
Assistant Administrator for Disaster Assistance

[Exemption 2]

From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's Information Systems Controls for FY 2005

Background

Attached is the audit report on SBA's Information Systems Controls for FY 2005 issued by Cotton & Company LLP as part of the audit of SBA's FY 2005 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 loan systems, 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, and (4) service continuity controls. The report also provides recommendations for strengthening controls in these areas.

SBA generally agreed with the auditor's findings and recommendations with the exception of finding 2A on

[Exemption 2]

Neither finding 2A and recommendation 2A, nor finding 2C and recommendation 2C were changed or modified. For recommendation 2A, we will endeavor to work with SBA during the audit resolution process to come to agreement on the centralization of network accounts. For recommendation 2C, the CIO must adequately ensure that security is enforced in its mainframe environment.

Responses from the Assistant Administrator for Disaster Assistance and the Acting Chief Information Officer (CIO) are included as attachments to this report.

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- [Exemption 2]

Attachments

AUDIT OF INFORMATION SYSTEM CONTROLS
FISCAL YEAR 2005 FINANCIAL STATEMENT AUDIT
U.S. SMALL BUSINESS ADMINISTRATION

Inspector General
U.S. Small Business Administration

Cotton & Company LLP audited the Fiscal Years (FYs) 2005 and 2004 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).

We conducted our audits in accordance with auditing standards generally accepted in the United States; standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin 01-02, *Audit Requirements for Federal Financial Statement.*

In planning and performing our work, we considered SBA's Information Technology (IT) internal controls over financial reporting by obtaining an understanding of SBA's internal controls, determining if internal controls had been placed in operation, assessing control risk, and performing tests of controls. We limited IT internal control testing to those controls necessary to achieve objectives described in GAO's *Financial Audit Manual* (FAM) and FISCAM. We do not provide an opinion on internal controls in this report. This report is for management use only. The full internal control report for SBA's FY 2005 financial statement audit is under separate cover.

Our consideration of IT internal controls over financial reporting would not necessarily disclose all matters in internal controls over financial reporting that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants (AICPA) and OMB Bulletin No. 01-02, as amended, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal controls 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.

Material weaknesses are reportable conditions in which the design or operation of one or more internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal control, misstatements, losses, or noncompliance may nevertheless occur and not be detected.

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.
- OMB Circular 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 Standards (FIPS) and in its 800 series Special Publications.

This report contains the results of our review, which identified certain IT control weaknesses, and our recommendations for improvement. We have reported these IT control weaknesses in SBA's FY 2005 financial statement internal control report as a reportable condition.

Very truly yours,

COTTON & COMPANY LLP

[Exemption 2]

Loren F. Schwartz, CPA, CISA

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. They impact 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, and 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, addresses the validity of transactions and whether 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 six major components operated and maintained by SBA offices and external contractors, as described below.

1. **Loan Accounting System (LAS)** is 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)** is 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. **Disaster Credit Management System (DCMS)** is a client-server application that supports loan-making functions associated with a disaster loan application, beginning with the processing of disaster declaration information and ending with final disbursement of funds. Loan-processing activities are supported by scanned images in a "paperless" environment. Only portions of DCMS have been fully implemented. The vision for DCMS is to create an electronic case file that will contain all relevant information concerning a loan application. This will enable DCMS users to view all documents online and from different geographical locations. DCMS is maintained by a third-party service provider, Corio, Inc., in Tempe, Arizona, with the backup facility in Herndon, Virginia. ODA, the system owner, is responsible for ensuring adequate controls over developing and maintaining the system.

4. **Denver Finance Center (DFC) systems** include 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.

5. **Joint Accounting and Administrative Management System (JAAMS)** is a client-server financial management system used by all SBA offices for administrative accounting functions. The JAAMS production server and database were relocated from UNISYS during FY 2004 to a third-party vendor, Corio, in 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 facility becomes inoperable.

6. **Local- and Wide-Area Networks (LANs and WANs)** are 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 operating these systems and periodically monitors to ensure compliance.

In addition, SBA's financial management activities rely on systems developed, maintained, or operated by external parties for processing and exchanging data related to functions, such as loan servicing and payroll. External parties include Corio, Colson Services Corporation, UNISYS, and the USDA National Finance Center (NFC). 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 2005 RESULTS

SBA continued to improve internal control over its information system environment during FY 2005 in certain areas. Specifically, SBA:

- Upgraded the JAAMS database and application to include stronger logical access controls and auditing capabilities.
- Enhanced controls over its network by adding additional Intrusion Detection System sensors to the internal network.

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

- Management did not take appropriate action to correct known prior weaknesses in a timely manner.
- Controls over administering network accounts remained weak.
- Controls over logging and monitoring activities at the network and application levels remained weak.

In the remainder of this report, we discuss results of the FY 2005 review and the status of management actions to address prior-year recommendations and new weaknesses identified in FY 2005. We also present our recommendations for improvements. This report includes the following attachments:

Attachment	Title
1	Status of Prior-Year Audit Recommendations
2	SBA Responses with Auditor Comments
3	SBA Management Responses

[Exemption 2]

Freedom of Information/Privacy Act Release
Redaction Marker

Description	Security Program Controls - 5 pages
FOIA or PA Exemption(s)	FOIA Exemption (b)(2)
Reason	Information related to IT security practices could facilitate breaches

Freedom of Information/Privacy Act Release
Redaction Marker

Description	Attachment 1 - Status of Prior-Year Audit Recommendations - 14 pages
FOIA or PA Exemption(s)	FOIA Exemption (b)(2)
Reason	Information related to IT security practices could facilitate breaches.

Freedom of Information/Privacy Act Release
Redaction Marker

Description	Attachment 2 - SBA Responses with Auditor Comments - 2 pages
FOIA or PA Exemption(s)	FOIA Exemption (b)(2)
Reason	Information related to IT security practices could facilitate breaches.

Freedom of Information/Privacy Act Release
Redaction Marker

Description	Attachment 3 - SBA Management Responses - 9 pages
FOIA or PA Exemption(s)	FOIA Exemption (b)(2)
Reason	Information related to IT security practices could facilitate breaches

REPORT DISTRIBUTION

Recipient	No. of Copies
Chief Information Officer	1
Associate Administrator for Disaster Assistance	1
General Counsel	3
Chief Financial Officer	1
Chief Financial Officer Attn: Jeff Brown	1
Government Accountability Office	1