PLANNING FOR THE LOAN MANAGEMENT AND ACCOUNTING SYSTEM MODERNIZATION AND DEVELOPMENT EFFORT

Report No.: 8-13
Issued: May 14, 2008

Prepared by the
Office of Inspector General
U. S. Small Business Administration

U.S. Small Business Administration
Office Inspector General

Memorandum

To: Eric R. Zarnikow
Associate Administrator for Capital Access

Christine Liu
Chief Information Officer

Deepak Bhargava
LMAS Project Manager

Date: May 14, 2008

/s/ Original Signed
From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Report on Planning for the Loan Management and Accounting System Modernization and Development Effort
Report No. 8-13

This report addresses SBA's Loan Management and Accounting System (LMAS) modernization and development effort. The LMAS project, currently in the planning phase, was initiated in November 2005 to modernize SBA's mainframe-based Loan Accounting System (LAS) and make it independent from the mainframe, which was inflexible, presented security risks, and was based on obsolete technology. This report addresses progress that the Agency has made since project inception, the soundness of SBA's project management approach, and the adequacy of oversight activities that have been established to review the conduct and requirements of the planning effort. It is intended to communicate areas of risk that need to be addressed as the LMAS project progresses.

In September 2005 the OIG reported that, according to SBA's strategic systems plan, the single biggest challenge facing SBA was the modernization of its loan accounting process, which was still being supported by LAS as the central hub.[1] We noted that LAS was close to the end of its expected useful life and was not compliant with SBA's Information Technology Architecture. To address these issues, we recommended that SBA immediately develop and deploy an effective LAS migration or modernization plan.

[1] *SBA Needs to Implement a Viable Solution to its Loan Accounting System Migration Problem*, Report Number 05-29, September 30, 2005.

We initiated this audit of LMAS to identify technical and management issues early in the project's development life cycle. The objectives of the audit were to evaluate the (1) progress SBA has made since project inception, (2) soundness of the project management approach, and (3) adequacy of project oversight. To address our objectives, we interviewed SBA personnel, and reviewed SBA policy documents, LMAS project planning materials, contracts, and budget submissions.

We also reviewed documents provided by the LMAS Project and Steering Oversight Council and LMAS Change Control Board. In addition, we assessed SBA's compliance with Federal laws and regulations regarding the development and protection of Federal information systems and data. We further reviewed documents that identified current risks and vulnerabilities related to the LAS system. Our audit was conducted between March 2007 and January 2008 in accordance with *Government Auditing Standards* prescribed by the Comptroller General of the United States.

BACKGROUND

The LMAS project is one in a series of attempts by SBA during the past several years to update existing financial software application modules that currently comprise LAS and to migrate them off of the mainframe environment. [FOIA Ex. 2

]. LAS has been in place for over 30 years, is inflexible, and provides an end-user interface that is both difficult to navigate and comprehend.

As required by the Federal Information Security Management Act (FISMA) and the Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, [FOIA Ex. 2

].

To identify the best solution for addressing the limitations of LAS and the security risks of operating in a mainframe environment, in December 2004 the Office of the Chief Information Officer (OCIO) prepared a *Migration Mainframe Business Case Analysis*, outlining several alternatives. Based on this analysis, the OCIO recommended migrating LAS off the mainframe without adding any new user requirements or functionality. This alternative was determined to present the lowest risk and to be the most cost effective solution as it did not constitute a re-design or new systems development effort. The OCIO's analysis indicated that this alternative would allow SBA to replace LAS in a more strategic manner

without the time constraint imposed by the impending expiration of the mainframe contract. The initial goals of the proposed migration plan were to:

- Reduce the extremely high cost of the current mainframe hardware;
- Have a solution in place prior to the expiration of the mainframe contract in February 2007 to avoid the need to re-compete the contract; and
- Address the security issues associated with the current mainframe-based entry screens.

By migrating LAS off of the mainframe, the Acting Chief Information Officer (CIO) in 2005 estimated that SBA could potentially save $16.4 million during the first 5 years of operation outside of the mainframe. The CIO proposed to initiate the project in January 2005, with the migration of LAS to a new operating platform and termination of the mainframe contract in February 2007. However, the OCIO's proposal to initiate this project was not approved by SBA's Business Technology Investment Council.

In September 2005 the OIG reported that even though LAS presented a substantial risk to the Agency, SBA had not yet adopted and implemented a definitive migration strategy or replacement approach for LAS.[2] We recommended that the Agency adopt a plan to expedite the migration of LAS off the mainframe and to make it the highest priority of SBA.

Following the OIG report in November 2005, SBA announced that it was initiating the LMAS project. At that time, SBA stated its intent to implement a single integrated loan and financial management system that not only included migration to a new operating platform, but also included the modernization of all the loan system components—from the core loan functions to the 19 subsystems associated with loan processing and servicing operations. A November 14, 2005, project initiation memorandum stated that, given the budget environment, the Agency's intent was to develop the project incrementally. It also stated that the project was expected to take several years or more and would have significant budget requirements. In February 2006, the Administrator again announced that the Agency would incrementally transition from the legacy loan systems to a more modern and cost effective LMAS.

To manage the project, SBA established an LMAS Project and Steering Council comprised of senior executives that meet weekly to evaluate the project status and

[2] *SBA Needs to Implement a Viable Solution to its Loan Accounting System Migration Problem*, Report Number 05-29, September 20, 2005.

provide direction. The Committee members include the CIO, Deputy CIO, Chief Financial Officer, the Administrator's Senior Advisor for Policy and Planning, and the Associate Administrators for Management and Administration, Capital Access, and Disaster Assistance. Additionally, the Associate Administrator for Capital Access was designated to be the project champion.

RESULTS IN BRIEF

Despite the urgency of addressing LAS security vulnerabilities, SBA was unable to replace the system prior to the expiration of the mainframe contract in February 2007, causing the Agency to renew costly contracts for mainframe and application support services for another 5 years. These services are expected to cost approximately $6 million per year.

Currently, LMAS remains in the project planning phase—the first stage of the systems development effort. The project is expected to stay in this phase for another year because SBA revised its acquisition strategy in October 2006, and decided to adopt the Statement of Objectives (SOO) methodology in December 2006 instead of using a requirements-based Request for Proposal (RFP). The SOO methodology is a seven-step approach to performance-based acquisition, under which SBA will identify the contractor who can design the best system for accomplishing SBA's business objectives. SBA believes this approach will save the Agency time and money and result in a better product because it is based on elaborate market research, due diligence, and prototyping processes in selecting the integration contractor. Under revised plans, it is unclear when LAS will be migrated off of the mainframe as the timing of the migration effort will be determined by the solution provider, who will not be identified until SBA awards the contract in late April 2008. However, the LMAS project manager has indicated that once portions of LMAS are completed, they will be migrated off the mainframe.

Because SBA was unable to migrate LAS off the mainframe, [FOIA Ex. 2

]. By delaying the migration, SBA is not adhering to Federal guidance that requires timely remediation of information security risks. [FOIA Ex. 2

].

The audit also disclosed that SBA had not established either an enterprise-wide or project-level quality assurance (QA) function to ensure that LMAS project deliverables meet SBA's requirements and quality standards, as required by

OCIO. While the LMAS Project and Steering Council has provided independent oversight of the project, it cannot perform the wide range of quality assurance activities and technical reviews required for a project that is as large and complex as LMAS.

Finally, the project lacks an approved Quality Plan that establishes the standards and procedures that will be employed to ensure adherence to OCIO's requirements, as required by Federal Acquisition Regulations (FAR). Because SBA did not finalize a Quality Plan in time for the project solicitation, it will need to ensure that such requirements are developed before a contract is awarded for LMAS. According to the OCIO, SBA has requested that vendors who compete for the LMAS contract include in their proposals a Quality Assurance Surveillance Plan, and will ensure this plan is in place prior to the solution provider's commencement of any work task.

SBA will also need to establish an enterprise-wide and a project-level QA function for the LMAS project. Doing so early in the project life cycle is essential to provide independent assurance on project reporting and metrics, compliance with SBA Information Technology policy, and an independent assessment of the project deliverables. Although the Agency has not effectively established a project-level QA function for LMAS, OCIO is pursuing two enterprise-wide QA activities. It is currently piloting an Enterprise Change Control Board, which when fully implemented, will review LMAS. Also under the new OCIO organizational structure, an enterprise-wide quality assurance (QA) component is being proposed.

On May 14, 2008, the Chief Information Officer provided a formal response to the draft that incorporated comments from the Office of Capital Access, generally concurring with recommendations 1, 2, and 3. However, management did not provide time frames for implementing proposed actions to be fully responsive to the recommendations. Further, we did not receive comments from the LMAS project manager addressing recommendations 4 and 5. Therefore, we plan to pursue a management decision on these two recommendations through the audit resolution process. The full text of management's comments can be found in Appendix II.

RESULTS

SBA Has Not Migrated LAS Off the Mainframe

To-date, SBA has expended approximately $1 million of the $1.5 million budgeted for the initial development of the system to:

- Update the project capital asset plans and submit them to OMB;

- Engage in market research to identify the most likely commercial-off-the-shelf (COTS) products that could be used replace either all or part of LAS; and

- Contract for project management services to assist in project support and an RFP for the acquisition of a replacement system.[3]

Contrary to the OCIO's recommendation in the *Business Case Analysis* and concerns raised by the OIG in May 2006, SBA did not migrate LAS off the mainframe platform when the mainframe contract expired in February 2007 to reduce the cost and security risks associated with the mainframe hardware. Consequently, in February 2007, SBA entered into new contracts for mainframe and applications support. These contracts will expire in January and April 2012, respectively, and together, are estimated to cost approximately $30 million over the 5-year life of the contracts.

SBA's limited progress in developing LMAS is largely attributable to the Agency's decision this year to revise its acquisition strategy. According to SBA's contract for LMAS project management services, a modernization roadmap and integrator S*tatement of Work* for the project were scheduled to be completed and accepted by SBA in September 2007. In October 2006, SBA revised its acquisition strategy from a requirements-based RFP to an SOO methodology, and on October 5, 2007, announced that it was looking for a solution provider for the LMAS project. Rather than building a system based on defined system requirements, the SOO approach will identify the contractor who, based on an understanding of SBA's business processes, can design the best system for accomplishing SBA's business objectives. SBA believes this approach will save the Agency time and money and result in a better product because it is based on elaborate market research, due diligence, and prototyping processes in selecting the integration contractor.

Current plans call for SBA to select the best solution provider and award the contract by April 22, 2008. According to an October 5, 2007, SBA press release, the total cost of developing LMAS over the next 3 to 5 years and the cost of maintaining and operating the system for the next 10 years could approach $125 million.

Because SBA revised its acquisition strategy, the Agency has essentially restarted the LMAS project, placing it in the same position as it was in 2005 when LMAS was first initiated. Consequently, LMAS remains in the initial activities related to the project planning phase. Unless carefully managed, this strategy could increase

[3] On March 23, 2006, SBA hired Macro Solutions of Arlington, VA for systems development support.

project risks as it places a high reliance on the contractor to both develop system requirements and to design the solution, potentially locking the Agency into using one service provider. It also could impact SBA's ability to take advantage of changes in technology that occur during the project's life cycle. However, SBA has acknowledged these risks and has indicated that it will take steps to mitigate them.

By Delaying its Mainframe Migration, SBA is Not Adhering to Federal Guidance That Requires Timely Remediation of Information Security Risks

Although LAS is designated a [FOIA Ex. 2] per FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, [FOIA Ex. 2

]. According to SBA's November 27, 2007, *Plan of Action and Milestones* (POA&M), [FOIA Ex. 2

].

Currently, SBA's migration plans are linked to the solution to be identified under the SOO approach. Because a contract will not be awarded to a solution provider until late April 2008, it is unlikely that migration will occur before the new contracts expire in 2012, and SBA will continue to incur significant mainframe costs. Further, it is unclear what priority will be given to the migration effort and when in the project cycle it will occur under SBA's revised acquisition strategy. If not addressed in the project plan, migrating LAS off the mainframe could be pushed toward the end of the project. Additionally, because the timelines for the LMAS project are not sufficiently integrated with that of SBA's new mainframe contract, LMAS development activities may not dovetail with processing requirements of the mainframe contract.

By delaying the mainframe migration, SBA has not complied with Federal guidance that requires timely remediation of information security risks, and has left the Agency vulnerable to potential system attacks by external sources. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, requires that organizations employ appropriately tailored security controls. Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, also requires agency heads to, "Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of

such information." As mentioned above, [FOIA Ex. 2]. These vulnerabilities, if not mitigated, will likely affect conclusions reached in future Federal Information Security Management Act (FISMA) reviews and financial audits of SBA. Consequently, we believe that SBA should take interim steps to address the security vulnerabilities until the migration can be completed.

SBA Lacks Both an Enterprise-wide and Project-level Quality Assurance Function to Ensure that LMAS Adheres to Quality Standards

OCIO's *Systems Development Management* policy requires that an enterprise QA function be established to provide oversight of software development projects, which is independent of all SBA projects and programs. The purpose of the enterprise QA function is to ensure that all IT projects undertaken by SBA adhere to SBA's quality standards and procedures throughout the software development and maintenance process. This function is intended to allow SBA to fulfill its mission under the Clinger Cohen Act to provide independent assurance that software development, testing and configuration management efforts are aligned with SBA's IT architecture and are compliant with SBA development standards and policies.

In addition, OCIO requires that a QA group be established at the project-level to execute QA activities for each software project. These activities include verifying that project plans, standards, and procedures are in place and can be used to review the software project and to evaluate the deliverable software products against these standards. The group is to be headed up by a QA manager, who is independent of the project and is responsible for ensuring that adequate resources and funding are provided for performing QA activities.

Despite these requirements, SBA lacks both an enterprise QA function and an adequate project-level QA function to oversee the LMAS project. The CIO is in the process of establishing an enterprise QA group and has hired a manager for the group, but has not been allocated additional positions with which to staff up the group. The project-level QA function is currently being performed by the LMAS Project and Steering Council, which is made up of senior executives. These executives include the CIO, Deputy CIO, Chief Financial Officer, the Administrator's Senior Advisor for Policy and Planning, and the Associate Administrators for Management and Administration, Capital Access, and Disaster Assistance.

While several of the council members have the organizational freedom to be the "eyes and ears" of senior management on the LMAS project, with the exception of the CIO, they do not possess the expertise needed to conduct technical reviews of the software development activities. They also cannot devote the time that would

be required to perform all of the QA activities. For example, the individual(s) managing the QA process would be expected to participate in software design and code reviews, ensure that software and test documentation is subject to configuration management, and participate in software verification and validation activities. They would also be expected to continuously review project activities and audit software work products throughout the project's life cycle to provide management the information with which to judge whether LMAS is adhering to established quality guidelines. Because council members have full time responsibilities for the organizations they manage, they cannot devote the time to QA that is needed nor do they have the IT background needed to review project deliverables for adherence to OCIO configuration management and other quality requirements.

According to the LMAS Project Manager, project-level QA will also be met through Independent Verification and Validation (IV&V), which determines whether products produced at each step of the development effort fulfill requirements and function as intended. However, while IV&V testing is important to ensure that system requirements are met, it is fundamentally different than software quality assurance and has different reporting interfaces. IV&V is a systems engineering process that is independent from the project team, which emphasizes the *completeness and correctness* of the products/deliverables; while software QA emphasizes *compliance* with standards and procedures and is matrixed with the project team to provide daily oversight of the project. Therefore, the IV&V testing will not adequately ensure that the LMAS software is designed in compliance with OCIO's quality standards.

Inadequate software quality could lead to project cost and schedule overruns, a system that does not meet SBA's requirements, software failures that require costly repairs, limited interoperability of system components, and inflexibility of the system to adapt to new customers, tasks and other hardware and software. Given the size and complexity of the LMAS, and that multiple system interfaces are planned, SBA should consider outsourcing the project-level QA activities to obtain a dedicated team with the expertise needed to perform the full range of QA activities, as other Federal agencies have done.

For example, the State Department recently outsourced QA on a large, complex network modernization project entitled State Messaging and Archive Retrieval Toolset (SMART). This QA function established quality goals, related performance baselines and periodically assessed project performance results against established quality and performance baselines. As a result, SMART project stakeholders had additional assurance that project activities and deliverables met predetermined standards and that an effective corrective action process was deployed early in the project's lifecycle thereby avoiding costly rework.

SBA Has Not Finalized a Quality Plan for the LMAS Project

OCIO's *Systems Development Management* policy requires that a quality plan be established in the early stages of systems development projects. The quality plan establishes standards and procedures that will ensure adherence to the OCIO's policies and establish high level quality requirements, thereby facilitating the identification of defects early in the project life cycle and avoiding costly rework. These quality standards include documentation and deliverable acceptance requirements, testing, configuration control, problem reporting and corrective action processes, and periodic audits. Further, the quality plan should be developed prior to solicitation, as required by the *Federal Acquisition Regulations* (FAR). These regulations state that "the contracting officer shall include in the solicitation and contract the appropriate quality requirements."[4] FAR further provides that agencies may either prepare the quality plan or require vendors to submit a plan for consideration in the development of the agency's plan.[5] The FAR also states that requiring compliance with "higher level" quality standards (e.g., industry standards, such as ISO 9001) is appropriate in solicitations and contracts for complex or critical items.[6]

Despite these requirements, SBA released its solicitation proposal for LMAS without having an approved quality plan for LMAS. A draft plan was developed, but it was never finalized or approved by the CIO. Consequently, the lack of a quality plan early in the LMAS planning phase limits the consideration of quality standards, processes, and metrics in the initial planning iterations and project management performance baselines. In subsequent project phases (such as execution, monitoring and control) it can also significantly increase the risk of noncompliance with SBA's enterprise quality standards; adversely affect key control processes, such as project performance reporting, change control management, and defect repair and prevention; and lead to costly rework.

The LMAS project manager told us that because the FAR allows agencies to require its solution provider to propose quality plans, and the provider that SBA selects will be responsible for preparing the LMAS S*tatement of Work*, the Agency plans to have the provider propose the draft quality plan. While we agree with SBA's interpretation of the FAR, when the solicitation is for a complex or critical system, such as LMAS, FAR provides that compliance with higher level standards should be required. We noted that SBA's solicitation did not require compliance with higher level standards, such as those defined in OCIO's *Systems Development Management* policy or industry standards.

[4] FAR 46.201(a).
[5] FAR 37.604.
[6] FAR 46.202-4(b).

RECOMMENDATIONS

We recommend that the Associate Administrator for Capital Access:

1. Make cost-effective remediation of mainframe vulnerabilities a priority and ensure that migration of LAS occurs before the current mainframe contract expires in 2012 to reduce SBA's mainframe costs and timely mitigate associated security risks.

We recommend that the Chief Information Officer:

2. Ensure interim remediation and prioritization of identified LAS vulnerabilities are completed consistent with the guidelines established by FIPS 200 and OMB A-130.

3. Design and implement an Enterprise-wide QA function that fully addresses the risk and scope of the LMAS project and ensures the OCIO can fulfill responsibilities under the Clinger-Cohen Act to provide independent quality assurance and oversight of Information Technology investments.

We recommend that the LMAS project manager:

4. Consider outsourcing the project-level QA function to ensure alignment between LMAS project deliverables with SBA's quality standards.

5. Finalize and obtain OCIO approval of the Quality Plan for LMAS and incorporate the plan's quality standards into the contract that is ultimately awarded for development of LMAS.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On April 18, 2008, we provided SBA a draft copy of the report for comment. We discussed the findings and recommendations with the Chief Information Officer and LMAS project manager. On May 14, 2008, the Chief Information Officer provided written comments to the draft that incorporated comments from the Office of Capital Access. These comments, which address recommendations 1, 2 and 3, are summarized below. The full text of these comments can be found in Appendix II. We did not; however, receive comments from the LMAS project manager addressing recommendations 4 and 5.

Management generally concurred with recommendations 1, 2 and 3, but did not provide time frames for implementing proposed actions. Management agreed to

form a team to re-evaluate open mainframe vulnerabilities to determine alternative cost-effective solutions to remediate vulnerabilities and to develop a strategy for addressing the vulnerabilities that will consider the associated risk and cost implications. Management also agreed to ensure that interim remediation and prioritization of LAS vulnerabilities is consistent with FIPS 200 and OMB A-130 guidance. Finally, management stated that it is currently working on an Agency-wide QA oversight function, which will include developing QA standards, monitoring the LMAS project plan and implementing QA activities throughout the LMAS project schedule. These actions will be fully responsive to recommendations 1, 2 and 3 once the Agency submits time frames for implementing proposed actions. We will pursue a management decision on recommendations 4 and 5 through the audit resolution process.

ACTIONS REQUIRED

Because your proposed actions do not provide target dates to be considered fully responsive to recommendations 1, 2 and 3, we request that you provide a written response by May 28, 2008, providing the time frames you propose for implementing the recommendations.

APPENDIX I. SUMMARY OF LOAN ACCOUNTING SYSTEM VULNERABILITIES REPORTED IN SBA'S FY 2007 PLAN OF ACTION AND MILESTONES SUMMARY

LAS Subsystem*	Number Identified as High-Risk	Number Identified as Medium-Risk	Number Identified as Low-Risk	Total Number of Vulnerabilities by Subsystem
Subsystem 1	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 3	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 4	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 5	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 6	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 7	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 8	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2
Subsystem 9	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2**
Totals	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2	FOIA Ex. 2

* For security purposes, the subsystems have not been named.
**One vulnerability was not deferred to FY 2013.

Source: SBA's November 27, 2007, Loan Accounting System Plan of Action and Milestones