REVIEW OF ALLEGATIONS CONCERNING HOW THE LOAN MANAGEMENT AND ACCOUNTING SYSTEM MODERNIZATION PROJECT IS BEING MANAGED

Report Number: 9-17
Date Issued: July 30, 2009

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 Rider
Chief Information Officer
/s/ Original Signed

Date: July 30, 2009

From: Debra S. Ritt
Assistant Inspector General for Auditing

Subject: Final Report on the Review of Allegations Concerning How the Loan Management and Accounting System Modernization Project is Being Managed
Report No. 9-17

This report presents the results of our review of allegations regarding the Small Business Administration's (SBA) management of the Loan Management and Accounting System (LMAS) Modernization Project. LMAS, which will receive supplemental funding from the American Reinvestment and Recovery Act, is integral to SBA's strategy for improving, streamlining and automating information technology systems related to lender processes and lender oversight.

The project was initiated in November 2005 to integrate the Agency's loan monitoring and financial management systems and to move them to a new operating platform. The project 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.

In December 2008, the Office of Inspector General received a complaint primarily alleging that (1) because the Quality Assurance (QA) process established for the project was not independent from the project management staff, issues identified by the Quality Assurance/Independent Verification and Validation (QA/IV&V) contractor were not being reported to senior management; (2) a defined process for accepting contract deliverables had not been established; (3) deliverables for one of the contracts were behind schedule; (4) contractor employees participated in meetings without being cleared or trained on information security procedures; and (5) the risk management process established for the project was immature. The complaint also made other minor allegations involving desktop security and events

that had not yet occurred or were outside the scope of the LMAS project. Our review of the complaint focused on only the five major issues outlined above.

To determine whether the QA process was independent from project management staff, we examined SBA's files for the three LMAS blanket purchase agreements (QA/IV&V, project management, and systems integration) to identify the project reporting structure and assess compliance with SBA's *Systems Development Methodology* (SDM) requirements for QA. We also evaluated actions taken by SBA to implement our prior audit recommendations that an independent project-level QA process be established and that an enterprise-wide QA function be implemented.[1] We assessed whether project issues identified by the QA/IV&V contractor were being reported to senior management by comparing contractor findings of deficiencies with those noted on the project's risk register[2] and project plans,[3] and through discussions with program management and the Chief Information Officer (CIO).

To determine whether a process had been established for accepting contract deliverables, we compared the deliverable review process established for the LMAS project with requirements established in the SDM and with the contractor's SDM criteria. To assess the timeliness of contract deliverables, we interviewed the Program and Project Managers and compared due dates on multiple project plans. To determine whether contractor staff participated on the project before being cleared, we: reviewed SBA's clearance policies; identified contract employees from project documentation; obtained information on the meetings they attended and tasks they were assigned; and determined whether they had the required clearance forms.

To determine the maturity of LMAS risk management, we compared LMAS risk management practices with those established in the *Risk Management Plan* for the project and the Office Management and Budget's (OMB) Capital Planning Guide.[4] We also obtained information from contract procurement officials, the Office of the Chief Information Officer (OCIO), and LMAS project officials. We performed our review between September 2008 and April 2009 in accordance with Chapter 6 of the *Government Auditing Standards* prescribed by the Comptroller General of the United States.

---

[1] Recommendations No. 4; OIG Report No. 08-13, *Planning for the Loan Management and Accounting System Modernization and Development Effort*, May 14, 2008.

[2] The risk register is an iterative document that summarizes all risks that may affect the project, their causes, and potential responses.

[3] The Program Manager defined the project plans as "work breakdown structures."

[4] Supplement to OMB Circular A-11, Part 7: *Planning, Budgeting and Acquisition of Capital Assets*.

BACKGROUND

The LMAS project is one in a series of attempts by SBA during the past several years to upgrade existing financial software and application modules and to migrate them off the mainframe environment. LMAS remained in the planning phase until September 2008 when SBA awarded three blanket purchase agreements to: (1) establish QA/IV&V monitoring and oversight ($5 million); (2) provide project management support ($7.5 million); and (3) provide systems integration services ($250 million). To-date, three task orders have been issued from the third blanket purchase agreement to:

- migrate the existing Joint Administrative Accounting Management System (JAAMS) application to a new hosting site;
- provide a proof of concept pilot; and
- develop a road map for the LMAS project.

To oversee the project, SBA established the LMAS Project Steering Council, which is comprised of senior management officials that meet weekly to evaluate the project status and provide direction. The Council members include the CIO, Acting Chief Financial Officer (CFO), the Senior Advisor for Policy and Planning, the Consultant to the Administrator, the Associate and Deputy Associate Administrators for the Office of Capital Access (OCA), the Acting and Deputy Associate Administrators for Disaster Assistance, the Directors for Financial Assistance and Financial Systems and LMAS, and the Supervisory Financial Analyst for Financial Assistance. OCA is the project sponsor and the day-to-day management of the project is the responsibility of the Program Manager, who reports to the CFO.

The OIG has issued two reports on the LMAS project since it was first conceived in 2005. In September 2005 the OIG reported that even though the Loan Accounting System (LAS) posed a substantial risk, SBA had not yet adopted and implemented a definitive migration strategy or replacement approach.[5] In May 2008 an OIG audit of the planning process for LMAS found that costly mainframe contracts had to be renewed because migration of the system was delayed. The Agency also had not established either an enterprise-wide or project-level QA function to ensure that LMAS project deliverables met SBA's requirements and quality standards, as required by the Agency's SDM policy.[6] This policy requires that an enterprise QA function, which is independent of SBA projects and programs, be established to ensure that IT projects adhere to Agency quality

---

[5] OIG Report No. 05-29, *SBA Needs to Implement a Viable Solution to Its Loan Accounting System Migration Problem*, September 30, 2005

[6] OIG Report No. 8-13, *Planning for the Loan Management and Accounting System Modernization and Development Effort*, May 14, 2008.

standards and procedures throughout the systems development and maintenance process. These standards are outlined in the OCIO's *Enterprise Quality Assurance Plan*.

The enterprise QA function also enables the OCIO to meet its mandate under the Clinger-Cohen Act to provide independent assurance that systems development, testing, and configuration management efforts are aligned with SBA's IT architecture and quality standards. Additionally, project managers are responsible for implementing a project-specific QA program built on the standards established in the *Enterprise Quality Assurance Plan*.

After the May 2008 OIG report, which recommended outsourcing the project-level QA function, the LMAS Program Manager contracted with the IV&V contractor to provide project-level QA and closed the recommendation.

RESULTS IN BRIEF

Our review confirmed that the project-level QA process was not independent from project management staff; a process had not been established for accepting contract deliverables until January 2009; several deliverables were behind schedule; contractors participated in meetings and were assigned tasks without being cleared or trained on SBA security procedures, and the project's risk management process was immature. We did not, however, find that the Program Manager filtered problems identified by the QA/IV&V contractor. More specifically, we found that:

- An independent QA function had not been established for the LMAS project, as we previously recommended. While a contractor had been hired to evaluate and monitor compliance with quality standards, the contractor reported to the Program Manager, which did not provide the level of independence called for by the Agency's SDM. The CIO also had not designated an independent QA Manager for the project. Because the Program Manager functioned as the QA Manager, he was in a position to determine which problems identified by the QA/IV&V contractor would be reported to senior management. However, we found no evidence to suggest that he withheld issues from senior management. We also determined that the CIO had not established an enterprise-wide QA function as previously recommended.

- The project lacked a defined process for accepting deliverables until months after task orders were awarded. A process was later defined in January 2009, which differed from the process suggested by the

Agency's SDM policy. For example, it did not identify documents to be reviewed, review methods, associated review time frames, or officials that would be responsible for reviewing deliverables.

- Deliverables associated with task orders from the systems integration blanket purchase agreement were past due, which may impact timely project completion. For example, the completion date for the Integrated Baseline Review (IBR) under Systems Integration Task Order 1 slipped three months from December 11, 2008 to March 12, 2009. The extension of the IBR due date was improper because SBA's Earned Value Management (EVM) policy requires that it be performed prior to contract initiation to establish cost, schedule, and performance goals. The March 31, 2009, completion date for the migration of JAAMS under Task Order 1 was also not met.

- Seventeen of 45 contractor employees started on the project before completing SBA's clearance process, some of whom worked on the project for more than 45 days before completing the clearance process or receiving the required computer security awareness training. These employees attended meetings, and according to the LMAS *Action Items List,* 10 were assigned action items. The Program Manager believed that the employees were merely attending high-level meetings, which did not require vetting through SBA's clearance process.

- The LMAS risk register did not contain all of the information recommended by OMB's *Capital Programming Guide*[7] and the *LMAS Risk Management Plan*, such as risk ratings and plans for mitigating some of the identified risks. Without a complete risk register that identifies how project staff will respond to specific risks, the success of the LMAS project could be affected.

To address these issues, we recommended that the LMAS contract be amended to require that the QA/IV&V contractor report to the Program Manager and that an independent QA Manager be designated by the CIO. We also recommended that a well-defined process be established for accepting LMAS deliverables, contractor employees not be allowed to work on LMAS until they have been properly vetted in accordance with SBA policies and procedures, and that the LMAS risk register be revised to include all fields identified in the LMAS *Risk Management Plan* and key information that is currently missing in the risk register. Finally, we

[7] Supplement to Office of Management and Budget Circular A-11, Part 7: *Planning, Budgeting and Acquisition of Capital Assets*.

recommended that the CIO establish an enterprise-wide QA function to ensure that all IT projects comply with Agency quality standards.
Management's response generally disagreed with the audit results. We believe management's views were primarily those of the Program Manager, who was the subject of the allegations. We provided the Program Manager additional time to address the audit findings before issuing the draft report. However, the Program Manager was not able to provide adequate evidence supporting his disagreements on the audit findings. The Program Manager's views have been incorporated and evaluated within the body of the report. Further, while management agreed to take action on all of the recommendations, we found that the actions proposed in response to Recommendations 1, 2, 3, 5, and 7 were not sufficient to fully address the related findings. These actions largely do not comply with established IT governance protocols, such as the Agency's SDM, or are contrary to Agency policy.

Finally, we are particularly concerned that the CIO has chosen not to immediately establish a QA oversight function as a vehicle for assessing and improving IT projects, plans to provide only a "high level" Quality Manager for the LMAS project, and has not specified when the LMAS Quality Manager will be designated.

RESULTS

The Project-Level QA Function for LMAS Was Not Independent from Project Management

The complaint alleged that the QA process for monitoring LMAS performance was not independent from the Program Manager and that not all issues identified by the QA contractor were being reported to senior management. The SDM states that the project-level QA function should have a reporting channel to senior management from a QA Manager that is independent of project line management. This requirement, which the CIO confirmed applied to LMAS, was communicated to Agency staff through SBA Procedural Notice 9000-1596, issued on November 9, 2005.

However, we found that the QA/IV&V contract required the contractor to report exclusively to the Program Manager and the Contracting Officer's Technical Representative (COTR), who reports to the Program Manager. The CIO was unaware that the QA/IV&V contractor reported exclusively to the Program Manager and COTR. She also had not designated a QA Manager for the LMAS project to ensure that the project-level QA function was independent from the Program Manager. Although the CIO had been made aware of these findings in December 2008, as of May 8, 2009, a QA Manager still had not been designated

for LMAS. Having a QA process that functions independently from LMAS project management provides assurance that quality and performance issues will be accurately and completely reported to senior SBA managers.

Further, although the Program Manager was in a position to determine which problems identified by the QA/IV&V contractor would be reported to senior management, we found no evidence that he withheld significant LMAS problems or risks from senior managers.

Finally, we followed up on our previous recommendation that the CIO implement an enterprise-wide QA function needed to fulfill her oversight responsibilities for information technology investments under the Clinger-Cohen Act. Although in May 2008 the CIO agreed to implement the recommendation, as of July 30, 2009, an enterprise-wide QA function had not been established.

A Well-Defined Process for Accepting Contract Deliverables Had Not Been Established

The complaint alleged that the project lacked a well-defined process for submittal, review, and approval of project deliverables. Further, the complaint alleged that the delivery of services was subject to the personal interpretations of the Program Manager instead of solid SBA policies and procedures to guarantee that the best work products possible were generated. The Agency's SDM requires that a defined process be established for accepting deliverables and suggests that the process should:

- Identify documents to be reviewed, the method of review, and associated review time frames;

- Specify the types of reviews to be performed;

- Designate a review team within the Agency that includes individuals who are responsible for application development, project management, configuration management, and QA to identify defects and ensure a final quality product; and

- Ensure that the Project Manager and QA Manager approve deliverables.

We found that a process for accepting deliverables was not established until January 29, 2009, after some deliverables were rejected, including the LMAS QA Plan. Further, the LMAS process did not fully follow the process suggested by the SDM requirements because it left to the Project Manager's discretion what documents would be reviewed, the type of review to be performed, and the

composition of the review team. As a result, there was limited assurance that all deliverables would be reviewed and whether reviews would be made by the appropriate parties.

The Program Manager told us that the LMAS team found no evidence of an established, documented deliverable management process in existence at SBA. Therefore, one had to be created specifically for LMAS, which is why the process was not established sooner. He also believed that the LMAS deliverable process implemented complies with the intent of the process suggested by the SDM. Further, he told us that the LMAS solution provider (SRA) was using its own systems development methodology, called ELITE, which was fully compliant with industry standards established by the Software Engineering Institute.

In January 2009, the Program Manager presented to the CIO the solution provider's mapping of its proprietary ELITE methodology to SBA's SDM to show that the LMAS project was being managed in accordance with Agency policy for systems development projects. In a May 2009 meeting, the CIO told the OIG that she had approved of SRA's approach and was satisfied that the Program Manager was complying with Agency QA requirements.

We examined the mapping document that the Program Manager provided to the CIO and concluded that it did not provide sufficient detail for the CIO to make a determination about whether the deliverables acceptance process used by the contractor clearly defined the types of reviews to be performed of deliverables or that the appropriate reviewing parties had been identified. For this reason, we do not believe that there is adequate assurance that the LMAS project has a well-defined process for accepting deliverables. Further, the LMAS Project Manager has sole authority to determine what deliverables get reviewed, who is accountable, and the basis for acceptance.

Contractor Deliverables Were Behind Schedule

The complaint alleged that the prime contractor was behind schedule in providing deliverables on the integration services blanket purchase agreement, and that there was no action plan to address the delays. Based on our interview with the Program Manager and a review of the work breakdown structures, we determined that the prime contractor missed multiple deliverable due dates for task orders.

One delay involved a 3-month extension of the due date for the IBR from Task Order 1, which was originally scheduled for completion on December 11, 2008. The IBR is a structured review process involving all relevant SBA stakeholders and the contractor to obtain agreement on project schedule, cost, and performance

metrics and to identify risks associated with the project plan. The revised IBR completion date in a March project plan was listed as March 12, 2009. This extension, which occurred after contract initiation, was contrary to SBA's Agency Earned Value Management Policy[8] that states:

> "Per OMB Memorandum M-05-23 and Agency earned value management policy, integrated baseline reviews will be performed prior to contract initiation…" and
>
> "…it is mandatory that all major investments (investments that cost $200,000 or more in a single year, or $500,000 or more in 3 years, and all projects deemed to be of high visibility by the Business Technology Investment Counsel) use the EVMS."[9]

The Program Manager acknowledged that the IBR should have been performed earlier in the process and stated that it will be for future task orders. Further, he acknowledged that the March 31, 2009, completion date for the migration of JAAMS under Task Order 1 was also not met. The migration was delayed 3 weeks, and JAAMS did not become operational at the new site until April 20, 2009. The Program Manager attributed the late deliverables to extreme delays in getting the contractor's security background checks completed, and hardware failures. However, we confirmed that the length of the security clearance process was not unusual and should have been factored into the milestones established for the task order.

In addition, the baseline schedule for deliverables has been revised multiple times, giving the misleading appearance that the contract is on schedule even though original deliverable dates were not met. Per discussions with the Program and Project Managers, the deliverable tracking process established for LMAS was based on the project plans, which are updated periodically with modified deliverable due dates. Since LMAS project management did not conduct an initial IBR to establish performance, schedule and cost baselines, the Agency will not be able to accurately measure performance, which is necessary for meaningful Earned Value Management reporting.

Contractor Employees Attended Meetings without Required Security Vetting

---

[8] Earned Value Management is a project measurement technique that relates resource planning to technical, cost, and schedule requirements. All work is planned, budgeted, and scheduled in time-phased "planned value" increments, constituting a cost and schedule measurement baseline.

[9] *SBA Earned Value Management System Policy for Information Technology (IT) Projects*, December 2005.

The complaint alleged that contractors were present in planning and other meetings prior to meeting SBA requirements for background investigation and security clearance and had not completed security training requirements. Consequently, the complaint alleged that contractors waiting for clearances were privy to other contractor work plans, which could result in an unfair competitive advantage and legal action.

SBA Procedural Notice 9000-1684, *SBA Form 1228 Process,* requires that contractors receive a favorable preliminary background check prior to entering on duty. In addition, the LMAS systems integration task order states that the contractor is responsible for having its employees working under the task order execute all certifications required by SBA prior to beginning work. SBA requires that SBA Form 1228, *Computer Access Clearance/Security Form,* be used to initiate and document the security clearance process for new contractor employees.[10]

Based on our review of LMAS project meeting minutes and the LMAS *Action Items List*, we found that 17 of the 45 contractors on the LMAS project from November 12, 2008 to February 13, 2009, participated in the project before their background investigations were completed. These contractors attended meetings, such as the 7(a) Regular Loan Accounting Events Session and Conference Room Pilot meeting, and/or were assigned action items for the LMAS project prior to meeting SBA's background investigation and security clearance requirements.

Additionally, as of February 13, 2009, 17 (including 2 who also started work before completing background investigations) of 45 contractors had not completed their Computer Security Awareness training within 45 days, as required by the Agency's Standard Operating Procedure. Allowing contractor employees to work on the project before they have been properly vetted for security exposes sensitive SBA information to loss, or misuse.

The Program Manager acknowledged that contractors started work on the project prior to being cleared, but believed that it was ok to do so as the contractors were not given access to sensitive SBA information. He believed that SBA procedures required security clearances to be completed prior to granting access to SBA systems or data. The Program Manager contended that 16 of the unvetted contractors worked on LMAS Task Order 2 without access to sensitive systems or data, and that the contract lead worked offsite on refining the project plan, which was not sensitive.

---

[10] SOP 90 47 2, *Automated Information System Security Program,* classifies all SBA data as sensitive and requires all contractor personnel to undergo background investigations. In addition, contractor personnel occupying positions designated as critical-sensitive cannot be given access to sensitive data until an appropriate security clearance has been granted.

Risk Tracking Process Was Not Sufficiently Developed

The complaint alleged that the LMAS risk management process was immature. In order to manage IT acquisition performance goals, OMB published the *Capital Programming Guide*, which recommends that agencies track project risks in a risk register. The register should, at a minimum, indicate the risk priority, rating, response strategy, and status. To implement the OMB guidance for the LMAS project, SBA created a risk register for the project.

The risk register; however, did not contain complete information on all identified risks, such as the dates that risks were identified, residual risk, contingency plans where risks cannot be resolved, and risk ownership. Due to the incomplete capture of risk information, SBA may not be able to properly respond to unplanned incidents or to remediate project risks which may contribute to cost overruns, schedule shortfalls, and the system's inability to perform as expected. We reviewed our findings with the Program and Project Managers and provided them with the relevant OMB guidance.

RECOMMENDATIONS

We recommend that the LMAS Program Sponsor, the Associate Administrator for Capital Access:

1. Take steps to modify the contract to require the QA/IV&V contractor to report all findings and recommendations to the Program Manager *and* an independent QA manager designated by the CIO.

2. Establish a process for reviewing and accepting LMAS deliverables that complies with SDM requirements.

3. Ensure contractor employees work on LMAS only after their SBA Form 1228 Computer Access Clearance/Security Form has been signed and that they receive computer security awareness training as required.

4. Consider revising the risk register to include all fields identified in the LMAS *Risk Management Plan* and complete all missing information in the risk register such as due dates, mitigation plans and risk owners.

We also recommend that the CIO:

5. Designate a QA Manager for the LMAS project to ensure that the project-level QA function is independent from the project.

6. Immediately establish an enterprise-wide QA function that is compliant with SBA's SDM QA policy.

7. Take steps to ensure that a well-defined deliverable acceptance process is established for the LMAS project in accordance with SBA's *Enterprise Quality Assurance Plan*.

AGENCY COMMENTS AND OFFICE OF INSPECTOR GENERAL RESPONSE

On June 12, 2009, we provided a draft of this report to SBA for comment, and on July 22, 2009, we received consolidated comments from the Associate Administrator for Capital Access, Chief Information Officer, and the Director, Office of Financial Systems who serves as the Program Manager for LMAS. These comments are contained in their entirety in Appendix I.

Management generally disagreed with the audit results, but agreed to take action on all of the recommendations. We are concerned that the views expressed on the audit findings are primarily those of the Program Manager, who was the subject of the allegations. Because the Program Manager's views have already been incorporated and evaluated within the body of the report, we are not repeating his comments to the audit findings here.

While the respondents agreed to take action on all of the recommendations, we found that the actions proposed in response to Recommendations 1, 2, 3, 5, and 7 were not sufficient to fully address the related findings. These actions do not comply with established IT governance protocols; such as the SDM, which are designed to mitigate risk and achieve project objectives.

We are particularly concerned that the CIO has chosen not to immediately establish a QA oversight function as a vehicle for assessing and improving IT projects, plans to provide only a "high level" Quality Manager for the LMAS project, and has not specified when the LMAS Quality Manager will be designated. Furthermore, several of the responses attempt to modify existing SBA policy. We suggest any such changes be initiated through SBA's Clearance Procedures as outlined in SOP 00 23 6. As the Agency undertakes subsequent phases of LMAS and additional development projects, it will be critical that the OCIO provide proper oversight to ensure its standards and procedures are followed throughout the project development cycle.

We recognize the actions taken by SBA to address some of the issues that the audit team brought to their attention and look forward to resolution of all findings and implementation of all recommendations.

Recommendation 1

Management's Comments

Management has directed the QA contractor to simultaneously provide all reports to the Program Manager and OCIO's acting enterprise-level QA Manager to ensure that the QA process is independent from the project management staff.

OIG Response

Management's response is partially responsive to the recommendation. The contract terms limit communications solely to the Program Manager and COTR. Therefore, we believe modification is necessary. Modifying the contract to require the QA/IV&V contractor to report to the Program Manager and the CIO's designated QA Manager will promote the independence and impartiality of the project's QA decision-making.

Recommendation 2

Management's Comments

Management stated that the LMAS process for reviewing and accepting deliverables goes far beyond the SDM requirements. The LMAS team has created a well-defined deliverable review and approval process that exceeds the Agency's goals as stated in the SDM. However, the LMAS team will continue to review the suggestions documented in the *Enterprise Quality Assurance Plan*, evaluate the benefits and adopt the suggestions that will further improve the program's deliverable management process.

OIG Response

At the time of the complaint, there was no LMAS deliverable review process. In January, 2009 the LMAS project team implemented a deliverable review process. However, it did not contain key elements of SDM's *Enterprise Quality Assurance Plan*. This plan requires that a defined process be established for accepting deliverables and outlines oversight responsibilities between OCIO and the project team to monitor compliance with SBA systems standards. At the present time the

LMAS Project Manager has sole discretion to approve contract deliverables. Although management stated that it would evaluate and adopt suggestions to improve the project's deliverable management process, it did not specify the steps it would take to make the current process compliant with the current oversight requirements of the SDM. Therefore, we do not consider management's comments to be fully responsive to the recommendation.

Recommendation 3

Management's Comments

Management stated that it will continue to ensure that contractor employees who work at SBA office space or who need access to sensitive SBA systems or data will be granted access only after the Form 1228 has been signed. The LMAS team will ensure that these contractor employees complete required training. However, the LMAS team stated that it will not require background investigations and clearances for those contractor employees who have short-term assignments that do not access SBA systems or data.

OIG Response

Management's response does not describe the process it will employ to ensure that contractor employees will not have access to sensitive SBA data unless they have met SBA's contractor clearance requirements. Management's decision to not require background investigations for short-term contractor employees is also contrary to SBA policy; and therefore, would require an exemption from policy. Further, as all SBA data is classified as sensitive, it is questionable that a contractor employee could work on the LMAS project for as long as 6 months without exposure to any SBA data, including loan data. If SBA proposes a process that will ensure that certain contractor employees do not have access to SBA data, which is approved by the CIO, then we would consider the response to be sufficient to reach management decision. However, as currently stated, management's comments are not responsive to the recommendation.

Recommendation 4

Management's Comments

Management stated that the LMAS team has published a detailed *Risk Management Plan* that contains the same fields as those in the Risk Register. SBA believes the recommendation to complete all missing information in the Risk

Register is not cost effective or reasonable and is not based on fixing any perceived gap in the LMAS management.

OIG Response

We found management's comments to fulfill the intent of our recommendation, and therefore, it is responsive.

Recommendation 5

Management's Comments

Management stated the CIO will designate a high-level QA Manager to fulfill the independent review function. In the meantime, the CIO is providing oversight of LMAS from an enterprise-level QA standpoint.

OIG Response

We do not consider management's comments to be fully responsive to the recommendation because it has not specified a target date for appointing an independent project-level QA manager. Further, the breadth of duties of the independent project-level QA Manager as described in the SDM and *Enterprise Quality Assurance Plan* require sustained and in-depth involvement. It is not clear whether the proposed "high-level" QA Manager or CIO could devote the amount of time that would be required of the project-level QA Manager described in the SDM.

Recommendation 6

Management's Comments

Management stated that an enterprise QA framework and staffing requirements have been drafted and are under review with an expected finalization date of October 30, 2009. The QA function will oversee all IT investments, including LMAS.

OIG Response

The OIG believes that the full implementation of the QA framework, as well as staffing, to fulfill this role by October 30, 2009 is responsive. However, we note SBA has had an *Enterprise Quality Assurance Plan* since April 2004. This need

was also addressed in a prior OIG recommendation, which is past due for implementation.[11]

Recommendation 7

Management's Comments

Management stated that the LMAS process for reviewing and accepting deliverables goes far beyond SBA's SDM requirements. However, SBA will continue to review the LMAS *Deliverable Management Process* and incorporate changes to further improve this process.

OIG Response

SBA's *Enterprise Quality Assurance Plan* requires the OCIO Quality Manager and Project Manager to jointly plan and oversee key deliverables, and establishes a vehicle for the OCIO to ensure enterprise standards are maintained in critical project control areas, such as IBRs, security reviews and testing. However, currently the LMAS Project Manager has sole discretion to approve contract deliverables, and the OCIO has not ensured a QA plan that conforms to the *Enterprise Quality Assurance Plan* has been developed and implemented. Therefore, management's response has not adequately addressed the recommendation.

ACTIONS REQUIRED

Because your comments did not fully address Recommendations 1, 2, 3, 5, and 7, we request that you provide a written response by August 14, 2009, providing proposed actions and target dates for implementing the recommendations.

We appreciate the courtesies and cooperation of the OCIO and LMAS project staff during this audit. If you have any questions concerning this report, please call me at (202) 205-[FOIA ex. 2] or Jeffrey Brindle, Director, Information Technology & Financial Management Group, at (202) 205-[FOIA ex. 2].

---

[11] Recommendation No. 4; OIG Report No. 08-13, *Planning for the Loan Management and Accounting System Modernization and Development Effort*, May 14, 2008.

APPENDIX I.

RESPONSE TO THE OIG REVIEW OF ALLEGATIONS CONCERNING HOW THE LOAN MANAGEMENT AND ACCOUNTING SYSTEM (LMAS) MODERNIZATION PROJECT IS BEING MANAGED

Project No. 8012

Date: July 20, 2009

To: Debra S. Ritt
Assistant Inspector General for Auditing

From: Eric R. Zarnikow
Associate Administrator for Capital Access [FOIA ex. 6]

Christine H. Rider
Chief Information Officer [FOIA ex. 6] - Acting CIO

Deepak Bhargava [FOIA ex. 6]
Director, Office of Financial Systems (OFS) & LMAS

Subject: Response to the Draft Report on the Review of Allegations Concerning How the Loan Management and Accounting System (LMAS) Modernization Project is Being Managed (Project No. 8012)

This is a response to the draft audit report that was issued to management to obtain comments and a statement of actions to be taken. We request these comments be considered prior to the distribution of the Office of Inspector General's (OIG's) final report. Our comments address the OIG draft audit report's results and recommendations.

The draft audit contains seven recommendations, four for the Program Sponsor and three for the Chief Information Officer (CIO). We did note that one of the significant areas of concern addressed as part of the audit was a concern that issues identified by the Quality Assurance/Verification and Validation contractor were not being reported to senior management. We were pleased to see that there was no evidence found as part of the audit that issues were being withheld from senior management.

To set a context to our comments, the Governance structure of the LMAS program includes the following players:

- Program Sponsor: the Associate Administrator for Capital Access
- Steering Council: the senior level functional leadership for loans and financial management as well as IT, contract, and administrative support.
- Program Manager: the Director, Office of Financial Systems, Office of the Chief Financial Officer (OCFO)
- Project Managers: the development team leads for each of the three task orders and sub-task functions

Response to the Recommendations: The following are the responses to the seven recommendations in the draft audit report:

Recommendation 1: Take steps to modify the contract to require the Quality Assurance/ Verification & Validation (QA/V&V) contractor to report all findings and recommendations to the Program Manager *and* an independent QA manager designated by the CIO.

> **Response:** The SBA has directed the QA contractor to provide all QA Reports (findings and recommendations) simultaneously to the Program Manager and to the CIO (Acting enterprise-level Quality Assurance Manager). This was discussed in a meeting on June 26, 2009 and follow up email on July 1, 2009, which was also sent to the QA team, the CIO, the COTR and the CO. These actions resulted in the desired outcome.

Recommendation 2: Establish a process for reviewing and accepting LMAS deliverables that complies with SDM requirements.

> **Response:** The LMAS process for reviewing and accepting deliverables goes far beyond the Systems Development Methodology (SDM) requirements. The LMAS team has created a well-defined deliverable review and approval process that exceeds the Agency's goals as stated in the SDM. However, the LMAS team will continue to review the suggestions documented in the Enterprise Quality Assurance Plan, evaluate the benefits and adopt the suggestions that will further improve the program's deliverable management process.

Recommendation 3: Ensure contractor employees work on LMAS only after their SBA Form 1228 Computer Access Clearance/Security Form have been signed and ensure they receive computer security awareness training as required.

> **Response:** The LMAS team will continue to ensure that the contractor employees who need access to the SBA's systems, sensitive data, and/or work at SBA office space are granted access ONLY after their SBA Form 1228 Computer Access Clearance/Security Form has been signed. LMAS team will also ensure that these contractor employees complete the Security Awareness training as per the requirements. However, considering the cost of clearing contract employees, i.e., approximately $600/individual, SBA will not make this a requirement for the contractor employees who are working offsite on short-term (3-6 months) assignments and do not need access to SBA's systems or sensitive data.

Recommendation 4: Consider revising the Risk Register to include all fields identified in the LMAS Risk Management Plan and complete all missing information in the risk register such as due dates, mitigation plans and risk owners.

> **Response:** LMAS team has published a detailed Risk Management Plan that contains the same fields as those in the Risk Register. SBA believes the recommendation to complete all missing information in the Risk Register is not cost effective or reasonable and is not based on fixing any perceived gap in the LMAS management. Furthermore, OMB guidance does not state that all the fields in the risk register must be populated. Rather, fields are populated as part of the Risk Management process. At any given point of time,

the Risk Register will have risks that do not have all of the fields populated. The project team will not have all the required information or answers when the risk is first identified. Creating a risk and populating what is known, however, remains a critical component of the LMAS risk management process. In addition, The Project Management Institute's (PMI) "A Guide to the Project Management Book of Knowledge" (PMBOK) does not require that all risks be actively managed. It states, "Sometimes, risks with obviously low ratings of probability and impact will not be rated, but will be included on a watch list for future monitoring."

The LMAS team uses the risk register as the watch list for lower priority risks. Not actively managing lower priority risks does not imply an oversight because this process ensures that high priority risks get the appropriate attention. Practically, the project team cannot manage thousands of risks, so we have created a process to manage the high priority risks and to document all risks for future monitoring.

Recommendation 5: Designate a Quality Assurance Manager for the LMAS project to ensure that the project-level QA function is independent from the project.

Response: The CIO will designate a high-level Quality Assurance Manager to fulfill this independent review. In the meantime, the CIO has taken on the role of providing oversight of LMAS from an enterprise-level QA standpoint.

Recommendation 6: Immediately establish an enterprise-wide Quality Assurance function that is compliant with SBA's SDM QA policy.

Response: The CIO has drafted an Enterprise Quality Assurance framework as well as staffing requirements to fulfill this function. These plans are currently under review and expected to be finalized, with identified resources from existing in-house personnel (and additional contract support if deemed necessary, contingent upon funds availability) – by October 30, 2009.

SBA's plan is for this enterprise-wide QA function to oversee all IT investments, and not just LMAS.

Recommendation 7: Take steps to ensure that a well-defined deliverable acceptance process is established for the LMAS project in accordance with SBA's *Enterprise QA Plan*.

Response: The LMAS process for reviewing and accepting deliverables goes far beyond SBA's SDM requirements. However, SBA will continue to review the LMAS Deliverable Management Process and incorporate changes to further improve this process.

Response to the Results:

1. **The Project-Level QA Function for LMAS Was Not Independent from Project Management.**

   Response: Quality Assurance should be independent from individual project management but not overall management exercise by the Program Manager. One of the roles of the Program Manager is to ensure the quality of the products and services provided and ensure the contractor follows published plans, standards, and procedures for each project. Therefore, it was always the intent of the Program Manager to have the QA contractor report directly to him to offer quality assurance advice and analytics on the delivery of products and services on the individual projects managed by project managers. This does not obviate the independent quality assurance capability of the SBA (residing in OCIO) or the quality assurance in SRA's oversight function of its own staff.

   The structure of the LMAS project team ensures that the QA function is independent from the SBA Project Managers for each project. Specifically, the Program Manager assigned three different task orders to two different SBA Project Managers – Task 1 to the Deputy Director, OFS; and Tasks 2 & 3 to the LMAS Project Manager. QA reports to the Director, OFS and LMAS Program Manager, not to the SBA Project Manager for any given task order. The Program Manager also designated a COTR for the QA contract and required the QA contractor to provide all the findings to the Program Manager, the COTR, OCIO, and the SBA Project Managers. This structure is in place to ensure QA remains independent from the SBA Project Managers on any given LMAS project. The QA team reviews and audits the deliverables submitted by other contractors. The QA team reports its findings to the LMAS Program Manager, independent of the SBA Project Managers and the contractors. These findings are also posted on LMAS SharePoint site.

   Thus, there are sufficient checks and balances with respect to the QA. The SBA intends to have a project level Quality Manager and Enterprise level SBA Quality Manager. Once these positions are designated / hired, the findings will also be reported to them.

   In the meantime, the LMAS Program Manager has directed the QA contractor to provide all QA Reports (findings and recommendations) simultaneously to the Program Manager and to the CIO (Acting enterprise-level Quality Assurance Manager).

2. **A Well-Defined Process for Accepting Contract Deliverables Had Not Been Established.**

   Response: The auditors believe LMAS is not following a well-defined process for accepting contract deliverables, because the listing of documents to be reviewed, type of review to be performed, review team responsible for the review and a method of review – as ***suggested*** by Enterprise Quality Assurance Plan - were not documented in advance. The OIG report does not take into consideration the document review and approval process the LMAS team has already created and implemented. Further, this report result, even if based on an SDM requirement rather than an SDM *suggestion*, seems insignificant when considering all the processes, documentation, tracking, artifacts, and controls that have already been implemented by the LMAS team.

SDM doesn't have a process for reviewing and accepting the deliverables (deliverable management process). SDM offers a high level review and audit process under the Enterprise Quality Assurance Plan that is different from a deliverable review and acceptance process that requires specific processes and templates for deliverable submission, feedback communication, deliverable acceptance, deliverable rejection, and deliverable tracking. The LMAS team has created and put into place a well defined deliverable review and approval process that goes far beyond the high level suggestions in the Agency's SDM and meets the deliverable management needs.

For example, Section 5.1 of the Enterprise Quality Assurance Plan (EQAP) states that "The QA process ensures that each document has undergone quality control checks relative to technical contents, is reviewed to ascertain compliance with the standards published in the SDM, and that corrective actions were executed." The process that is in place for LMAS is meeting this SDM suggestion. The LMAS team has established the deliverable management process that requires review of deliverables by functional and technical experts. The LMAS team is reviewing deliverables with the key users and technical experts. In most cases, the reviewers include selected functional and technical experts from OCIO, OCA, ODA, and OCFO depending on the type of deliverable. Feedback is requested, documented, communicated, and deliverables are modified, and ultimately accepted or rejected.

LMAS utilizes templates for receiving and commenting on deliverables, providing feedback to vendors, accepting or rejecting deliverables. These templates exceed the suggested framework in SDM. The creation and use of these templates by the LMAS team has greatly increased the efficiency and consistency of the deliverable review process.

User and technical feedback is collected, compiled, and shared with the vendors. The vendors perform modifications to the deliverables based on the feedback and resubmit for formal acceptance. The LMAS team formally accepts or rejects each deliverable. The process is tracked using an online tracking log that includes dates and status information for each deliverable. The tracking offers a great deal of transparency, and goes far beyond what is suggested in the SDM. Nevertheless, the LMAS team will continue to review the suggestions documented in the Enterprise Quality Assurance Plan, evaluate the benefits, and adopt the suggestions that will further improve its deliverable management process.

3. **Contractor Deliverables Were Behind Schedule.**

Response: SBA issued Firm Fixed Price (FFP) task orders to the Solution Provider with clearly identified target completion dates.

As per the task order's schedule, the target completion date for Task Order 2 (verify the flexibility of the Oracle solution using proof of concept) and Task Order 3 (develop Blueprint and detailed implementation plan) is August 31, 2009. However, the solution provider proposed an aggressive timeline for SBA to verify the flexibility of the solution by April 30, 2009. SBA verified the flexibility of the solution as part of the Conference Room Pilots (CRPs) conducted between April 20, 2009 and April 24, 2009. This task was completed ahead of the task order completion date of August 31, 2009.

SBA's hosting contract for Oracle Federal Financials was to expire on March 31, 2009. As part of the Task Order 1 (hosting and managing Oracle Federal Financials), the solution provider agreed to work with SBA to meet this target date. The solution provider developed the project plan to meet this aggressive timeline but did not consider the time it takes to complete the security background checks for its employees, a pre-requisite for starting work on this task order. SBA could not allow the solution provider to connect its data center with SBA's network or give access to the sensitive data until the contract staff was cleared.

The solution provider also experienced hardware failures that contributed to deliverable delays on Task Order 1. *As Task Order 1 was experiencing delays, SBA recognized the delays and worked with SRA to take corrective action.* As a result, SRA assigned a new Task Lead for the project for managing project plans and coordinating activities and assigned the existing Task Lead to complete the technical tasks. This addition of a resource was a major improvement that ultimately resulted in the completion of Task 1.

On March 24, 2009, the LMAS team conducted a detailed Production Readiness Review as a quality check prior to transition (risk management) to determine the readiness of the Oracle Federal Financials environment at the new hosting facility. Instead of merely accepting a hosting environment that was not ready for production and accepting moderate risk just to meet a published schedule, the team used the results of the Production Readiness Review to delay the transition by three weeks. SBA executed its risk mitigation plan and awarded the bridge contract to the incumbent and avoided interruption in service. The transition was completed on April 20, 2009, three weeks after the target date.

One part of the OIG report includes the need to conduct the Integrated Baseline Reviews sooner in the project lifecycle. The LMAS team agrees and has instituted a requirement to include an early-cycle IBR for future task orders. The LMAS team has developed a detailed IBR Guidance, which was provided to the solution provider.

4. Contractor Employees Attended Meetings without Required Security Vetting.

Response: The contractors who were working on LMAS projects prior to completing the background investigation were working offsite and were NOT given access to SBA's systems or sensitive information. These contractors were performing roles such as configuring Oracle Loans in the solution provider's development environment and reviewing publicly available information on SBA's loan programs and demonstrating their solution. They attended the meetings to verify publicly available information about SBA's loan programs and demonstrate the flexibility of the Oracle COTS Solution.

LMAS team ensures that contractor employees only receive access to SBA's systems or sensitive data after their SBA Form 1228 Computer Access Clearance/Security Form has been signed. The LMAS team also provides contractors with Security Awareness training CDs and maintains a tracking log of the contractors who have completed the training. A portion of the Task 1 (that required implementing the infrastructure at SAVVIS facility without connecting to SBA's network) and Task 2 & 3 didn't require access to SBA's systems or sensitive data. Task 2 was performed in solution provider's environment with test data created by the vendor for demonstration purposes only.

The OIG's draft audit states that SBA's Procedural Notice 9000-1684 (effective 6/4/2007) requires that contractors must receive a favorable preliminary background investigation prior to "entering on duty." This is not true. The Procedural Notice 9000-1684 states that the SBA can not permit access to SBA's networks until after receipt of the signed SBA Form 1228. The attachment to this notice also states, "COTR submits '1228' to Office of Information Security (OIS) for signature if contractor is located in SBA HQ; If COTR and contractor are located in an SBA field office, COTR will send '1228' directly to Office of Security Operations (OSO)" Likewise, the LMAS Blanket Purchase Agreement (BPA) with SRA states that "OMB Circular A-130 requires that before granting access to government Automated Information Systems (AIS) (including data), SBA must screen contractor personnel commensurate with the level of risk presented by their access to sensitive SBA AIS." Further, the Federal Acquisition Regulations (FAR) explains that "Agencies must follow FIPS PUB Number 201 and the associated OMB implementation guidance for personal identity verification for all affected contractor and subcontractor personnel when contract performance requires contractors to have routine physical access to a Federally-controlled facility and/or routine access to a Federally-controlled information system." 48 C.F.R. § 4.1301 (emphasis added).

Thus, there is no requirement for a contractor to clear a background investigation prior to working on the task order if the contractor personnel does not need access to the SBA's system or sensitive data and does not work at SBA HQ or SBA field office. In the present case, contractors without background investigations were not given such routine access to the SBA's facilities or any access to information systems. A portion of the Task 1 (that required implementing the infrastructure at SAVVIS facility without connecting to SBA's network) and Task 2 & 3 did not require access to SBA's systems or sensitive data. Task 2 was performed in the solution provider's environment with test data created by the vendor for demonstration purposes only.

The LMAS team has complied with the BPA, FAR, and SBA Procedural Notice and will continue to comply by ensuring that contractor employees only receive access to SBA's systems or sensitive data after their SBA Form 1228 Computer Access Clearance/Security Form has been signed. The LMAS team also provides contractors with Security Awareness training CDs and maintains a tracking log of the contractors who have completed the training.

Further, considering the cost to clear contractor staff (approximately $600/individual), SBA will not make this a requirement for the contractor employees who are working offsite on short-term assignments and do not need access to SBA's systems or sensitive data since such background investigations are not required for those personnel.

5. Risk Tracking Process Was Not Sufficiently Developed.

Response: The Project Management Institute's "A Guide to the Project Management Book of Knowledge" (PMBOK) states, "Sometimes, risks with obviously low ratings of probability and impact will not be rated, but will be included on a watch list for future monitoring." The LMAS team uses the risk register as the watch list for lower priority risks. PMBOK does not require the active management of lower priority risks; rather, it

recommends a process to ensure that highest priority risks get the appropriate attention. Practically, the project team can not manage thousands of risks, so we have created a process to manage the high priority risks and to document all risks for future monitoring.

The LMAS risk management process has a documented Risk Management Plan, and incorporates the Risk Register, a risk working team, and a risk management team. The fields in the Risk Register match the fields in the LMAS Risk Management Plan. Risks are created, reviewed, prioritized, updated, managed, and when appropriate closed and/or upgraded to issues. Risks are communicated via the online Risk Register, bi-weekly risk meetings, and also in written status reports.

Although the Risk Management Plan contains the same fields as those in the Risk Register, SBA believes the recommendation to complete all missing information in the Risk Register is not cost effective or reasonable and is not based on fixing any perceived gap in the LMAS management. Furthermore, OMB guidance does not state that as soon as a risk is identified, all the fields in the risk register must be populated. Rather, fields are populated for the high priority risks only as part of the Risk Management process. At any given point of time, the Risk Register will have risks that do not have all of the fields populated because Risk Management is a process and the project team will not have all the required information or answers when the risk is first identified. Creating a risk and populating what is known, however, remains a critical component of the LMAS risk management process. In addition, as noted above, PMBOK does not require active management of lower priority risks.

The risk management process for LMAS went through significant changes and improvements in the first few weeks/months after SRA initiated the work on task orders. The Risk Management Plan was revised and the risks in the Risk Register were updated. The consolidated Risk Register was created to merge the risk lists prepared by the solution provider (SRA) and SBA. A working group and a review committee were established. Risks were prioritized and grouped by task order. Also, an online SharePoint list was created to maintain the Risk Register. The LMAS team has created views and reports to facilitate analysis.

The project team is encouraged to document risks, even if all of the information associated with a particular risk is unknown. LMAS instituted a proactive risk process to ensure risks are openly communicated as they are being researched, verified, assigned, and mitigated. The users of the LMAS Risk Register should not expect every field to be populated for every risk. It is possible to document a risk, but not immediately have a contingency plan, mitigation plan, or even a risk owner. Additionally, the risks are addressed in order of priority so the risks that have the highest probability and impact get addressed first. There may be lower priority risks that are not fully addressed but they are documented in the LMAS Risk Register for monitoring. This is a mature process that allows for real time risk sharing and risk mitigation strategy development.

Thank you for the opportunity to provide comments on the draft audit report.

CC: Ana Ma, Chief of Staff
James Rivera, Acting Associate Administrator for Disaster Assistance
Jonathan Carver, Acting Chief Financial Officer
James VanWert, Senior Advisor for Policy and Planning
Robert B. Naylor, Consultant to the Administrator