ENFORCEMENT OF SBA'S INFORMATION TECHNOLOGY ENTERPRISE ARCHITECTURE DURING THE DEVELOPMENT OF THE DISASTER CREDIT MANAGEMENT SYSTEM

AUDIT REPORT NUMBER 4-14

MARCH 2, 2004

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

AUDIT REPORT
Issue Date: March 2, 2004
Number: 4-14

To: Stephen D. Galvan
Chief Information Officer

/s/ Original signed
From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Enforcement of SBA's Information Technology Enterprise Architecture during the Development of the Disaster Credit Management System

SBA's Office of Disaster Assistance (ODA) desires to improve the delivery of its disaster loan origination and servicing activities through the Disaster Credit Management System (DCMS) initiative. The Office of Inspector General is monitoring the DCMS project to ensure that the system developed and implemented will meet SBA standards for security, integrity, availability and also meet SBA's system development methodology guidelines. This is our second report in a series of reports and it presents issues regarding SBA's Information Technology-Enterprise Architecture (IT-EA) enforcement that have been identified since our review started in May 2003. SBA's attention is needed to address actual enforcement of the IT-EA during the systems development process.

BACKGROUND

ODA is the primary provider of low interest, long term loans to renters, homeowners, nonprofit organizations, and businesses of all sizes to rebuild after a disaster. The performance of ODA is vital to SBA's strategic goal of helping businesses and families recover from disasters. Currently, ODA operates the Automated Loan Control System (ALCS) to process disaster loan assistance. ALCS is a distributed system which is in operation at the four Disaster Area Offices and utilizes a mix of mainframe and microcomputer capabilities. The primary impetus of DCMS is to implement a Commercial-Off-The-Shelf (COTS) solution intended to provide more features, better usability, improved reliability and maintainability, better performance, and better security than either the current ALCS system or a custom developed system. This is planned to be accomplished by purchasing an existing software package and tailoring the software to meet SBA's business rules.

SBA's IT-EA identifies SBA's mission, the information necessary to perform the mission, the technology necessary for mission support, and the processes for implementing new technologies in response to changing business needs. It establishes an organization-wide roadmap for achieving optimal performance of mission-critical business processes within an efficient information technology environment. The SBA IT-EA is also supposed to provide discipline and a controlled process for modernizing information systems, developing new systems and implementing new IT technologies that optimize system performance.

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of our audit are to determine if SBA's implementation of DCMS (1) provides adequate safeguards, controls and testing before DCMS is placed into a production status, and (2) complies with overall objectives of the SBA IT-EA. This ongoing audit identifies issues which may cause undue risk to the DCMS project as they arise. Due to the critical time frames for implementation of DCMS, it is anticipated that corrective actions will occur promptly to reduce the level of residual risk to the project. To accomplish our objectives, we reviewed SBA's DCMS project materials and interviewed SBA and contractor personnel. Fieldwork was performed at SBA's Central Office in Washington, D.C. from July through December 2003. The audit was conducted in accordance with generally accepted Government Auditing Standards.

AUDIT RESULTS

Based on our review, ODA has followed a disciplined planning process and has strong management oversight of the DCMS project. After our initial audit report was issued, ODA increased its awareness and efforts to implement security and provide systems development oversight. Additionally, the Office of the Chief Information Officer (OCIO) provided more proactive oversight of the DCMS project. We did find, however, the need for the OCIO to more adequately enforce SBA's IT-EA standards for the DCMS project.

Finding 1: SBA did not adequately enforce its Enterprise Architecture

SBA had not adequately enforced its IT-EA during the initial phase of the development of the DCMS project. This occurred because at the time the DCMS project was initiated, OCIO did not believe it had the authority within SBA to enforce SBA's IT-EA and had not formulated a strategy to enforce SBA's IT-EA during system development projects. As a result, certain aspects of DCMS, including the planning to implement a new Virtual Private Network for ODA, adoption of certain middleware capabilities to communicate between DCMS and the SBA mainframe systems, and the adoption of DCMS scanning software, were initiated without prior OCIO review and full concurrence.

Executive Order 13011 established the Chief Information Officer (CIO) and gave the CIO the visibility and management responsibilities necessary to advise the agency head on the design, development, and implementation of the Agency's information systems. CIO responsibilities include: (1) participating in the investment review process for information systems; (2) monitoring and evaluating the performance of those information systems on the

basis of applicable performance measures; and, (3) as necessary, advising the agency head to modify or terminate those systems.

SBA Information Technology Investment Manual (ITIM) in Section 6.4.1, identified as part of the investment review process for ongoing IT projects, that an In-Process Review (IPR) should be conducted. Part of the IPR is identifying that the investment continues to adhere to current/planned IT-EA standards.

SBA issued more rigorous IT-EA standards in May 2003 which require that all IT-EA planned purchases are evaluated by the IT Architecture Review Board (ITARB). However, these standards were not in effect at the beginning of the DCMS project and, therefore, would not have been in effect at the beginning of the project through May 2003.

During our initial audit fieldwork for DCMS, OCIO officials identified that ODA was not being fully forthcoming during systems development life cycle (SDLC) oversight about IT-EA software, firmware and hardware that ODA was planning on procuring for DCMS. Specifically, information not identified included: (1) a planned separate DCMS Virtual Private Network (VPN), (2) a middleware product for use in communicating between the DCMS COTS product, the SBA mainframe and the SBA client-server environment, and (3) scanning software that is being planned for adoption by ODA for DCMS. According to OCIO officials, these products were adopted without full OCIO concurrence and without consideration for SBA's IT-EA.

SBA's initial IT-EA document issued in March 2000 identified that SBA supports two Wide Area Networks (WAN). One WAN was for general and administrative operations and the other WAN was for disaster operations. At that time, the document identified that economies may be realized in a reevaluation of WAN architecture.

According to ODA officials:

- The planned VPN was only a plan put forth by ODA's contract developer. The VPN needed to be approved by OCIO and the VPN was put on hold for three weeks while an agreement was reached between OCIO and ODA.
- The middleware was approved by the CIO in a proof of concept earlier in 2003.
- The planned scanning software has not been approved by OCIO as it would only be utilized by ODA for the DCMS system at this time.

We informed both ODA and OCIO that an IPR had not been performed on the DCMS which at the time between project initiation of September 1999 and May 2003 was the only requirement for IT-EA compliance issued by OCIO.

We also stressed to ODA that when developing a system, the developing office must include OCIO on three levels: (1) OCIO Security to certify the security of the planned system, (2) OCIO SDLC to oversee and approve the development process, and (3) the OCIO Enterprise Architect to ensure and validate that IT-EA issues are fully reviewed and approved by the ITARB. We are making no recommendations to ODA at this time due to ODA becoming more cognizant of IT-EA issues during our audit.

Recommendation:

We recommend that the Chief Information Officer:

1A. Perform "In-Process Reviews" for large-scale system development projects as part of the investment review process to ensure that IT Enterprise Architecture standards are enforced.

1B. Formulate and publish a strategy to provide for more proactive oversight of development projects from an IT Enterprise Architecture perspective.

Management Response:

The CIO agreed with both recommendations and stated that OCIO would perform "In-Process Reviews" as part of the Business Technology Investment Council process at the end of the first (DCMS) build cycle. Additionally, OCIO is committed to "getting to green" in strengthening its (IT EA) oversight responsibilities. Further, OCIO published policy notice 9000-1450 titled "Implementation of SBA EA Program Policies" on August 1, 2003. The Chief Information Officer's entire response less attachments is included as Attachment 1 to our report.

Assessment of Management Response:

SBA Management's comments are responsive to the recommendations.

* * *

The findings included in this report are the conclusions of the Auditing Division based upon the auditors' review of planning and project documents from the Disaster Credit Management System related materials. The findings and recommendations are subject to review and implementation of corrective action by your office following the existing Agency procedures for audit follow-up and resolution.

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

Should you or your staff have any questions, please contact Robert G. Hultberg, Director, Business Development Programs Group at (202) 205-7577.

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

ATTACHMENT 1

February 25, 2004

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Stephan D. Galvan [FOIA Ex. 6]
Chief Information Officer

Subject: Response to IG report, enforcement of SBA's EA during the development of the Disaster Credit Management System

OCIO is responding to your memo dated January 28, 2004, entitled "Enforcement of the SBA's Information Technology Enterprise Architecture (EA) during the development of the Disaster Credit Management System." Specifically, OCIO agrees with the two OIG recommendations contained in the draft audit report.

Formulate and publish a strategy to provide for more proactive oversight of development projects from an IT Enterprise Architect perspective.

Response: OCIO has published policy notice 9000-1450 titled "Implementation of SBA EA Program Policies," which was promulgated August 1, 2003. This policy notice refers to the "SBA Enterprise Architecture Program Policies and Procedures" and can be found at the following intranet site: http://ves.sba.gov/ocio/arch.html.

As stewards of the EA process, OCIO performs part of its oversight responsibility as defined in section 5.2.2, "Investment Performance Oversight - CONTROL PHASE". This section discusses the EA, Business Technology Investment Council process, and Program Office Investment Board roles in implementing project "m-Progress Reviews."

Finally, OCIO is attaching for OIG review its plan to ensure more effective oversight called "Plan for Improved Oversight of Office of Disaster Assistance's DCMS Project."

Perform "In-Progress Reviews" for large-scale system development projects as a part of the investment review process to ensure that IT Enterprise Architecture standards are enforced.

Response: As specified in its published policy and standards and implied in the "getting to green" actions, OCIO is committed to strengthening its oversight responsibilities; For example, OCIO participates in weekly conference calls with the Disaster Office staffs to discuss the status of the project and ensure that they are enforcing IT EA standards. We are also planning to participate in the 1st product review at the end of the current build cycle.

ATTACHMENT 2

REPORT DISTRIBUTION

Recipient	No. of Copies
General Counsel	3
General Accounting Office	1
Associate Administrator for Disaster Assistance	1
Office of the Chief Financial Officer Attention: Jeffrey Brown	1