



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

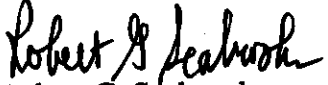
AUDIT REPORT

Issue Date: September 24, 2003

Number: 3-39

To: Herbert L. Mitchell
Associate Administrator for Disaster Assistance

Stephen D. Galvan
Chief Information Officer

From: 
Robert G. Seabrooks
Assistant Inspector General for Audit

Subject: Monitoring of SBA's Implementation 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 report presents issues that have been identified since our review started in May 2003. SBA's immediate attention is needed to address weaknesses in security planning and security requirements documentation. Additionally, SBA needs to plan to perform an Independent Verification and Validation review and schedule a Certification and Accreditation of the system before it is placed into a production status.

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 will be accomplished by purchasing an existing software package and tailoring the software to meet SBA's business rules.

DCMS will introduce paperless loan application, virtual loan processing, access to outside data sources, improved workflow and improved document preparation. Currently, SBA is in the "blueprinting" phase of the system development. During this phase, the level of fit between the business requirements and standard application functionality is assessed, gaps are identified and corresponding solutions are developed. The contractor has already demonstrated the concept of operations in a conference room pilot.

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of our audit are to monitor SBA's implementation of DCMS to ensure that SBA (1) provides adequate safeguards, controls and testing before DCMS is placed into a production status, and (2) complies with overall objectives of the SBA Systems Development Manual (SDM). Our audit is intended to identify 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 May through July 2003. The audit was conducted in accordance with Government Auditing Standards.

AUDIT RESULTS

Based on our initial review, ODA has followed a disciplined planning process and has strong management oversight over the project. We did find, however, the need for improvement in security planning, quality assurance and certification and accreditation planning. Additionally, the Office of Chief Information Officer (OCIO) needs to provide more disciplined oversight of the DCMS project to ensure that it meets SBA's requirements for a system under development.

Finding 1: SBA did not Conduct a Risk Analysis for System Security

SBA has not conducted a security risk analysis for the DCMS project. This occurred because OCIO was not fully engaged in project oversight to identify this potential vulnerability. As a result, development has proceeded without an understanding of the vulnerabilities, baseline security requirements and security specifications, and safeguards needed to mitigate potential system risk.

SBA's SDM Section 1.5 requires that a risk assessment for system security be performed at project initiation. At the initial project phase, needs are defined, a project plan is developed, system category is determined, feasibility is assessed, benefit/cost analysis is performed, and a security risk analysis is performed.

SBA is currently in the "blueprint" phase of the contractor's Enterprise Lifecycle Information Technology Engineering (ELITE) methodology. ELITE is a hybrid methodology that combines the contractor's in house procedures with Oracle Corporation's Application Implementation Methodology (AIM). The methodology consists of five phases; planning, blueprint, realization, transition and production.

SBA's SDM has six phases:

- Initiate project,
- Define system,
- Design system,
- Build system,
- Evaluate system, and
- Operate system.

The blueprint phase of the ELITE methodology corresponds approximately to somewhere in between Define system and Design system in SBA's methodology, thus, a security risk assessment should already have been performed.

Recommendation:

- 1A. We recommend that the Associate Administrator for Disaster Assistance (AA/DA), in conjunction with the OCIO, immediately conduct a security risk assessment for the DCMS project.

Management Response:

The AA/DA and the CIO agreed with the recommendation and stated that ODA and OCIO will work together to perform a security risk assessment. They noted that a risk assessment would not have been possible prior to the selection of a COTS solution. Their joint response is included in its entirety less attachments as Attachment 1.

Assessment of Management Response:

SBA Management's comments are responsive to the recommendation. The OIG audit recommendation was made after the COTS package was selected and being developed.

Finding 2: SBA Has Not Fully Determined DCMS Security Requirements

Security requirements for DCMS have not been fully determined. This occurred because OCIO has not been fully involved in project oversight and system planning. As a result, the system is in early development stages without determining unique security requirements. It may prove difficult in later stages to retrofit the system to conform to established security requirements.

SBA's SDM Section 1.6.2 requires that security requirements be established in the initiate project phase of development. SBA has moved forward with system development and is well beyond the initiate project phase of development.

Recommendation:

- 2A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with OCIO identify and fully document DCMS security requirements.

Management Response:

The AA/DA and CIO did not concur with the recommendation. SBA Management stated that they documented security requirements as part of the solicitation for a COTS solution. These requirements are found in the DCMS Security Requirements document dated May 2002 that was attached to SBA Management response, as well as the DCMS task order that specifies all such requirements. Finally, ODA has delivered to OCIO a draft Security Plan which is awaiting OCIO's response.

Assessment of Management Response:

SBA Management's comments are not responsive to the recommendation. We examined the document provided by SBA and found that it was not a stand-alone security requirements document. It was the results of a key-word search of the Revalidated Statement of Need and Functional Requirements document dated June 2002. This document contained a one-paragraph section on security with three bullets and 11 requirements from the document's requirements matrix.

We note that the one-paragraph section on security was very general and lacked depth, while the 11 requirements from the matrix were mostly co-incidental or peripheral to security. The section on security and 10 of the 11 requirements were identical to those on an earlier requirements document dated August 2000. In two years, only one requirement was added; to log user changes or deletions of records. This requirement was not considered mandatory, only desirable.

The results of SBA's key word search indicate that no requirements exist regarding access controls, privacy or encryption of electronically transmitted data. Additionally, we found no evidence of security requirements regarding system and data integrity, reliability of service or physical security. This is especially troublesome as SBA has selected core COTS products without adequate security requirements to aid in making the decision beforehand. Therefore, SBA may have to retrofit the COTS package to ensure that it meets SBA's baseline security requirements.

Finding 3: SBA has not Established a Security Plan for DCMS

SBA has not yet prepared a system security plan for DCMS. This occurred because OCIO did not fully participate in project oversight and system planning. Without a security plan, SBA is not in a position to implement cost-efficient safeguards to minimize risk to the potential application.

SBA's SDM Section 2.4 requires that a system security plan be prepared as part of the define system phase of development.

SBA has already acquired COTS software for the project and is actively developing that software. Therefore, SBA may have to either retrofit security into the project or buy other COTS software which can be successfully retrofitted with adequate security once security plan requirements and safeguards are known.

Recommendation:

- 3A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, immediately prepare a system security plan for the DCMS project.

Management Response:

The AA/DA and CIO concurred with the recommendation and noted that the plan was delivered to OCIO in August 2003. They noted that the development of the plan followed the decision to implement a specific software product as the DCMS core component. Developing a plan prior to product selection would have been inappropriate due to the lack of detailed information available before that time. According to ODA, the plan was delivered in the design and build phase and included an in depth evaluation of the COTS product and other key components.

Assessment of Management Response:

SBA Management's comments are responsive to the recommendation. OIG notes that SBA's SDM requires that a System Security plan be prepared at the define system phase and refined during the subsequent phases.

Finding 4: SBA does not plan to conduct an Independent Verification and Validation of the DCMS before Implementation

At present, SBA does not plan to conduct an Independent Verification & Validation (IV&V) of DCMS system requirements and performance capabilities before implementation. ODA management believes that having an independent contractor perform project oversight is an adequate substitute for not performing an IV&V. Without an IV&V, it is possible for the software to deviate from its planned requirements without management's knowledge and for the system to not perform as anticipated.

SBA's SDM Section 3.6 requires an independent Quality Assurance team to perform independent verification and validation of test results.

SBA currently has plans for testing and quality assurance. The contractor will perform testing at all stages of the project, some of which will be witnessed by SBA. Additionally, SBA plans to implement a pilot of the system rather than a full-scale implementation.

SBA's OCIO recently advised the Office of Inspector General that in the future all large-scale development projects will undergo an IV&V before implementation. We believe that ODA and the OCIO should work together to identify how an IV&V should be formulated and included into the DCMS project.

Recommendation:

- 4A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, fully incorporate an appropriate IV&V as a part of the DCMS schedule for DCMS system implementation.

Management Response:

The AA/DA and CIO concurred in part with the finding and recommendation. They agreed that IV&V testing is appropriate, but disagreed that ODA had not planned to do it. The AA/DA and CIO believe that the relationship and contract with Data Networks Corporation (DNC) is a mechanism equivalent to an IV&V. DNC's participation in system planning, development and (future) user testing provides an independent view of the system capabilities. Additionally, IV&V tasking was placed in the scope of the initial agreement with DNC.

Assessment of Management Response:

SBA Management's response is not fully responsive to the recommendation. They agreed with the need for IV&V, but believe that its contract with DNC fulfills this need. We disagree. The initial agreement with DNC provided as evidence lists IV&V only as a potential task for DNC. No concrete evidence that DNC will perform an IV&V was provided. Additionally DNC may not meet NIST conditions for technical, managerial and financial independence in performing an IV&V.

Finding 5: SBA has not Planned a Certification and Accreditation Review of DCMS

SBA has not planned a Certification and Accreditation (C&A) review of DCMS prior to system implementation. This occurred because OCIO has not been fully involved in project oversight and system planning. As a result, the system implementation may be delayed due to lack of C&A or the C&A may be done hastily or superficially.

OMB Circular A-130, Management of Federal Information Resources, requires that Senior Management authorize processing prior to implementing a new system. The authorization (accreditation) is based on the results of the certification review.

Recommendation:

- 5A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, plan for a C&A review of DCMS before the system is implemented.

Management Response:

SBA Management concurred in part with the finding and recommendation. They agreed that a C&A review is necessary but disagreed that ODA had not planned a C&A review of DCMS. ODA has detailed schedule plans from the contractor, which includes an OCIO C&A review in connection with user validation testing, set for December 1, 2003. A C&A kickoff meeting was conducted on June 26, 2003 and an initial data collection form was completed and delivered to OCIO security on July 10, 2003. OCIO considers five months time in scheduling a C&A review to be adequate to meet SDM and IT security requirements.

Assessment of Management Response:

SBA Management's comments are partially responsive to the recommendation. The DCMS Schedule –Work Breakdown Structure and Deliverables document dated March 2003 did not have a proposed C&A in its schedule. Additionally, during a meeting with us on June 18, 2003, ODA management acknowledged that there was no C&A scheduled for DCMS at that time. ODA management has since scheduled a C&A review.

Finding 6: SBA OCIO has not Provided Adequate Oversight of the DCMS Project

OCIO was not adequately involved in the DCMS project. This occurred because there was confusion between the Applications Development group and the Security group as to their required level of oversight and their responsibilities for ensuring that the system being developed by ODA meets the SBA Systems Development Manual. As a result, the DCMS may not meet SBA application development and security requirements. Additionally, the system may not make its planned implementation date since security may have to be retro-fitted into the project.

The Federal Information Security Management Act (FISMA) requires that the CIO ensure that information security is addressed throughout the life cycle of each agency information system.

The DCMS project is in a development stage of its system life cycle. Although a different office is developing the project, the CIO has responsibility to ensure that security items such as risk analysis, security requirements, and system security plan are incorporated into the project. OCIO Security did not become involved in the DCMS project until March 2003 and did not start reviewing project deliverables until July 2003.

Recommendation:

- 6A. We recommend that the Chief Information Officer formulate a strategy to provide for more proactive project oversight and system planning efforts to ensure that the SDM is followed by SBA sponsoring offices for large-scale systems development projects.

Management Response:

SBA Management concurred with the recommendation and stated that they will be more proactive on project oversight in the future.

Assessment of Management Response:

SBA Management's comments are responsive to the recommendation. OCIO has subsequently provided us with a plan for improved oversight of ODA's DCMS project.

* * *

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.

Please provide us your management decision for each recommendation within 30 days. Your management decisions should be recorded on the attached SBA Forms 1824, Recommendation Action Sheet," and show either your proposed corrective action and target date for completion, or explanation of your disagreement with our recommendations.

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

Attachments

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, D.C. 20416

August 25, 2003

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Cheri L. Cannon *Cheri L. Cannon*
Acting Associate Administrator for Disaster Assistance
Office of Disaster Assistance

Stephen D. Galvan *Stephen D. Galvan*
Chief Information Officer
Office of the Chief Information Officer

Subject: Response to OIG Draft Audit Report, "Monitoring of SBA's
Implementation of the Disaster Credit Management System"

This constitutes the joint response of the Office of Disaster Assistance (ODA) and the Office of the Chief Information Officer (OCIO) to the Office of Inspector General's (OIG) draft audit report on the subject of monitoring the implementation of the Disaster Credit Management System (DCMS). We believe that ODA has followed a disciplined planning process in the implementation of the DCMS and believe that ODA has strong management controls and oversight over the project. Nonetheless, both offices believe better cooperation and oversight in the future is key to the success of the DCMS project. Our response to each finding and recommendation follows below.

OIG Finding 1: SBA did not Conduct a Risk Analysis for System Security

In finding number 1, OIG states that SBA has not conducted a security risk analysis for the DCMS project. This occurred, OIG believes, because OCIO was not fully engaged in project oversight to identify this potential vulnerability.

OIG Recommendation:

- 1A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, immediately conduct a security risk assessment for the DCMS project.

Response to 1A:

We concur. ODA and OCIO will work together in conducting a security risk assessment for the DCMS project. We note, however, that pending the selection of a COTS solution, an assessment would not have been possible without details of the selected solution. We also note that ODA and OCIO have been both active and strategic partners in the deployment of DCMS since February 2002.

SBA IS AN EQUAL OPPORTUNITY EMPLOYER AND PROVIDER

OCIO will be increasing its oversight of this and other IT initiatives.

OIG Finding 2: SBA has not Determined DCMS Security Requirements

In finding number 2, OIG states that SBA has not yet determined security requirements for DCMS. This occurred, OIG believes, because OCIO has not been fully involved in project oversight and system planning.

OIG Recommendation:

- 2A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, immediately identify and fully document DCMS security requirements.

Response to 2A:

We non-concur. A fundamental requirement of the DCMS is compliance with the SBA's established security requirements. Because of this requirement ODA documented security requirements, in conformance with the SDM, as part of its solicitation for a COTS solution. These requirements can be found in DCMS Security Requirements document dated May 2002 (see attachment A), as well as the DCMS Task Order that specifies all such requirements. Finally, ODA has prepared and has delivered to OCIO a draft Security Plan and is waiting for OCIO response thereto.

ODA will continue to cooperate with OCIO on Security issues and will implement all necessary security arrangements as specified by OCIO and the DCMS Task Order.

OIG Finding 3: SBA has not Established a Security Plan for DCMS

OIG states that SBA has not yet prepared a system security plan for DCMS. OIG alleges that this occurred because OCIO did not fully participate in project oversight and system planning.

OIG Recommendation:

- 3A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, immediately prepare a system security plan for the DCMS project.

Response to 3A:

We concur. We note, however, that a "System Security Plan for DCMS" was delivered to the appropriate OCIO Security Officer on August 4, 2003. The development of the Plan since April 2003, followed immediately ODA's decision to select the SuperSolutions Corporation's Daybreak product as the DCMS core component.

Developing a Security Plan prior to the selection of SuperSolutions would have been inappropriate due to the lack of detailed information available to ODA before that time.

The plan delivered to OCIO was developed throughout the design and build phase and includes an in-depth evaluation of the COTS product and other key components.

OIG Finding 4: SBA does not plan to conduct an Independent Verification and Validation of the DCMS before Implementation

OIG states that SBA does not plan to conduct an Independent Verification & Validation (IV&V) of DCMS system requirements and performance capabilities before implementation.

OIG Recommendation:

- 4A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, incorporate an IV&V as a part of the DCMS schedule for DCMS system implementation.

Response to 4A:

We concur in part and non-concur in part. We believe that IV & V testing is appropriate for the DCMS, but disagree that ODA had not planned on it. ODA does believe it is critical to have an independent verification and validation of the functionality in DCMS to the system requirements. We believe we have the mechanisms in place to accomplish this through our existing relationship and contract with Data Networks Corporation (DNC). As well, DCMS will be rigorously tested throughout the realization and transition phases of development. The system will also undergo significant testing by ODA employees who will use it.

Most significantly, DNC has been on contract through all of the planning phase of DCMS and has participated fully in the development of the ODA system requirements. By using DNC as project support, ODA expects full participation in the user validation process. ODA has invested substantially to obtain DNC's expertise throughout the process and believes that DNC has key personnel available with precise knowledge of the requirements to augment our validation of DCMS requirements. This will thereby provide an independent view of the system's capabilities. Finally, IV & V tasking was deliberately placed in the scope of the basic agreement with DNC under which DNC task orders are issued (see attachment B).

OIG Finding 5: SBA has not Planned a Certification and Accreditation Review of DCMS

OIG states that SBA has not planned a Certification and Accreditation (C&A) review of DCMS prior to system implementation. This occurred because OCIO has not been fully involved in project oversight and system planning.

OIG Recommendation:

- 5A. We recommend that the Associate Administrator for Disaster Assistance, in conjunction with the OCIO, plan for a C&A review of DCMS before the system is implemented.

Response to 5A:

We concur in part and non-concur in part. We concur that a C & A review is necessary. We non-concur that ODA had not planned on a C&A review of this system. ODA has detailed schedule plans for the development of DCMS from its integration contractor, SRA. The schedule includes an OCIO C&A review in connection with the user validation testing, set for the week of December 1, 2003. Specifically, the DCMS project manager and the OCIO security team conducted a DCMS C&A kick-off meeting on June 26, 2003. An initial C&A data collection form was completed and delivered to OCIO security on July 10, 2003, along with numerous other documents. ODA is awaiting OCIO's evaluation of the initial data request before proceeding to the next phase of the C&A process.

OCIO considers 5 months lead time in scheduling a C&A review more than adequate to meet SDM and Agency IT security requirements.

OIG Finding 6: SBA OCIO has not Provided Adequate Oversight of the DCMS Project

OIG states that OCIO was not adequately involved in the DCMS project. This occurred, OIG alleges, because there was confusion between the Applications Development group and the Security group as to their required level of oversight and their responsibilities for ensuring that the system being developed by ODA meets the SBA Systems Development Manual.

OIG Recommendation:

- 6A. We recommend that the Chief Information Officer formulate a strategy to provide for more proactive project oversight and system planning efforts to ensure that the SDM is followed by SBA sponsoring offices for large-scale systems development projects.

Response to 6A:

We concur. OCIO will provide more proactive oversight of IT security projects.

We appreciate the opportunity to comment on the Draft Audit Report. If you have further questions, please feel free to contact Michael V. Sorrento, ODA's project manager. He can be reached at (202) 205-6734 or Howard Bolden, Agency Computer Security Manager at (202) 205-7173.

ATTACHMENT 2

REPORT DISTRIBUTION

<u>Recipient</u>	<u>No. of Copies</u>
General Counsel.....	3
General Accounting Office.....	1
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
Associate Deputy Administrator For Management and Administration	1