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

ADVISORY MEMORANDUM
Issue Date: April 27, 2006
Number: 06-21

To: Herbert L. Mitchell
Assistant Administrator,
Office of Disaster Assistance

Christine H. Liu
Chief Information Officer
Office of Chief Information Officer

/S/ Original Signed
From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: The Disaster Credit Management System Upgrade Project needs a Certification & Accreditation Prior to Production

The purpose of this memorandum is to inform SBA of the need for its Disaster Credit Management System (DCMS) Upgrade to have a Certification & Accreditation (C&A) performed prior to it being placed into production.

The DCMS allows for a paperless loan processing environment which includes disaster management, loss verification, legal functions, document management and portfolio management capabilities. The system was designed for 1,500 users. However, the 2005 Gulf Hurricanes have required SBA to process loan activity over three times larger than any previous disaster season. Through increased scaling, DCMS user capacity was increased to approximately 3,500 users in two shifts, as an interim measure to meet the demand.

The DCMS Upgrade Project was approved by the SBA Business Technology Investment Council in December 2005. The DCMS Upgrade Project was initiated because:

- The current capacity of users of the DCMS had been reached,
- The Upgrade scaling is projected to be 2.5 to 3.5 times the current capacity,
- There is a need for a reliable disaster recovery environment, and

- There is a need for a robust test environment for both fine tuning and adding upgrades to application modules, over the long-term.

The DCMS Upgrade project involves the following:

- Installing upgraded hardware for the current tiered architecture,
- Moving the production environment from Tempe, Arizona to Sterling, Virginia,
- Moving the disaster recovery environment from Sterling, Virginia to Tempe, Arizona,
- Isolating some DCMS services, e.g., loss verification onto their own production servers, from the current architecture, and
- Reconfiguring and optimizing the Oracle Data Base Management System, and related architecture.

According to the National Institute of Standards and Technology (NIST) "Guideline for Certification and Accreditation of Federal Information Systems" 800-37, Chapter 1.1 – Completing a security accreditation ensures that an information system will be operated with appropriate management review, that there is ongoing monitoring of security controls, and that reaccreditation occurs periodically in accordance with federal or agency policy and whenever there is a significant change to the system or its operational environment. Examples of significant changes to an information system that should be reviewed for possible reaccreditation include but are not limited to: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform or firmware component; or (iv) modifications to cryptographic modules or services.

We reviewed the DCMS Upgrade project plan and discussed the project with the DCMS Herndon Operations Center (OC) Director. We identified that the DCMS Upgrade Project does not include a planned C&A of the Upgrade Project. We concluded that based upon the scope of the DCMS Upgrade Project and a review of NIST 800-37, DCMS should be reevaluated under a full certification and accreditation of the system prior to it being placed in production.

Recommendations

We recommend the Assistant Administrator for Disaster Assistance in conjunction with OCIO:

1.A Complete a full reaccreditation of the DCMS Upgrade Project before it is placed into production in accordance with NIST 800-37 and SBA Standard Operating Procedure 90-47.2. Or, complete an Interim Authorization to Operate (IATO) accreditation of the DCMS Upgrade Project in accordance with NIST 800-37 and SBA Standard Operating Procedure 90-47.2. The IATO will only be in use for a limited time frame while a full scope certification and accreditation of the DCMS Upgrade Project is performed at the new production location.

Management Response:

Management generally concurred with findings and recommendations in this memorandum. Their response is provided in Attachment A and states that an Interim Accreditation will be performed on DCMS to provide authority to operate for a 4-month period.

* * *

Our review was conducted in conjunction with the President's Council on Integrity and Efficiency (PCIE) as part of its examination of relief efforts provided by the Federal government in the aftermath of Hurricane Katrina and Rita. As such, a copy of the report has been forwarded to the PCIE Homeland Security Working Group which is coordinating Inspectors General review of this important subject. The nature and brevity of this assessment precluded the use of our normal audit protocols; therefore, this review was not conducted in accordance with generally accepted government auditing standards. Had we followed such standards, other matters might have come to our attention.

The recommendations in this report are subject to review and implementation of corrective action by your office in accordance with existing Agency procedures for audit follow-up. Please provide your management decisions for the recommendations to our office within 30 days of the date of this report using the attached SBA Forms 1824, Recommendation Action Sheet.

If you have any questions, please contact Jeff Brindle, Director Information Technology and Financial Management Audit Group at (202) 205-[FOIA Ex. 2].

cc: Stephen D. Galvan, Chief Operating Officer

ATTACHMENT A

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

Date: April 25, 2006

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

/S/ Original Signed by Cheri L. Cannon for
From: Herbert L. Mitchell
Assistant Administrator
Office of Disaster Assistance

/S/ Original Signed
Christine H. Liu
Chief Information Officer
Office of Chief Information Officer

Subject: The Disaster Credit Management System Upgrade Project Needs a Certification and Accreditation Prior to Production

Thank you for the opportunity to review and comment on the Advisory Memorandum of April 2006 regarding certification and accreditation for the Disaster Credit Management System Upgrade Project. The attached is a coordinated response.

Should you or your staff have any questions about the attached, please contact Michael Sorrento, Director, DCMS Operations at (703) 487-[FOIA Ex. 2] or Ethel M. Matthews, Chief Information Security Officer at (202) 205-[FOIA Ex. 2].

Attachment
Response to Disaster Credit Management
System Upgrade Project Audit Finding

ATTACHMENT A

Response to Disaster Credit Management System Upgrade Project Audit Finding

OIG Recommendation:

We recommend that the Assistant Administrator for Disaster Assistance in conjunction with OCIO:

1.A Complete a full re-accreditation of the DCMS Upgrade Project before it is placed into production in accordance with NIST 800-37 and SBA Standard Operating Procedure 90-47.2. Or, complete an Interim Authorization to Operate (IATO) accreditation of the DCMS Upgrade Project in accordance with NIST 800-37 and SBA Standard Operating Procedure 90-47.2. The IATO will only be in use for a limited time frame while a full scope certification and accreditation of the DCMS Upgrade Project is performed at the new production location.

OCIO/ODA Response:

Concur with comment/clarification

In order to support the planned deployment in June 2006, an Interim Accreditation will be performed to provide authority to operate for a 4-month period. The C&A Package will include the following attachments: an updated System Security Plan (existing format), Vulnerability Scan Reports covering all of the servers, a Risk Mitigation Plan of Action and Milestones, and a Continuous Monitoring Plan. Full accreditation will be planned for completion no later than October 2006. The C&A Package will include the following attachments: a revised System Security Plan (new NIST SP 800-18 Rev 1 format), Security Test and Evaluation Report, a Risk Assessment Report, a Risk Mitigation Plan of Action and Milestones, and a Continuous Monitoring Plan.