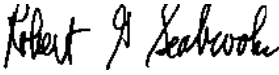




U.S. SMALL BUSINESS ADMINISTRATION  
OFFICE OF INSPECTOR GENERAL  
WASHINGTON, D.C. 20416

|                                   |
|-----------------------------------|
| <b>AUDIT REPORT</b>               |
| <b>Issue Date: March 30, 2000</b> |
| <b>Number: 0-15</b>               |

**To:** Lawrence E. Barrett, Chief Information Officer

**From:** Robert G. Seabrooks,   
Assistant Inspector General for Auditing

**Subject:** Audit of SBA's Proposed Systems Development Methodology

SBA's strategic goals depend heavily on the development of new information systems. In the past, however, SBA has been criticized for inadequate planning and poor systems development procedures. The Office of the Chief Information Officer (OCIO) is, therefore, developing a "Systems Development Methodology" (SDM) to help accomplish its strategic goals and address those criticisms. The SDM is a set of procedures and quality controls intended to reduce risks in the development of new systems and ensure that systems function as intended. In response to a request by the OCIO, the Auditing Division of the Office of Inspector General reviewed and evaluated the proposed SDM.

The proposed SDM, modeled on one obtained from the Department of Housing and Urban Development, is divided into six phases:

- **Initiate Project:** The need for the system is defined and validated. A project plan is developed; a feasibility study, risk analysis, and cost/benefit analysis are conducted; and the proposed system is categorized in terms of platform, development techniques, and type of effort.
- **Define System:** System objectives are expanded into specific, detailed functional and data requirements, which form the basis for the detailed design of the system.
- **Design System:** Detailed specifications are developed that emphasize the physical solution to the users' information management needs.
- **Build System:** Developers transform the information provided in the Design System phase into machine-executable form, and ensure that all of the individual components of the system function correctly and interface properly with other components.

- **Evaluate System:** Independent testers measure the system’s ability to perform the functions required by the users and ensure an acceptable level of performance.
- **Operate System:** The system is initially installed at a pilot site and eventually released into its full-scale production environment. Training in using the system is conducted and system performance is monitored.

## OBJECTIVES AND SCOPE

The objectives of our review were to determine whether the proposed SDM (1) is consistent with government and industry standards, and (2) will help ensure that new information systems are developed on time, within budget and with the intended functionality. We used guidance obtained from the Information Systems Audit and Control Association (ISACA) to evaluate the SDM. That guidance incorporates criteria established by the Office of Management and Budget, General Accounting Office, National Institute of Standards and Technology, Department of the Treasury, other Federal Agencies and the Institute of Electrical and Electronic Engineers.

We evaluated the proposed SDM with respect to its structure, key closure points,<sup>1</sup> security and internal controls, participation and responsibilities of key groups, communications between key groups, and documentation and programming standards. Fieldwork was conducted from August 1999 through February 2000 at SBA Headquarters in Washington, DC. The review was conducted in accordance with Government Auditing Standards.

## RESULTS OF AUDIT

We found that the proposed SDM (1) is generally consistent with government and industry standards, and (2) will help ensure that new information systems are developed on time, within budget and with the intended functionality. We did note, however, some differences between the SDM and applicable guidelines as described below.

### *Specify a Role for the OIG in the Initiate Project Phase*

Although the proposed SDM does specify OIG (audit) roles that are consistent with the ISACA guidance in the subsequent phases, it does not specify an OIG role in the Initiate Project phase. In the Initiate Project phase, the ISACA guidance specifies the audit role of reviewing and evaluating the “Needs Statement” and other phase deliverables. The requirements of this phase are critical to the success of subsequent phases, and specifying a role for the OIG can help ensure those requirements are satisfied before subsequent phases are initiated.

---

<sup>1</sup> Closure points are the formal end to a phase that require completion of documentation and may require management review meetings to ensure that all phase activities have been carried out and all deliverables have been completed.

### *Address Records Management Requirements*

In the Define System phase, the proposed SDM calls for determination of functional requirements in several categories, such as performance, security, and internal controls, but it does not specifically call for determination of records management requirements. Federal government agencies are required to preserve and maintain records of their organization, functions, policies, decisions, procedures, operations and activities. With respect to automated information systems that create, process and maintain electronic records, there are a number of specific federal records management requirements. Accordingly, Title 36 CFR section 1234.10 requires agencies to establish procedures for addressing records management requirements before approving new electronic information systems or enhancements to existing systems. The SDM could be improved by designating a role for the agency's records manager in the Define System phase, with responsibility for determining records management requirements.

### *Require Development of a Vulnerability, Threat, Safeguard Matrix*

The proposed SDM currently calls for identification of system assets, associated threats and vulnerabilities, and appropriate countermeasures to safeguard against them, but it does not specify a standardized deliverable to help ensure accomplishment of this requirement. According to the ISACA guidance, good system development methodologies specify preparation of predefined products and deliverables, and in better methodologies these products are standardized. The proposed SDM does specify a number of predefined products and deliverables, such as checklists and analyses, to help ensure the satisfaction of key requirements. A matrix, as illustrated below, is an example of a standardized deliverable that would help ensure comprehensive identification of threats, vulnerabilities, and safeguards for all system assets and components.

| <b>Asset Category</b> | <b>Threat</b>  | <b>Vulnerability</b> | <b>Safeguard(s)</b>                         |
|-----------------------|--|----------------------|---|
| Computer Hardware     | Destruction  | Fire                 | Fire Suppression System                     |
| Mission Critical Data | Unauthorized Disclosure, Modification or Destruction | Network Penetration  | Firewalls, Access Controls, Data Encryption |

### *Complete the Application and Programming Standards and Related Documents*

SBA's current programming and applications standards are either outdated or incomplete. The official standards document is the OIRM Operations and ADP Standards Manual, created in 1990, when major applications were developed on mainframe computer systems. Per OCIO personnel, this manual is not suited for client-server system development – currently the agency's primary development platform.

Client-server development standards are addressed in a separate document that is not complete at this time (OISS Application Standards). The chapter of the document that pertains to programming standards is complete, however, and should be incorporated in the SDM either by reference or as an appendix.

The ISACA guidelines specify that organizations must identify and follow policies, procedures and standards in developing automated information systems. Some of the policies, procedures and standards referred to in the SDM, however, have not yet been developed. These include:

- Cost / Benefit Analysis Methodology
- Standard Release Procedures
- Gap Analysis Procedures

Without complete guidance and reference documentation, there is a greater chance that system development projects may deviate from acceptable practices.

## **Recommendations**

We recommend that the Chief Information Officer:

- 1A. Make the following changes to the proposed SDM, and establish the SDM as official agency policy for system development projects.
  - Modify Table 1-11 to designate a role in the Initiate System phase for the OIG, with the responsibility to review phase products to ensure critical requirements have been satisfied.
  - Modify section 2.0 to designate a role for the agency records manager with the responsibility to ensure that federal records management requirements are defined.
  - Modify section 1.6 to require the preparation of a threat, vulnerability and safeguard matrix, or other standardized deliverable, to help ensure safeguards are identified for all significant asset threat combinations.
  - Incorporate Chapter 4 of the OISS Application Standards in the SDM either by reference or as an appendix, and specify in section 4.3.2 that these are the standards to be followed for client-server development projects.
- 1B. Establish responsibilities, budgets, milestones and deliverables to ensure completion of the Programming and Application Standards, Cost / Benefit Analysis Methodology, Standard Release Procedures, and Gap Analysis Procedures.

## Management Response

The Chief Information Officer responded that his office is committed to adopting a Systems Development Methodology (SDM) that is robust, flexible, useful, and conforms to government and industry standards. He also agreed to implement the report's recommendations.

## OIG Evaluation

The Chief Information Officer's reply was responsive to the report.

\* \* \*

This report is based on auditors' conclusions and their review of the proposed SDM and relevant standards. **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, Acting Director, Business Development Programs Group at (202) 205-7204.

## REPORT DISTRIBUTION

| <u>Recipient</u>   | <u>No. of Copies</u> |
|--|----------------------|
| Associate Deputy Administrator for Management and Administration ..... | 1                    |
| Associate Administrator, Office of Disaster Assistance.....            | 1                    |
| Chief Financial Officer .....  | 1                    |
| General Counsel .....  | 2                    |
| U.S. General Accounting Office .....                                   | 1                    |