Please Note: Multiple sections from the following report have been withheld due to potential security vulnerabilities.

AUDIT OF SBA'S CONTINUITY OF OPERATIONS PLANNING PROGRAM

AUDIT REPORT NUMBER 5-17

MARCH 30, 2005

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
Washington, DC 20416

AUDIT REPORT
Issue Date: March 30, 2005
Number: 05-17

To: Stephen D. Galvan
Chief Operating Officer
Chief Information Officer

Jerry E. Williams
Acting Chief Information Officer

From: Robert Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's Continuity of Operations Planning Program

Attached is a copy of the subject audit report. The report contains two findings and 12 recommendations addressed to the Chief Operating Officer and one finding and three recommendations to the Chief Information Officer.

SBA reviewed a draft of this report and generally agreed with the findings and recommendations. SBA's entire response is incorporated in Appendix A of this report.

The recommendations in this audit report are based on the conclusions of the Auditing Division. The recommendations are subject to review, management decision and action by your office in accordance with existing Agency procedures for audit follow-up and resolution.

Any questions or discussion of the findings and recommendations contained in the report should be directed Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at

Attachment

AUDIT OF SBA'S CONTINUITY OF OPERATIONS PLANNING PROGRAM

Table of Contents

SUMMARY

It is the policy of the United States to have in place a comprehensive and effective program to ensure the continuity of essential Federal functions under all circumstances. To support this policy the Federal Executive Branch has implemented the Continuity of Operations program (COOP). An effective COOP includes plans and procedures that delineate essential functions; specify succession to office and the emergency delegation of authorities; provides for safekeeping of vital records and databases; identifies alternate operating facilities; provides for interoperable communications, and validates the capability through tests, training and exercises.

The audit objectives were to determine whether: (1) The SBA is in a position to achieve a timely and orderly recovery from an emergency and resumption to full service, (2) SBA's COOP and Business Resumption Plans (BRP) were sufficient to aid the recovery officials through a step by step process that would result in a successful recovery, (3) contingency plans contain all the elements of a viable COOP capability, and (4) SBA's Information Technology (IT) – System Disaster Recovery Plans (SDRP) were utilized and were adequate to aid in the restoration of SBA IT systems and the plans had been tested.

The audit disclosed the following issues adversely impacting SBA's COOP capability:

- SBA's COOP was not adequate to ensure that the Agency could successfully recover essential agency functions during disruptive emergency situations.

- SBA's COOP does not have an adequate chain-of-command, nor adequate oversight and funding. Additionally, SBA has not adequately tested its COOP and all program, disaster and field office BRPs that would be needed to resume office functions during emergency or disaster events.

- SBA's COOP and individual BRPs did not contain all necessary information to ensure that the plans were viable and that the Agency or its individual offices could utilize the plans in the event of an emergency. SBA has not implemented an effective review and approval program for its COOP and BRPs. The SBA Headquarters COOP did not adequately identify essential functions performed by the agency and which functions must be continued under all circumstances. SBA did not adequately identify facilities and equipment needed in its COOP and office BRPs in the event of an emergency disruptive situation and plan activation.

- SBA did not have adequate System Disaster Recovery Plans (SDRP) to ensure the recovery of critical IT systems supporting the Agency's essential functions. SBA did not restore its major systems during recovery test exercises by specifically using its SDRPs to perform the system restorations.

We made recommendations to the Chief Operating Officer to:

Ten (10) recommended actions redacted

We made recommendations to the Chief Information Officer to:

Three (3) recommendations redacted

INTRODUCTION

A. Background

FEMA issued Federal Preparedness Circular (FPC) 65 – Federal Executive Branch Continuity of Operations to all Federal Department and Agencies. FPC 65 establishes the criteria from which all Federal Executive Branch departments, agencies, and independent organizations should use to develop an effective Continuity of Operations Program. FPC 65 establishes the identification of essential functions and that those essential functions must be operational within 12 hours of COOP activation.

SBA has implemented its COOP under Standard Operating Procedure (SOP) 90-47 "Automated Information Systems Security Program." SOP 90-47 identifies that an Agency continuity of operations program must be in effect to ensure that critical Agency applications and systems will be available during emergency situations. Additionally, according to SOP 90-47, the Administrator has delegated COOP responsibilities to the Chief Information Officer. The Chief Information Officer has further delegated the COOP to the Agency Computer Security Program Manager to ensure the establishment and maintenance of a comprehensive continuity of operations plan for each computer installation.

The SBA Agency Computer Security Program Manager has assigned employees and contractors within the Office of Chief Information Officer (OCIO) and has a database management system (E-Planner) to store, maintain and keep the SBA COOP and BRPs current. To further oversee and implement COOP, OCIO has issued informal requirements for headquarters and field office BRPs to ensure consistency and completeness and the ability to test the plans. OCIO is also responsible for testing and training SBA employees named in the Agency COOP and office BRPs.

SBA reported to the Office of Management and Budget in its Federal Information Security Management Act (FISMA) Executive Summary on June 30, 2003 that Business Resumption Plans for all Regional/District Offices had been completed.

The COOP is the SBA Agency plan to continue essential functions across a broad spectrum of emergencies. The BRPs are the SBA headquarters program and field office recovery plans for initiating recovery of their business functions in the event of a disaster or other emergency event at either the SBA headquarters or at SBA field office locations. The SDRPs are IT recovery plans to restore major computerized systems in the event of an emergency at alternate locations.

B. Objectives and Scope

The audit objectives were to determine whether: (1) The SBA is in a position to achieve a timely and orderly recovery from an emergency and resumption to full operating service, (2) SBA's COOP and BRPs were sufficient to aid the recovery officials through a step by step process that would result in a successful recovery, (3)

contingency plans contain all the elements of a viable COOP capability, and (4) SBA's IT System Disaster Recovery Plans (SDRP) were utilized and were adequate to aid in the restoration of IT systems and the plans had been tested.

We selected and reviewed SBA's COOP to determine its compliance with FEMA FPC 65. Since SBA's Headquarters COOP relies heavily on individual program office contingency plans, we selected and reviewed copies of all SBA headquarters program office BRPs. Additionally, we judgmentally selected and reviewed 20 SBA field office BRPs. Offices considered essential to the SBA financial and disaster assistance functions were given priority for selection purposes. We used FPC 65 guidance to determine whether these plans included all the elements of a viable COOP capability. Additionally, we reviewed individual office BRPs to determine compliance with OCIO informal pronouncements to satisfy the information requirements for the SBA COOP.

We reviewed SBA's FY 2003 – FY 2007 Information Technology Strategic Plan and Information Security Strategic Plan to determine whether they satisfied FPC 65 requirements for SBA to create a continuity of operations multi-year strategy and program management plan. Additionally, we reviewed SBA's agency-wide computer based training program and all COOP exercise reports and critical system disaster recovery reports to determine whether SBA has implemented an effective Testing, Training and Exercise (TT&E) Program.

We reviewed SDRPs for 13 SBA mission critical systems to determine whether they satisfied requirements set in OMB Circular A-130, NIST Special Publication 800-34 and SBA's Headquarters Continuity of Operations Plan. Interviews were conducted with Office of the Chief Information Officer officials to discuss the efforts of SBA's Continuity of Operations Program.

Audit fieldwork was performed from March through December, 2004; and included tests that we considered necessary to answer our audit objectives. The audit was performed in accordance with generally accepted Government Auditing Standards.

RESULTS OF AUDIT

FINDING 1 SBA's COOP is not Adequate to Assure the Recovery of Essential Agency Functions

Details of audit findings redacted
Approximately 5 ½ pages

Management Comments

SBA generally agreed to the finding and recommendations. SBA indicated that it had reassigned the COOP and BRP oversight responsibilities from the CIO to the COO. On behalf of the COO, a Senior Advisor for Policy Planning is leading a small task force with participation from the major SBA program offices. This COOP task force is preparing a project plan with milestones that uses the FEMA FPC 65 as a blueprint for COOP implementation, augmented by the findings and recommendations of the audit report. SBA's complete response is included in Appendix A.

With respect to the testing of the agency COOP and field office BRPs (recommendation 1B), management stated that SBA's COOP is tested twice a year. Additionally, SBA tested three BRPs in May 2004 and plans to test two or three BRPs for each testing cycle.

Evaluation of Management's Comments

SBA's comments were generally responsive to the recommendations. However, SBA would require approximately 20-30 years to fully test all of its roughly 100 BRPs if it continued to test about five BRPs per year. Therefore, we have amended our initial recommendation from 33 percent of SBA BRPs tested every year to 25 percent of SBA BRPs tested every year. We will work with the COOP task force during the audit resolution process to come to agreement on the number of BRPs that need to be tested

both annually and over a time frame cycle that would ensure the viability and completeness of SBA's BRPs testing program.

FINDING 2 SBA's COOP and BRPs were Incomplete and Could not Assure the Recovery of Essential Agency Functions

Details of audit findings redacted
Approximately 5 ½ pages

Management Comments

SBA generally agreed with the findings and recommendations. SBA stated that as part of the responsibility of the COOP task force, it will create and codify the review and approval process of the COOP and BRPs. SBA is currently reviewing the BRPs in the E-Planner data base to check for compliance with the new FEMA regulation and will be issuing further guidance prior to requesting field office to review and update their plans. SBA's complete response is included in Appendix A.

Evaluation of Management's Comments

SBA's comments were responsive to the recommendations.

FINDING 3 SBA Information Technology System Disaster Recovery Plans were not adequate to Ensure the Recovery of Major Systems

Details of audit findings redacted
Approximately 2 1/3 pages

Management Comments

SBA generally agreed with the findings and recommendations. SBA identified that it is reevaluating its "mission critical" systems to identify those that should be removed from the mission critical list or merged with other systems and will update the SDRPs for the reduced number of mission critical systems.

Evaluation of Management's Comments

SBA's comments are responsive to the recommendations.

* * *

The findings included in this report are the conclusions of the Office of Inspector General's Auditing Division. The findings and recommendations are subject to review, management decision, and corrective action by your office in accordance with 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 both your proposed corrective action and target date for completion, or explanation of your disagreement with our recommendations.

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 Jeffrey R. Brindle, Director, Information Technology and Financial Management Group at (202) 205-7490.

Attachments

U.S. SMALL BUSINESS ADMINISTRATION
WASHINGTON, DC 20416

Date: March 23, 2005

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Stephen D. Galvan
Chief Operating Officer

Subject: SBA Response to Audit of SBA's Continuity of Operations Program (COOP)

Summary

From March through December 2004, OIG staff audited SBA's COOP, *dated June 2003*, to determine its compliance with FEMA Federal Preparedness Circular (FPC) 65. The report identifies several COOP inadequacies relating to:

- Chain of command, oversight, funding, awareness, participation of key personnel in training, and testing/training;
- Review and approval process, identification of essential functions, vital records, and facilities and equipment needed for recovery functions;
- System Disaster Recovery Plans (SDRPs) and their use in recovering mission critical information systems.

To address these deficiencies, the audit report offers three findings with twelve recommendations directed to the Chief Operating Officer and three recommendations directed to the Chief Information Officer. In general, SBA agrees with the report's findings and recommendations and is using the audit as a blueprint for improving the implementation of its COOP, a process that will require the remainder of the fiscal year to complete. Moreover, we believe that substantial progress continues to be made to address the identified issues. Most notably, SBA reassigned the responsibility for direction and oversight of the COOP from the OCIO to the COO. Under the leadership of the COO, SBA has formed a small task force with cross-agency staff participation to complete, update, and implement the COOP and ensure that related emergency preparedness plans (e.g., IT Continuity Plan, Incident Management System, and Business Resumption Plans) are updated, tested, and viable for use in responding to an incident. We have also just completed training for the Incident Management and Damage Assessment Teams, with plans to brief the Management Board in the near future.

Additional comments with proposed action tagged to individual recommendations follow:

FINDING 1 SBA's COOP is not Adequate to Assure the Recovery of Essential Agency Functions (management, testing, up-to-date delegations of authority, training, funding & staffing)

Details of management response redacted
Approximately 1 1/8 page

FINDING 2 SBA's COOP and BRPs were Incomplete and could not Assure the Recovery of Essential Agency Functions

Details of management response redacted
Approximately 1 ½ pages

FINDING 3 **SBA Information Technology System Disaster Recovery Plans were not adequate to Ensure the Recovery of Major Systems**

Details of management response redacted
Approximately ½ page

APPENDIX B

REPORT DISTRIBUTION

Recipient	Copies
Office of the Chief Financial Officer Attention: Stephen D. Galvan	1
Office of the Chief Information Officer Attention: Jerry E. Williams	1
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	3
U.S. Government Accountability Office	1