# AUDIT OF SBA'S PLANNING AND ASSESSMENT FOR IMPLEMENTING PRESIDENTIAL DECISION DIRECTIVE 63

## AUDIT REPORT NO. 1-09

## MARCH 26, 2001

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

| **AUDIT REPORT** |
|---|
| **Issue Date: March 26, 2001** |
| **Number: 1-09** |

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

Robert G Seabrooks

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

**Subject:** Audit of SBA's Planning and Assessment for Implementing Presidential Decision Directive 63

As part of a government-wide initiative, sponsored by the President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE), we completed the second of four planned audits of SBA's critical infrastructure protection program. The first audit covered SBA's planning and assessment activities for protecting its critical, cyber-based infrastructure. This audit covered the planning and assessment activities for protecting the critical, physical (non-cyber-based) infrastructure. The third and fourth audits will address implementation activities, i.e., risk mitigation, emergency management, interagency coordination, resource and organization requirements, recruitment, education and awareness.

## BACKGROUND

Presidential Decision Directive 63 (PDD 63), issued in May 1998, calls for a national effort to assure the security of the United States' critical infrastructures. Critical infrastructures are the physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, banking and finance, energy, transportation, and essential government services. PDD 63 requires every department and agency of the Federal Government to develop and implement a plan for protecting its own critical infrastructure – also known as minimum essential infrastructure (MEI).

The Critical Infrastructure Assurance Office (CIAO), an interagency office established to assist in the development of a national plan for protecting the country's critical infrastructure defines MEI as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services."

SBA's Computer Security Program Manager, who reports to the Chief Information Officer, has been designated the Critical Infrastructure Assurance Officer with overall responsibility for protecting SBA's critical infrastructure.

## RESULTS OF PRIOR AUDIT

In September 2000, we reported that SBA had made significant progress toward implementing key aspects of PDD 63, and that it needed to (1) complete the identification of its critical infrastructure, (2) perform vulnerability assessments, (3) complete remedial plans, (4) update the Critical Infrastructure Protection Plan, (5) develop a multi-year funding plan, and (6) include infrastructure assurance in its strategic planning and performance measurement framework.

In October 2000, SBA revised its Critical Infrastructure Protection Plan and took other steps to address these recommendations. These actions, however, focused on the Agency's cyber-based infrastructure, not the physical (non-cyber-based) infrastructure.

## OBJECTIVES, SCOPE AND METHODOLOGY

The objective of this audit was to determine whether SBA's planning and assessment activities for protecting its critical, physical infrastructure meet the requirements of PDD 63. To accomplish this, we reviewed the Agency's Critical Infrastructure Protection Plan (CIPP) and related material, and interviewed SBA personnel associated with these products. We conducted the review following guidance provided by the PCIE / ECIE working group on critical infrastructure assurance. That guidance incorporated criteria from PDD 63, "The National Plan for Information Systems Protection," various Executive Orders and circulars, GAO, and relevant laws and regulations. Fieldwork was performed at SBA's Central Office in Washington, DC from January to March 2001. The audit was conducted in accordance with Government Auditing Standards.

## AUDIT RESULTS

SBA has continued making progress toward implementing PDD 63 requirements, but its focus has been on protecting the Agency's critical, cyber-based infrastructure. To fully comply with PDD 63, the Agency needs to expand its infrastructure protection efforts to address its critical, physical infrastructure.

### Efforts to Date Have not Focused on Physical MEI

SBA's Critical Infrastructure Protection Plan (CIPP), revised in October 2000, focuses on protecting the Agency's cyber-based infrastructure; the plan identifies mainframe computer systems, and Local and Wide Area Networks as the critical, cyber-based assets supporting the five identified Minimum Essential Critical Programs. The CIPP does not address the physical assets (e.g. personnel and facilities) supporting these Minimum Essential Critical Programs. The focus on cyber-based systems was primarily due to PDD 63's emphasis on such systems. The Agency does, however, recognize the need to address physical MEI and has started to

concentrate its efforts in that direction. In addition, many of the activities needed for protection of the critical, physical infrastructure (e.g. building security and fire prevention) are in place, but have not been integrated into the critical infrastructure protection program.

According to the Critical Infrastructure Assurance Office, a key first step in the process of protecting critical infrastructure is "determining what information systems, data, and associated assets – **facilities, equipment, personnel** – constitute the critical infrastructure…." [emphasis added]. After the critical physical infrastructure is identified, vulnerability assessments should be performed, remedial plans developed, resource requirements identified, and policies and procedures updated as necessary.

**Need to Coordinate with the General Services Administration**

PDD 63 and "The National Plan for Information Systems Protection" call for agencies to establish effective CIP coordination with other applicable entities. Protection of SBA's physical infrastructure, in particular, requires coordination with the General Services Administration (GSA). This is because, while SBA is responsible for protecting its physical infrastructure, GSA is responsible for the security of the Federal and leased buildings in which SBA operates. Because SBA's PDD 63 efforts to date have not focused on the physical infrastructure, the Agency has yet to coordinate with GSA. Without effective coordination, the effectiveness and efficiency of SBA's infrastructure protection program may be diminished by either non-performance or duplication of key functions.

**Recommendations:**

We recommend that the Chief Information Officer ensure that the Chief Infrastructure Assurance Officer:

1. Revise the CIPP to address protection of the Agency's physical MEI. The revised plan should provide milestones and responsibilities for identification of physical MEI, performance of vulnerability assessments, development of remedial plans, determination of resource requirements, and updating of policies and procedures as necessary.

2. Coordinate physical infrastructure protection efforts with the General Services Administration.

## SBA Management's Comments

SBA's Chief Information Officer agreed with the recommendations and stated that his office has already taken steps to address the issues. The Chief Information Officer's response is included as Attachment 1.

## OIG Evaluation of SBA Management's Comments

The Chief Information Officer's comments are responsive to our recommendations.

* * *

The findings included in this report are the conclusions of the Office of Inspector General's Auditing Division based upon the auditor's testing of the Agency's Critical Infrastructure Protection Plan and 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 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) 205-7204.

Attachments

Attachment 1

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

**Date:** March 22, 2001

**To:** Robert G. Seabrooks
Assistant Inspector General for Auditing

**From:** Chief Information Officer

**Subject:** Audit of Planning and Assessment for Protecting SBA's Critical, Physical Infrastructure

We have reviewed the report on the Planning and Assessment for Protecting SBA's Critical, Physical Infrastructure. We agree with both recommendations.

We have already taken steps to address the issues in the recommendations. We are working closely with the Office of Administration (OA) which has responsibility for SBA's physical infrastructure and physical security. OA is developing the physical MEI component for inclusion in the Critical Infrastructure Protection Plan.

The Office of Administration has a close working relationship with the General Services Administration and is coordinating SBA's physical protection efforts, where appropriate, with GSA.

We recently hosted executive briefings, given by General Services Administration personnel, on Continuity of Operations to acquaint SBA senior managers with their responsibilities for safeguarding Agency assets and infrastructure. These briefings covered PDD 63 and PDD 67. We will be having more detailed briefings for SBA Functional Program Managers in April 2001.

If you require additional information, please contact Howard Bolden, Agency Computer Security Program Manager, on (202)205-7173.

Lawrence E. Barrett

Lawrence E. Barrett

**Attachment 2**

## REPORT DISTRIBUTION

| Recipient | No. of Copies |
|---|---|
| Associate Deputy Administrator for Management and Administration | 1 |
| Office of the Chief Financial Officer<br>Attention: [FOIA Ex. 6] | 1 |
| General Counsel | 2 |
| U.S. General Accounting Office | 1 |

FOIA Ex. 6