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

AUDIT REPORT NUMBER 0-27

SEPTEMBER 26, 2000

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

AUDIT REPORT
Issue Date: September 26, 2000
Number: 0-27

To: Lawrence E. Barrett, Chief Information Officer

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

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

As a result of a joint initiative by the President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE), we completed the first of four planned audits of SBA's critical infrastructure protection program. This report covers SBA's planning and assessment activities for protecting its critical cyber-based infrastructures.

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. Advances in information technology have caused these infrastructures to become increasingly automated and inter-linked. These same advances have also created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. PDD 63 requires every department and agency of the Federal Government to develop and implement a plan for protecting its own critical infrastructure.

The Critical Infrastructure Assurance Office has set a December 2000 target date for Federal Agencies and Departments to assess their critical information systems vulnerabilities, adopt a multi-year funding plan to remedy them, and create a system for continuous updating. Although SBA was not identified as a "Tier One" or "Tier Two" agency with specific milestones for the completion of PDD 63 requirements, the Agency has committed to the

completion of those requirements, and has, in fact, completed some of the requirements.

OBJECTIVES, SCOPE AND METHODOLOGY

The objective of the audit was to evaluate the adequacy of SBA's Critical Infrastructure Protection Plan (CIPP), infrastructure identification efforts, and initial vulnerability assessments. To accomplish this objective, we reviewed the Agency's CIPP and related materials, and interviewed SBA and contractor 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, and relevant laws and regulations. Fieldwork was performed at SBA's Central Office in Washington, DC from January to May 2000. The audit was conducted in accordance with Government Auditing Standards.

AUDIT RESULTS

SBA has made significant progress toward implementing key aspects of PDD 63, but additional actions are still needed. In November 1998, the agency completed a CIPP that identified a number of tasks to be accomplished. Subsequently, however, based on feedback from the Critical Infrastructure Assurance Office, the agency shifted the focus of its information systems security efforts to related areas such as PDD 67 (Continuity of Operations), Year 2000 Contingency Planning, and recommendations made in previous OIG audits of information systems controls. Although these efforts satisfied a number of PDD 63 requirements, the Agency did not complete all of the tasks identified in its CIPP and needs to refocus its efforts toward meeting PDD 63 requirements.

Complete the Identification of the Critical Infrastructure

PDD 63 requires all Federal Government agencies to develop and implement plans for protecting their own critical infrastructures. According to the Critical Infrastructure Assurance Office, a key first step in this process is "determining what information systems, data, and associated assets – facilities, equipment, personnel – constitute the critical infrastructure…."

SBA's CIPP identified five critical business functions, and called for a study to identify and establish the boundaries of the infrastructure that supports those functions. Performance of this study was delayed, however, pending completion of related efforts. As a result, SBA has not fully identified and established the boundaries of its critical infrastructure, and is therefore, not in position to meet the other requirements of PDD 63.

Perform Vulnerability Assessments

The next step in infrastructure assurance is performing vulnerability assessments. SBA's CIPP also included a task for conducting vulnerability assessments for the cyber infrastructure supporting its critical business functions. The Agency developed a schedule for conducting vulnerability assessments on systems with security weaknesses identified in previous OIG audits, and as of May 2000, has completed those assessments for systems supporting two of its key business functions. These assessments identified vulnerabilities and recommended corrective actions. Because of the shift in focus to related efforts and because it has not completed the study to identify the boundaries of its critical infrastructure, however, SBA has not performed vulnerability assessments for all of its critical infrastructure.

Complete Remedial Plans

PDD 63 and "The National Plan for Information Systems Protection" provide that remedial plans should be developed based on the vulnerability assessments. These plans should identify timelines for implementation, assignment of responsibilities, and funding. The vulnerability assessments SBA performed contained recommendations for correcting the identified vulnerabilities, but they did not identify timelines for implementation, responsibilities and funding. As a result, a successful remedial effort may not be achieved.

Update the Critical Infrastructure Protection Plan

PDD 63 requires agencies to update their plans for protecting their critical infrastructures every two years. SBA originally planned to update its November 1998 CIPP in May 2000, but this was delayed pending completion of additional vulnerability assessments. The plan needs to be updated to fully identify how the agency intends to protect its critical infrastructure and to reflect the progress it has made. The updated plan should identify the tasks remaining to be accomplished and set milestones for their completion. It should also reference the related materials and accomplishments (e.g. vulnerability assessments and business resumption plans) to identify the PDD 63 requirements that have been satisfied. Based on guidance from the PCIE / ECIE Working Group on Infrastructure Assurance, the plan should:

- Provide for evaluation of new assets to determine whether they should be included in the critical infrastructure,

- Identify a schedule for completing and updating Vulnerability Assessments and Remedial Plans,

- Provide for periodic testing and re-evaluation of risk mitigation steps (policies, procedures, and controls) by agency management,

- Require a review of existing policies and procedures to determine whether the agency should revise them to reflect PDD 63 requirements,

- Identify how security-planning procedures are incorporated into the basic design of new cyber-based systems and new operational programs, and

- Require the agency to identify the resource and organizational requirements for implementing PDD 63.

Develop a Multi-Year Funding Plan

PDD 63 and "The National Plan for Information Systems Protection" call for agencies to develop and adopt multi-year funding plans to remedy security weaknesses identified in their vulnerability assessments. SBA needs to develop a multi-year funding plan to ensure sufficient funding to meet PDD 63 requirements.

Include Infrastructure Assurance Functions in SBA's Strategic Planning and Performance Measurement Framework

PDD 63 provides for agencies to include infrastructure assurance functions within their Government Performance and Results Act (GPRA) strategic planning and performance measurement framework. SBA's GPRA plans did not include infrastructure assurance objectives and plans. As a result, infrastructure assurance functions may not receive the management attention necessary to meet PDD 63 requirements.

RECOMMENDATIONS

We recommend that the Chief Information Officer:

1. Complete the study to determine what information systems, data, and associated assets – facilities, equipment, personnel – constitute the agency's critical infrastructure.

2. Conduct or complete vulnerability assessments on the critical infrastructure by December 31, 2000.

3. Develop remedial plans to address critical infrastructure vulnerabilities. The plans should address responsibilities, milestones for completion, and funding.

4. Update the Critical Infrastructure Protection Plan (CIPP).

5. Develop and adopt a multi-year funding plan to remedy the vulnerabilities identified by Vulnerability Assessments.

6. Include infrastructure assurance functions within the agency's Government Performance and Results Act (GPRA) strategic planning and performance measurement framework.

SBA MANAGEMENT'S RESPONSE

SBA's Chief Information Officer agreed with the recommendations.

* * *

The findings included in this report are the conclusions of the Auditing Division based upon the auditors' review 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.**

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, Director, Business Development Programs Group at (202) 205-7204.

Attachment

ATTACHMENT

REPORT DISTRIBUTION

Recipient	No. of Copies
Associate Deputy Administrator for Management and Administration	1
Office of the Chief Financial Officer Attention: Jeffrey Brown	1
General Counsel	2
U.S. General Accounting Office	1