AUDIT OF SBA'S IMPLEMENTATION OF ITS CYBER-BASED CRITICAL INFRASTRUCTURE PROTECTION PLAN

AUDIT REPORT NUMBER 3-03

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

AUDIT REPORT
Issue Date: January 10, 2003
Number: 3-03

To: Lawrence E. Barrett
Chief Information Officer

From: Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's Implementation of Its Cyber-Based Critical Infrastructure Protection Plan

As part of a government-wide initiative, sponsored by the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE), we completed an audit of SBA's implementation of its critical infrastructure protection program for SBA's cyber-based infrastructure. The protection of SBA's critical infrastructure is required by Executive Order 13231 "Critical Infrastructure Protection in the Information Age" and Presidential Decision Directive (PDD) 63 – Critical Infrastructure Protection.

Since PDD 63 was issued in 1998, a number of its original cyber security requirements have been transcended by more recent laws or executive orders on critical infrastructure protection. The Government Information Security Reform Act (GISRA) enacted in FY 2000 now requires reporting on many of the cyber security issues and performance measures originally required under PDD 63. However, PDD 63 was not superseded by GISRA. In the most recent reporting time frame, GISRA required responses on the condition of Agencies critical infrastructure protection efforts.

BACKGROUND

PDD 63, issued in May 1998, called for a national effort to ensure 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. Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and government services. Advances in information technology have caused these infrastructures to become increasingly

automated and inter-linked. These same advances have created new vulnerabilities that threaten the normal operation of the economy and government. The vulnerabilities include equipment failures, human error, natural disasters, physical attacks, and cyber attacks.

PDD 63 required every department and agency of the Federal Government to develop and implement a plan for protecting its own critical or mission essential infrastructure. The plan is referred to as a "Critical Infrastructure Protection Plan" (CIPP). PDD 63 also required Federal agencies to designate a Critical Infrastructure Assurance Officer (CIAO) who has overall responsibility for protecting the agency's critical infrastructure. SBA has designated the Computer Security Program Manager, who reports to the Chief Information Officer (CIO), as the CIAO.

This is the third of four planned audits of SBA's critical infrastructure protection program. The first audit covered SBA's planning and assessment activities for protecting its mission critical, cyber-based infrastructure. The second audit reviewed SBA's planning and assessment activities for protecting its mission critical, physical (non cyber-based) infrastructure. The fourth audit will address SBA's implementation of its CIPP for the critical, physical infrastructure.

OBJECTIVES, SCOPE AND METHODOLOGY

The objective of this audit was to determine whether SBA has adequately implemented its cyber-based infrastructure protection plan and is adequately protecting its cyber-based systems. Specifically, we assessed the adequacy of SBA's implementation activities in the following areas:

- Risk mitigation
- Emergency management
- Interagency coordination
- Resource and organization requirements
- Recruitment, education and awareness

To accomplish these objectives, we reviewed the Agency's most recent CIPP dated September 28, 2001, certification and accreditation documents for critical information systems, and other related documents. We interviewed knowledgeable SBA personnel. We followed the guidance provided by the PCIE/ECIE working group on critical infrastructure assurance. We also determined the status of prior audit recommendations in our audit report dated September 26, 2000. Fieldwork was performed at SBA's Central Office in Washington, DC, from June 2002 to August 2002. The audit was conducted in accordance with Government Auditing Standards.

AUDIT RESULTS

SBA continues to improve its critical infrastructure protection program. Since our audit report on Planning and Assessment for Critical Infrastructure Protection (0-27) issued in September 2000, SBA:

- Identified 37 high priority systems that broadly constitute the boundaries of its critical cyber based infrastructure.
- Performed vulnerability assessments for 22 of its 37 high priority systems.
- Began the process for mitigating risks identified in the vulnerability assessments.
- Developed an on-line Computer Security Training program that all SBA employees are required to undertake every year.
- Created a Computer Emergency Response program for identifying and reporting computer incident attacks to FedCIRC and other reporting entities.

SBA, however, has not fully implemented its critical infrastructure protection program to manage and protect the cyber based infrastructure protection efforts.

Finding 1: The CIPP was not Updated or Utilized to Manage SBA's Infrastructure Protection Efforts

The SBA CIPP had not been updated since September 2001 and it has not been utilized as a tool for managing SBA infrastructure protection efforts. This occurred because the Office of Chief Information Officer (OCIO) had utilized GISRA reporting requirements for management and oversight of the Agency computer security and infrastructure protection efforts. OCIO had concluded that GISRA had superseded PDD 63 as the main infrastructure protection agenda. As a result, some of the mandated requirements of PDD 63 have not been implemented and other requirements were not fully addressed.

According to PDD 63, every Department and Agency was required to develop a plan for protecting its critical infrastructure. Additionally, the Agency CIPP shall be updated every two years as needed to protect critical agency infrastructures.

The original SBA CIPP had identified five broad business areas which represented the Agency's mission essential infrastructure. These five broad business areas included at a high-level the Agency's critical cyber based infrastructure. However, the exact boundaries for the mission essential infrastructure were never fully established. Additionally, changes have taken place since FY 2001 in SBA's critical infrastructure and these changes have not been reflected in the SBA CIPP. These changes included the replacement of SBA's network by its Office Software and Computer Renewal project and the implementation of the Joint Administrative and Accounting Management system. These new systems which are part of SBA's critical infrastructure were implemented in FY 2002.

Recommendation:

1A. We recommend that the Chief Information Officer update SBA's Critical Infrastructure Protection Plan (CIPP) to include the exact boundaries of SBA's mission essential cyber-based infrastructure. This update would identify critical SBA systems by name and their relationship to the five broad boundaries of mission essential cyber-based infrastructure identified in previous CIPP reports.

Finding 2: Full Implementation of CIPP Requirements are Needed to Protect SBA's Critical Infrastructure

SBA has not fully implemented all of its CIPP requirements for protecting its critical cyber-based infrastructure. Updating the CIPP for SBA's current environment is necessary to ensure full protection of SBA's cyber-based infrastructure. As a result, SBA's critical infrastructure may contain areas of weakness which could potentially be exploited.

a. Risk Remedial Plans Continue to Need Improvement

SBA does not include remedial plans in its certification and accreditation documents for its 37 critical systems. The certification and accreditation documents contain the vulnerability assessments required by PDD 63. However, a statement whether the weaknesses are to be accepted, mitigated or corrected; the individuals responsible for correction; and the dates for full correction are not included in the accreditation documents. As a result, there are no formally agreed upon procedures between the accrediting authority and the certifying authority which document the remedial actions necessary to ensure the security and integrity of each SBA critical system.

PDD 63 requires that remedial plans include time frames for implementation, individuals responsible for mitigating or correcting the identified security vulnerability, and the funding required for correcting each deficiency.

SBA has identified risk areas from the 22 risk assessments completed since 2000 on its high priority systems. SBA has also mitigated, corrected or accepted a number of the risks identified in the risk assessments. Additionally, SBA has set-up a tracking data base to identify the status of its risks and facilitate ease of reporting to the Office of Management and Budget (OMB) for its Plan of Action & Milestones (POA&M).

By making remedial plans a part of the accreditation process, system owners will formally confirm their acceptance of the vulnerabilities identified along with a schedule to correct the vulnerabilities, the individuals responsible for correcting the vulnerabilities and the funding required to correct the vulnerabilities.

b. Emergency Management Program

SBA's computer emergency response program did not report computer security incidents to FedCIRC from June 2000 to July 2002 even though SBA had a Memorandum of Understanding with FedCIRC to report security incidents on a quarterly basis. Additionally, SBA did not report security incidents to the Office of Inspector General's Investigations Division even though such reporting was mandated in SBA's CIPP. Finally, a full test of SBA's computer emergency response program was not conducted before the program was implemented. This test might have uncovered these deficiencies before they occurred.

SBA's computer emergency response program was implemented in 2001. At that time, a computer emergency response program manual was finalized with procedures for reporting security incidents to the Agency Computer Security Program Manager. The program reported only one security incident to FedCIRC in FY 2001 although quarterly reporting of all security incidents was required through a MOU with FedCIRC. In July 2002, all known security incidents were reported to FedCIRC for FY 2002.

c. Interagency Coordination Needs Improvement

The CIPP does not require SBA to coordinate with other entities (e.g., other federal agencies; state and local governments; private sector agents, contractors, or partners) to protect its critical infrastructure. Consequently, no interagency coordination plans have been developed or implemented to protect the critical infrastructure from cyber-based attacks.

SBA did complete the discovery phase of a Project Matrix Review. The review determined that SBA systems did not meet the threshold for a full Project Matrix review. The Department of Commerce, therefore, declined to further evaluate SBA using Project Matrix criteria. No SBA system impacts national security, national economic stability, or critical public health and safety. SBA also performed information system security reviews at some of SBA's private sector contractor locations where important services are provided through a cyber-based infrastructure.

d. Resource and Organization Requirements

The CIPP did not require the identification of resource requirements such as information technology (IT) security personnel, to protect its critical infrastructure. Additionally, the CIPP did not require the addition of technical protection such as firewalls and intrusion detection software to protect its critical infrastructure.

SBA determined resource requirements outside of the CIPP. OCIO prepared an IT Security Program budget and submitted it to OMB for fiscal year 2003. OCIO also created an IT Security Budget Request Response worksheet that compared resources required to existing resources. The IT Security Budget Request Response worksheet included categories for anti-virus software, firewall upgrade and maintenance, and

intrusion detection software. However, none of these categories were incorporated into or included in SBA's CIPP.

e. Recruitment, Education, and Awareness

The CIPP did not include a recruitment requirement for IT security personnel. The CIPP also did not include a requirement to identify the education or skill level of its IT security personnel. Education or skill levels required are contained in position descriptions and vacancy announcements. Obtaining skilled and experienced IT security personnel has been difficult. OCIO has established a training and education program for its IT security personnel.

A requirement to make employees aware of the importance of security was included in the CIPP. This requirement has been implemented. OCIO developed an online Security Awareness Training Program that employees and contractors are required to complete annually.

Recommendations:

We recommend that the Chief Information Officer:

2A. Incorporate remedial plans into the Certification and Accreditation process. For the vulnerabilities in each risk assessment, identify whether the vulnerability is accepted, mitigated or corrected. Further, identify who specifically is responsible for correcting or mitigating the vulnerability, time frames for completion and estimated funding requirements.

2B. Include notification of the Office of Inspector General's Investigations Division (OIG ID) when computer emergency network intrusions or attempted intrusions are identified. Additionally, incorporate notification of OIG ID as a standard procedure in OCIO's emergency response program.

2C. Report security incidents to FedCIRC quarterly as required by SBA's Memorandum of Understanding with FedCIRC.

SBA MANAGEMENT'S COMMENTS

SBA's Chief Information Officer agreed with the recommendations. The CIO disagreed with a recommendation in our draft report to test the effectiveness of the computer emergency response system because it has been used several times and has performed as expected. We agreed with the CIO's assessment and the recommendation was withdrawn. See Attachment 1 for a full text of the CIO's response.

* * *

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.**

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 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: December 20, 2002

To: Robert G. Seabrooks
Assistant Inspector General for Auditing

From: Chief Information Officer

Subject: Audit of SBA's Implementation of its Cyber-Based Critical Infrastructure

We have reviewed the above-referenced report. We agree with all of the recommendations with the exception of 2D which recommends that we test the effectiveness of the computer emergency response system. The emergency response system, which involves reporting security incidents to FEDCIRC, has been used several times since its inception and has performed as expected. Due to the nature of the current threat environment (i.e., viruses, hackers, and denial of service attacks) we believe that the system will be used on a regular basis and, therefore, does not need additional "effectiveness testing". However, should we need to modify the current system; we will test the procedure prior to using it in a real situation.

If you require additional information, please contact Howard Bolden, Agency Computer Security Program Manager, at 205-7173.

Lawrence E. Barrett

Lawrence E. Barrett

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	3
U.S. General Accounting Office	1