AUDIT OF SELECTED SBA COMPUTER GENERAL SUPPORT SYSTEMS
AUDIT REPORT NUMBER 4-41

SEPTEMBER 10, 2004

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

AUDIT REPORT
Issue Date: September 10, 2004
Number: 4-41

To: Stephen D. Galvan
Chief Information Officer

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

Subject: Audit of Selected SBA Computer General Support Systems

Attached is the public version of the audit report on Selected SBA General Support Systems issued by Cotton & Company LLP. The report was issued as LIMITED-OFFICIAL-USE. Distribution of the full report requires specific authorization by the SBA Office of Chief Information Officer (OCIO) or SBA Office of the Inspector General (OIG).

The auditors reviewed the selected general support systems settings and configurations against standards issued by the National Institute of Standards and Technologies (NIST), National Security Administration (NSA), Center for Internet Security (CIS) and the manufacturer(s) guidelines.

The Federal Information Security Management Act (FISMA) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with those requirements. Systems that are implemented with secure configurations against a standard benchmark have less vulnerabilities and are better able to thwart network attacks.

The auditors concluded that the selected SBA general support systems and components reviewed contained a number of vulnerabilities which increased the potential for security exposures to exist and go undetected. Additionally, SBA's general support systems and components did not follow a standard system configuration. This generally occurred because SBA had not implemented standard configurations for its general support computer operating systems and components. Nor had SBA ensured that changes to the system configurations were made in a controlled manner. As a result, SBA's general support computer operating systems were potentially vulnerable to unauthorized utilization or inefficient operation.

SBA was in general agreement with the findings and recommendations, but did not provide a written response to the draft audit report. Actions to address the finding and recommendations will be evaluated during the audit resolution process.

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

Please provide us your proposed management decisions on October 31, 2004 on the attached SBA Forms 1824, Recommendation Action Sheet. If you disagree with the recommendations, please provide your reasons in writing.

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

COTTON & COMPANY LLP
auditors • advisors

333 North Fairfax Street • Suite 401 • Alexandria, Virginia 22314 • 703/836/6701 • fax 703/836/0941 • www.cottoncpa.com

September 9, 2004

Subject: Audit of Selected Computer General Support Systems and Controls at the U.S. Small Business Administration

We were engaged to conduct a performance audit of selected general support systems and their associated controls at the U.S. Small Business Administration (SBA). We utilized various best practices from National Institute of Standards and Technology (NIST), National Security Agency (NSA) and Center for Internet Security (CIS) as criteria for this project. The objective of our work was not to provide assurance on overall internal control. Consequently, we do not provide an opinion on internal control.

This report is intended solely for the information and use of SBA management. We would like to express our appreciation to the SBA representatives who assisted us in completing our work. They were always courteous, helpful, and professional.

If you have any questions or comments about this report, please contact me at your convenience. Thank you.

Very truly yours,

COTTON & COMPANY LLP

/S/
Loren Schwartz, CPA, CISA

PERFORMANCE AUDIT OF SELECTED COMPUTER GENERAL SUPPORT SYSTEMS AND CONTROLS AT THE U.S. SMALL BUSINESS ADMINISTRATION

EXECUTIVE SUMMARY

BACKGROUND

This report specifically covers our review of selected computer general support systems including servers, routers and firewalls at SBA headquarters. These items were selected, because they support applications deemed critical to SBA's operations.

OBJECTIVE, SCOPE, AND METHODOLOGY

The overall objective of our audit was to review existing information security controls and identify weaknesses impacting certain components of the general support systems. Our review was not intended to result in the issuance of an opinion, and we do not issue an opinion as defined by the American Institute of Certified Public Accountants. The individual scope, objectives and methodologies of our review(s) are included in the audit report section for each platform or system that we reviewed.

We conducted this review in accordance with Generally Accepted Government Auditing Standards for Performance Audits and accordingly, we performed such tests and other auditing procedures as necessary to meet the review objective. A review of the entire internal control structure was not required for the scope of this audit.

We performed fieldwork from March through June 2004 at SBA headquarters located in Washington, D.C., and at Cotton & Company's Alexandria, Virginia, office.

SUMMARY OF FINDINGS AND RECOMMENDATIONS

SBA's computer general support systems and components (UNIX Solaris, Internal and AT&T Checkpoint Firewalls, and Cisco Routers) contained a number of vulnerabilities which increase the potential for security exposures to exist and go undetected. Additionally, SBA's general support systems and components (UNIX Solaris, Internal and AT&T Checkpoint Firewalls, and Cisco Routers) did not follow a standard system configuration. This generally occurred because SBA had not implemented standard configurations for its general support computer operating systems and components. Nor had SBA ensured that changes to the system configurations were made in a controlled manner. As a result, SBA's general support computer operating systems were potentially vulnerable to unauthorized utilization or inefficient operation.

We recommend that SBA take actions to minimize the risk of security deficiencies by correcting the weaknesses disclosed in this report. Specific recommendations for resolving these weaknesses are detailed in the results section of this report. Due to the types of vulnerabilities identified, certain recommendations are made to SBA systems as a whole including contractor operated systems to ensure that vulnerabilities identified in this report may be addressed within the Agency for all related computer systems and platforms.

Attachment A

REPORT DISTRIBUTION

Recipient	Copies
Associate Deputy Administrator for Management & Administration	1
General Counsel	3
General Accounting Office	1
Office of the Chief Financial Officer Attention: Jeff Brown	1