

**AUDIT OF SBA'S  
EMAIL SYSTEM  
AUDIT REPORT NUMBER 4-42**

**SEPTEMBER 10, 2004**

This report may contain proprietary information subject to the provisions of 18 USC 1905 and must not be released to the public or another agency without permission of the Office of Inspector General.



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

<b>AUDIT REPORT</b>
<b>Issue Date: September 10, 2004</b>
<b>Number: 4-42</b>

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

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

**Subject:** Audit of SBA's Email System

Attached is the public version of the audit report on SBA's Exchange Email system 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 SBA's Exchange Email System settings and configurations against standards issued by the National Security Administration (NSA) specifically for Microsoft Exchange email systems.

The auditors concluded that SBA's Exchange Email system server was vulnerable [FOIA Ex. 2].

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 by 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-[FOIA Ex. 2].

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 SBA's E-Mail System at the U.S. Small Business Administration

We were engaged to conduct a performance audit of the Exchange E-Mail System at the U.S. Small Business Administration (SBA). We utilized the NSA *Guide to the Secure Configuration and Administration of Microsoft Exchange 5.x* 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 THE EXCHANGE E-MAIL SYSTEM AT U.S. SMALL BUSINESS ADMINISTRATION HEADQUARTERS**

## **EXECUTIVE SUMMARY**

### **BACKGROUND**

Cotton & Company LLP was engaged by the Office of the Inspector General, U.S. Small Business Administration (SBA), to conduct an audit of certain components of SBA's general support system. This report specifically covers our review of the SBA Exchange E-Mail System at SBA headquarters. The Exchange E-Mail System is deemed critical to the 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 Exchange E-Mail System. 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. We reviewed the configurable settings, management controls, and policies and procedures surrounding the email exchange server at SBA headquarters. We used the following criteria for our review:

*NSA Guide to the Secure Configuration and Administration of Microsoft Exchange 5.x.*

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**

[FOIA Ex. 2].

We recommend that SBA take actions to minimize the risk of security deficiencies by correcting the deficiencies disclosed in this report. Specific recommendations are detailed in the results section of this report.

**PUBLIC REPORT DISTRIBUTION**

<b><u>Recipient</u></b>	<b><u>Copies</u></b>
Associate Deputy Administrator for Management & Administration	1
General Counsel	3
Government Accountability Office	1
Office of the Chief Financial Officer Attention: Jeff Brown	1