

**AUDIT OF SBA'S [FOIA ex. 2]  
ELECTRONIC FORMS SYSTEM**

**AUDIT REPORT NUMBER 5-25**

**SEPTEMBER 23, 2005**

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

**AUDIT REPORT**

**Issue Date: September 23, 2005**

**Number: 05-25**

**To:** Delorice P. Ford  
Chief Privacy Officer

Charles McClam  
Acting Chief Information Officer

[FOIA ex. 6]

**From:** Robert G. Seabrooks  
Assistant Inspector General for Audit

**Subject:** Audit of SBA's [FOIA ex. 2] Electronic Forms System

We have completed an audit of SBA's [FOIA ex. 2] electronic forms system. The audit identified one finding and two recommendations. The audit results are presented below.

### **BACKGROUND**

SBA's [FOIA ex. 2] electronic forms system was implemented in 1997 to automate Agency workflow and is currently in use. [FOIA ex. 2] provides SBA employees with an electronic alternative to paper forms by means of database technology. This technology allows users to access, fill and save electronic forms to a specified location, either public or private. [FOIA ex. 2] is no longer supported by its vendor, [FOIA ex. 2] and no new official government forms are being converted to [FOIA ex. 2]

### **OBJECTIVES, SCOPE AND METHODOLOGY**

The objective of this audit was to determine whether SBA's [FOIA ex. 2] electronic forms system allows for the inappropriate disclosure of personally identifiable information. [FOIA ex. 2]

To accomplish these objectives we reviewed applicable laws and regulations, conducted interviews with SBA management responsible for the administration of

[FOIA ex. 2] and tested for disclosure at both SBA Headquarters and Field Office locations. We also interviewed SBA's Privacy Officer to establish a legal perspective on the disclosure of private information on SBA employees through [FOIA ex. 2]. Fieldwork was performed at SBA's Central Office in Washington, DC, National Guaranty Purchase Center in Herndon, VA and SBA Offices in Glendale, CA, Forth Worth, TX and Atlanta, GA, from March through August 2005. Our audit was conducted in accordance with Generally Accepted Government Auditing Standards.

## AUDIT RESULTS

We determined that SBA's [FOIA ex. 2] electronic forms system was susceptible to unauthorized disclosure of personal or Privacy Act information. This information included individual SBA employee's names, employee identifier or social security numbers, addresses, phone numbers and dates of birth. The lack of controls to prevent unauthorized disclosure of these records is a violation of the Privacy Act.

### **Finding 1: SBA's [FOIA ex. 2] System was not Secure Against Unauthorized Disclosure**

SBA's [FOIA ex. 2] electronic forms system did not have adequate security controls to prevent against unauthorized disclosure of personal and Privacy Act information of Agency personnel.

[FOIA ex. 2]

The Privacy Act of 1972 defines the term "record" to mean any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. Additionally, the Act identifies that no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.

We determined that the following SBA [FOIA ex. 2] system electronic forms contain information maintained by the agency on SBA employees [FOIA ex. 2]

- [FOIA ex. 2]
- [FOIA ex. 2]
- [FOIA ex. 2]
- [FOIA ex. 2]

These forms were selected for audit testing to [FOIA ex. 2]

Access to sensitive data for each of the forms was tested at: (1) SBA Headquarters in Washington, DC, (2) Glendale, CA, (3) Fort Worth, TX, and (4) Herndon, VA. In all locations tested, we were able to obtain personal or Privacy Act information on current or past SBA personnel via the [FOIA ex. 2] System. [FOIA ex. 2]

The Office of Chief Information Officer owns and operates SBA's [FOIA ex. 2] system and is responsible for ensuring that SBA employees are adequately trained to use the system

[FOIA ex. 2]

**Recommendation:**

- 1.A** We recommend that the Acting Chief Information Officer implement a replacement capability and fully discontinue the use of the [FOIA ex. 2] system.
- 1.B** We recommend that the Chief Privacy Officer identify the [FOIA ex. 2] System as in violation of the Privacy Act until the system is repaired or replaced.

**Management Comments:**

SBA did not provide formal management comments to this report, but met with us on September 9 and September 21, 2005. SBA fully agreed with the draft report. The Chief Privacy Officer identified that [FOIA ex. 2] would be identified as in violation of the Privacy Act in the current years' report.

[FOIA ex. 2]

SBA had converted [FOIA ex. 2] estimated full replacement of the [FOIA ex. 2] System by December 31, 2005. SBA plans to issue an Information Notice in the near future as part of their actions to close this issue.

**Evaluation of Management's Comments:**

SBA's comments were responsive to the recommendations. We modified the initial recommendations from the draft report to reflect that SBA decided to replace the [FOIA ex. 2] system rather than repair it.

\* \* \*

The findings included in this report are the conclusions of the Auditing Division based upon the auditors' review of the [FOIA ex. 2] electronic forms system. 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 Jeffrey R. Brindle, Director, Information Technology and Financial Management Group, at (202) 205- [FOIA ex. 2]

Attachments