AUDIT OF
E-APPLICATION SYSTEM

Report Number: 7-31
Date Issued: September 27, 2007

Memorandum

U.S. Small Business Administration
Office of Inspector General

To: Calvin Jenkins
Deputy Administrator for Government Contracting
and Business Development

Date: September 27, 2007

From: Debra S. Ritt
Assistant Inspector General for Auditing
/S/ original signed

Subject: Audit of E-Application System
Report 7-31

This report presents the results of our audit of the Small Business Administration's (SBA) E-Application system, an internet-based system that processes applications for the 8(a) and Small Disadvantaged Business (SDB) certification programs. The system, which was implemented in September 2004, is licensed to SBA and operated by the contractor, and interfaces with SBA's Electronic 8(a) Review System.[1] The goal of the E-Application system is to reduce the application processing time by allowing applicants to receive and submit 8(a) and SDB applications electronically, and by providing 8(a) program personnel with a tool to quickly evaluate and approve applications and identify those applications which require further review.

The OIG conducted an audit of the E-Application system to determine whether: (1) data stored in E-Application complies with applicable laws, rules and regulations governing security of government data and Personally Identifiable Information (PII); and (2) controls over data transfer between E-Application and SBA's Electronic 8(a) Review system are sufficient to ensure the complete and accurate transfer of information.

To accomplish our audit objectives, we reviewed documentation and the vendor contract, interviewed program personnel, and analyzed data files. We evaluated

[1] SBA's Electronic 8(a) Review System temporarily replaced SBA's Servicing and Contracting System/Minority Enterprise Development Central Office Repository (SACS/MEDCOR). This temporary system will be permanently replaced by a new Business Development Management Information System, which is under development.

the extent to which E-Application was in compliance with security requirements specified by the Federal Information Security Management Act (FISMA);[2] Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems;* and Special Publication 800-53, *Recommended Security Controls for Federal Information Systems,* issued by the National Institute of Standards and Technology (NIST). We conducted the audit between April and June 2007 in accordance with *Government Auditing Standards* as prescribed by the Comptroller General of the United States.

RESULTS

Our review determined that the system's security safeguards over sensitive government data were inadequate and did not meet FISMA, FIPS or NIST requirements. For example, SBA had not developed or implemented standard security operating procedures for E-Application. Additionally, the contractor that operates the system lacked data backup and recovery capability, leaving SBA data vulnerable to loss or misuse.

System controls were also insufficient to ensure the complete and accurate transfer of information from E-Application to SBA's Electronic 8(a) Review System. For example, existing system interfaces did not have sufficient data validation and verification controls to ensure the integrity of data transferred from E-Application to SBA's Electronic 8(a) Review System. These controls were not required in the contract to build the E-Application system. As a result, SBA lacks assurance that complete and accurate data is transferred from E-Application to its Electronic 8(a) Review System.

E-applications Lacked Adequate Security Operating Procedures and Backup Capability

FISMA and FIPS Publication 200 require formalized system security plans for Federal information systems, including contractor hosted systems. However, reviews performed by SBA since 2004 have identified significant unresolved security vulnerabilities in the E-Application system. For example, an SBA review conducted after deployment of the E-Application system disclosed that the vendor had not defined and implemented standard operating procedures to ensure security of the system. SBA reported this condition as a vulnerability and required the vendor to develop procedures to implement SBA's security policies by January 31, 2005. As of the date of this audit, security procedures had not been developed or implemented, and SBA has not held the contractor accountable.

---

[2] Public Law 107-347

Further, in 2006, the vendor moved the hosting site for E-Application from an approved service provider to an alternate site. After learning of the move, SBA performed a site visit and identified the following unremediated data backup and disaster recovery vulnerabilities, which placed E-Application data at risk of misuse or loss:

- No documented plan to bring the system up in the event of a disaster;
- No contract agreement for a backup storage site; and
- No contract agreement for an alternate data processing site.

Based on these vulnerabilities, E-Application did not meet the security requirements of FISMA, FIPS Publication 200, and NIST Special Publication 800-53. These standards require that Federal information systems have a continuity of operations plans and backup data storage and processing capabilities.

E-Application Lacked Controls to Ensure the Integrity of Data Transferred

Office of Management and Budget Circular A-123, *Management's Responsibility for Internal Control,* requires the establishment of controls to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. In addition, controls should be established at an application's interfaces to verify inputs and outputs. Despite these requirements, system controls were not in place to continuously validate the completeness and integrity of data transferred between E-Application and SBA's Electronic 8(a) Review System. Further, we compared data in E-Application with information that had been transferred to SBA's Electronic 8(a) Review System and found that the two systems did not always reconcile.

SBA's contract with the E-Application vendor did not require that controls be implemented to ensure the completeness and integrity of data transfers from E-Application to SBA's Electronic 8(a) Review System. This requirement was not incorporated into the vendor contract because SBA originally intended to strictly use E-Application as a data capture system for paperless 8(a) applications and did not plan on transferring data in E-Application to other SBA systems. Without such controls, SBA has no assurance that data transferred from E-Application to SBA's Electronic 8(a) Review System is complete and accurate.

To address this issue, prior to our audit, SBA hired a contractor to perform a data cleansing of applicant data in E-Application and SBA databases and to establish

procedures to perform automated daily validation of new and modified data items. However, the contractor was unable to complete this task because of incomplete E-Application system documentation of data structures, and data mapping.

Without data validation and verification controls, SBA has reduced assurance that complete 8(a) applicant data is transferred from E-Application to its Electronic 8(a) Review System.

RECOMMENDATIONS

We recommend that the Deputy Administrator for Government Contracting and Business Development:

1. Modify the existing contract with the vendor to require the development of security procedures to implement SBA's security policies, a disaster recovery plan, a backup data storage site, and an alternate data processing site.

2. Establish appropriate controls to ensure data entered into E-Application is accurately transferred to the Electronic 8(a) Review System.

3. Validate the accuracy of data already transferred from E-Application to the Electronic 8(a) Review System.

AGENCY COMMENTS

On September 4, 2007, we provided SBA with a draft of the report for comment. On September 26, 2007, SBA provided its formal response, which is contained in its entirety in Appendix I. SBA agreed with our findings and recommendations and stated that it will migrate the E-Application system from the vendor site to OCIO premises within the next 60 to 90 days. This migration will place the E-Application System in an environment that is compliant with security, data backup and disaster recovery requirements.

SBA also stated that it will implement an enhanced version of E-Applications that includes an annual review component and will retire the Electronic 8(a) Review System. This will obviate the need for data transfers.

OFFICE OF INSPECTOR GENERAL RESPONSE

We believe the actions proposed by SBA on the OIG recommendations are responsive. However, we believe the Agency should establish target dates for completing final action on recommendations 2 and 3.

ACTIONS REQUIRED

Because SBA provided no target dates for completing proposed actions for recommendations 2 and 3 we are requesting that target dates be provided by October 29, 2007.

We appreciate the courtesies and cooperation of the Small Business Administration Government Contracting and Business Development representatives during this audit. If you have any questions concerning this report, please call me at (202) 205-[Exemption 2] or Jeffrey R. Brindle, the Program Director, at (202) 205-[Exemption 2].

Memorandum

U.S. Small Business Administration
Office of Inspector General

To: Debra S. Ritt
Assistant Inspector General for Auditing

Date: September 26, 2007

From: Calvin Jenkins [Exemption 6]
Deputy, General Contracting and
Business Development

Subject: Response to Audit of E-applications System
Project No. 7019

The results of the subject audit pertain to the current system, which is hosted in an off-site facility by the vendor who originally developed the system. These results paint a picture of a system that displays serious deficiencies in terms of system security, data security, recovery and contingency planning and execution. We do not contest your assessment of these deficiencies. However, they will be rendered moot by our plan to migrate the system to the OCIO premises in the next sixty to ninety days.

At that time, OCIO will take over operation of the system, and will assume responsibility for all aspects of system and data security, as well as recovery and contingency planning and execution. Once migrated in-house, the system will be subject to all OCIO-approved standards and procedures for the above (and all) aspects of system operation. The vendor will enjoy absolutely NO access to the production system after this migration. The vendor will convey program updates to the system via email to OCIO. The latter will then apply the updates to the production system, only after subjecting the new code in a separate staging environment to OCIO-approved rigorous testing and QA procedures.

The audit also mentions that the data transfer between the E-Applications system and the Electronic 8(a) Review system suffers from the absence of adequate continuous data verification and validation controls that would otherwise ensure

the accuracy, completeness and integrity of the transfer. This exposure will also disappear with the execution of our plan, as it calls for the full development, testing and implementation of the embryonic Annual Review functionality currently dormant in the 8a SDB application, and the concomitant retirement of the separate Oracle-based Electronic 8 (a) Review system. Correspondingly, when the latter system is retired, the need for the data transfer will also disappear.

Thank you for the thorough and meticulous effort that your analysis reflects. It has helped us identify and address key areas where the E-Applications system can be dramatically improved. We look forward to working with you to ensure that the system meets all applicable security standards in the future.