The Library of Congress

Office of the Inspector General

Office of the Librarian

Development Office

Information Technology Review of the Raiser's Edge Software Program

Review Report No. 2006-IT-302
December 2007

UNITED STATES GOVERNMENT LIBRARY OF CONGRESS

Memorandum ***Office of the Inspector General***

TO: James H. Billington
Librarian of Congress

December 20, 2007

FROM: Karl W. Schornagel
Inspector General

SUBJECT: Information Technology Review of the Raiser's Edge Software Program
Review Report No. 2006-IT-302

This transmits our final report on the Raiser's Edge Software Program. The Executive Summary begins on page *i*, and complete findings and recommendations appear on pages 4 to 7.

The Development Office's response to our draft report is briefly summarized in the Executive Summary and in more detail after individual recommendations. Its complete response is included as an appendix to the report.

Based on the written comments to the draft report, we consider all of the recommendations resolved. Please provide within 30 calendar days, an action plan addressing implementation of the recommendations, including implementation dates, in accordance with LCR 211-6, Section 11.A.

We appreciate the cooperation and courtesies extended by the Development Office staff during the review.

cc: Chief Operating Officer

⏩TABLE OF CONTENTS

▶▶EXECUTIVE SUMMARY

The Development Office of the Library of Congress was established under the leadership of the present Librarian in 1987. Through the office, the Library seeks support from individuals, corporations and foundations that wish to play a key role in sharing, cultivating and celebrating knowledge and creativity. Library fundraising focuses on support for special acquisitions, preservation of Library collections, cultural and educational outreach programs, and various other projects and activities. Private donations to the Library have totaled approximately $307 million since the Development Office was established. The office uses Raiser's Edge, a commercial software product, as a tool for managing fundraising activities, including tracking receipts and managing special event information.

This report provides the results of our assessment of the application controls the Library uses in the operation of Raiser's Edge. We sought to determine whether the controls applied are commensurate with the level of protection required for the system's information and whether the system is operated according to Library of Congress Regulation (LCR) 1620, Information Technology Security Policy of the Library of Congress and applicable Information Technology Security Directives. We concluded that the level of controls applied in the operation of Raiser's Edge appropriately corresponds to the level of protection required for the data the system processes. However, we identified actions that should be taken to enhance the protection of system information. Specifically, we recommend that:

- [redacted]
- the Raiser's Edge system undergo the Certification and Accreditation evaluation required by LCR 1620 as soon as possible; and
- system managers regularly review Raiser's Edge's data to identify errors or data that is being inappropriately used.

Management generally agreed with our findings and recommendations.

INTRODUCTION

This report is the first in a series of Office of the Inspector General (OIG) reviews of various Library applications and systems. These reviews will focus on the effectiveness of management, operational, and technical controls that apply to a system's operation.

Criteria guiding OIG's reviews include the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) Circular A-130, the Library's Information Technology (IT) Security Policy, Information Technology Services (ITS) Security Directives, National Institute of Standards and Technology (NIST) Special Publications, Federal Information Processing Standards (FIPS), and best practices of the IT industry. Although the Library is not required by statute to follow some of these criteria, they represent best practices in the operation of an IT security program, and the Library has adopted many of them.

The Library acquired Raiser's Edge in 1998 for $13,670. The annual fee for the associated maintenance agreement is currently $26,624, which includes licenses for 40 concurrent users.

[redacted]

Raiser's Edge includes several modules to track fundraising donations, gifts, and events. The application also provides reports regarding administrative and managerial activities.

Although the application has web capabilities, the Library does not use those features. Raiser's Edge has no automated interfaces with other automated Library systems for exchanging data or information.

[1] Version 7.82, due at the end of 2007, will be available to the Library under the agreement. [redacted].

Data is generally entered into Raiser's Edge manually and transferring data from Raiser's Edge to other programs is likewise, a manual effort. There is currently no remote access to the application from outside the Library.

⏩OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this review were to review the input, processing, and output functions of Raiser's Edge to ensure that: (1) only complete, accurate, and valid data are entered and updated to the computer system, (2) processing of constituent gift, campaign, fund, and appeals information by the application is accurate, (3) processing efficiency meets management expectations, and (4) the integrity and confidentiality of data are maintained.

We tested applicable system controls to assess whether they were functioning effectively. We also evaluated the control environment to determine whether control objectives had been achieved.

During the course of our assessment, we:

- developed a thorough understanding of the control environment by reviewing applicable policies and procedures of the Development Office and the Raiser's Edge software application system;

- reviewed systems documentation for the Raiser's Edge application;

- interviewed key personnel involved with the input, processing, and output of the software application system; and

- reviewed relevant Library of Congress Regulations (LCRs), Code of Federal Regulations, and publications issued by the National Institute of Standards and Technology (NIST).

We performed our fieldwork from June 2006 through February 2007 and from July 2007 through August 2007. Our work was interrupted due to staff turnover and other, higher priority projects.

We conducted our review in accordance with Generally Accepted Government Auditing Standards issued by the Comptroller General of the United States (the "Yellow Book"), 2003 edition, and LCR 211-6, *Functions, Authority, and Responsibility of the Inspector General*.

FINDINGS AND RECOMMENDATIONS

We concluded that the overall level of controls applied in the operation of Raiser's Edge appropriately correspond to the risks of protecting the system's data. However, weaknesses in the application of some controls should be addressed to provide greater security for the system's information. Significant areas requiring attention include:

- [redacted]
- system certification and accreditation; and
- system capabilities to assist data monitoring activities.

The following sections provide our assessments of these issues and include three recommendations to strengthen the system's security.

I. Automated [redacted]

[redacted]

Among other things, [redacted]

[redacted]

[redacted]

Recommendations

We recommend that:

a. the Development Office document [redacted]

Management Response

[redacted]

II. Certification and Accreditation is Required for Raiser's Edge

A certification and accreditation (C&A) evaluation has not been performed on the Raiser's Edge system as required by the Library's IT security policy, LCR 1620. However, the system is scheduled for such an evaluation at the end of this year.

Under the IT policy, all Library service and infrastructure units are responsible for the C&A of all IT systems under their operational control every three years. The certification process identifies weaknesses in operating the application, system, or facility and evaluates the potential vulnerabilities of these weaknesses. Accreditation is the formal declaration by the Designated Approving Authority (DAA) that an automated information application, system, or facility is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is a business decision balancing the costs of the level of safeguards and the level of need for confidentiality, availability, and integrity of the information.

The C&A process ensures that the responsible manager with oversight on the system has a clear picture of the risk involved with that system, and the mitigation that can be employed to minimize the risk to the system, the organization, and the government agency.

The Office of the Inspector General interviewed the system owner and performed an initial system characterization and risk assessment of the Raiser's Edge system. Based on the assessment, we concluded that the security threat for the system was moderate. However, the risk assessment was not performed at the level of detail normally involved with a standard C&A evaluation. Such a standard evaluation of Raiser's Edge may reveal system weaknesses that are not identified in this report. We note that the Library has used the application since 1998 without incident.

Recommendation

We recommend that the Director of the Development Office ensure that the Raiser's Edge system undergo the Certification and Accreditation evaluation required by LCR 1620 as soon as possible.

Management Response

None

III. Reviews of the Server Logs Are Needed

The system's managers do not review Raiser's Edge system transaction logs for suspect data events to identify data that is being inappropriately accessed. This monitoring procedure is not performed primarily because the system does not make data conveniently available in logs for management review. As a result, the reliability of the system's data is questionable.

It is common industry practice for management to review data captured in system logs to ensure the integrity of a system. Moreover, the ability to generate reports or logs is built into the majority of modern applications. However, in Raiser's Edge's case, this capability is not available at the application level.

Nevertheless, it is still possible for the system's managers to review some of Raiser's Edge data. Because Raiser's Edge resides on a Microsoft Structured Query Language (SQL) server, system managers could review the system's data that resides in the transaction log built into the SQL server. SQL server utilities, including Lumigent Log Explorer and Audit DB, could assist system managers identify changed records and target suspect data events.

Recommendation

We recommend that system managers for Raiser's Edge regularly review the system's transaction logs for suspect data events to identify data that is being inappropriately accessed.

Management Response and OIG Comments

Management wished to clarify that the application data entered into the system was being reviewed daily. We acknowledge this fact; however, we reiterate our finding that system data events should be reviewed on a regular basis.

⏵⏵CONCLUSION

This review of the controls applied in the operation of Raiser's Edge is one in a series of OIG reviews of various Library systems. These reviews are designed to assist Library management by focusing on the effectiveness of management, operational, and technical controls that apply to a system's operation.

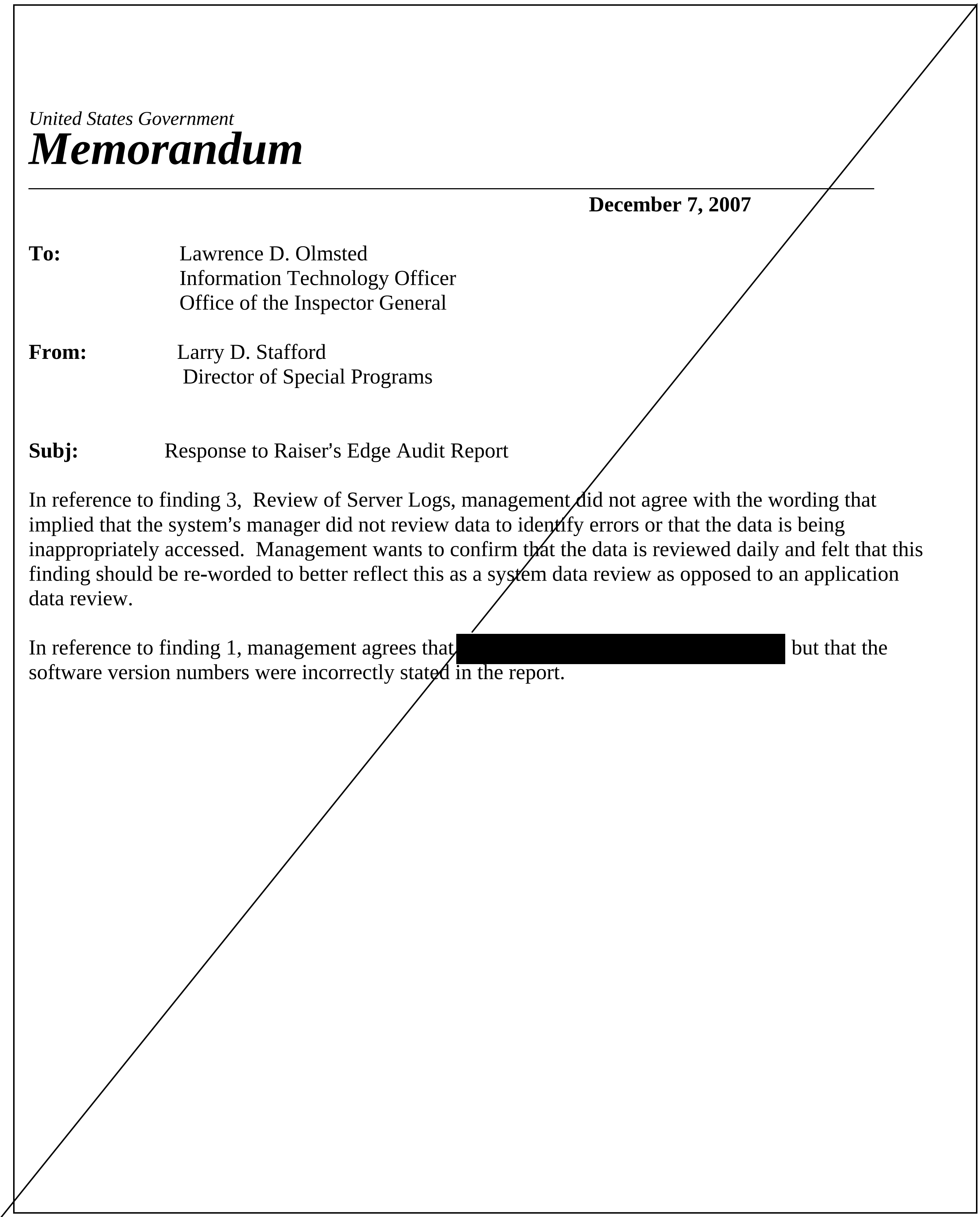
We concluded that the level of controls established for Raiser's Edge's operation are commensurate with the level of protection required for the information the system processes. Moreover, staff responsible for entering, maintaining, and protecting system data have a good understanding of the system's procedures and responsibly ensure those procedures are properly implemented.

However, we also concluded that weaknesses in the application of some controls should be addressed to provide greater security for the system's information. This report provides recommendations to address significant weaknesses that we identified. Most importantly, we recommended that Raiser's Edge undergo a standard C & A evaluation as soon as possible to confirm that the system's safeguards provide the level of security needed to adequately protect the system's information.

Major Contributors to This Report

Nicholas G. Christopher, Assistant Inspector General for Audits
John Kane, Senior Auditor
Lawrence Olmsted, Information Technology Specialist

APPENDIX: MANAGEMENT RESPONSE



United States Government

Memorandum

December 7, 2007

To: Lawrence D. Olmsted
Information Technology Officer
Office of the Inspector General

From: Larry D. Stafford
Director of Special Programs

Subj: Response to Raiser's Edge Audit Report

In reference to finding 3, Review of Server Logs, management did not agree with the wording that implied that the system's manager did not review data to identify errors or that the data is being inappropriately accessed. Management wants to confirm that the data is reviewed daily and felt that this finding should be re-worded to better reflect this as a system data review as opposed to an application data review.

In reference to finding 1, management agrees that [redacted] but that the software version numbers were incorrectly stated in the report.