

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

**TO:** James H. Billington  
Librarian of Congress  
March 15, 2002

**FROM:** Karl W. Schornagel  
Inspector General 

**SUBJECT:** Results of FY 2001 Financial Audit of the Library of Congress

The independent firm of Clifton Gunderson LLP, retained by the Office of the Inspector General to audit the Library of Congress' FY 2001 financial statements, has completed its task and issued the attached consolidated report on the Library's financial statements taken as a whole, internal control over financial reporting, compliance with laws and regulations, and management's assertion about the effectiveness of internal control over safeguarding collection assets.

We are pleased to report for the sixth consecutive year that in the auditor's unqualified opinion, the financial statements, including the accompanying notes, present fairly, in all material respects, the financial position of the Library of Congress in conformance with U.S. generally accepted accounting principles. However, there are two internal control reportable<sup>1</sup> conditions, two reportable instances of noncompliance with laws and regulations, and limitations in internal control over collection assets. The paragraphs that follow summarize the independent auditor's assessments of these issues.

**Internal Control Over Financial Reporting**

There are no material weaknesses in internal control over financial reporting (excluding safeguarding collection assets discussed on the next page) although there are two significant information technology-related deficiencies that could adversely affect the Library's ability to meet its financial management objectives.

First, security practices over information technology (IT) systems need to be improved. The Library-wide security program needs to be enhanced to comply with the 1987 Computer Security Act by establishing additional policy and upgrading the IT management structure. Specific topical areas needing improvement include application changes, systems development,

---

<sup>1</sup> According to federal financial audit criteria, audit findings are classified as to their importance. A reportable condition in the auditor's opinion represents a significant deficiency in the design or operation of an internal control which could adversely affect the Library's ability to meet its internal control objectives. A material weakness represents a more serious condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that errors, fraud, losses, or noncompliance in amounts that would be material to the financial statements may occur and not be detected promptly by employees in the normal course of performing their duties.

transitioning systems from a testing status to a production environment, physical and logical access controls, certification and accreditation of sensitive systems, and segregation of duties.

Second, the Library needs to establish a comprehensive disaster recovery program to maintain service continuity, minimize the risk of unplanned interruptions, and recover critical operations should interruptions occur. Specifically, the Library should develop a Library-wide disaster recovery plan, establish emergency response and operating procedures, segregate its alternate computer processing location, and develop written policies for performing backups.

### **Compliance With Laws and Regulations**

There are two reportable instances of noncompliance. First, as noted in prior years the Library has operated 10 revolving gift funds beyond the scope of its authority. Legislation authorizing these funds (and bringing the Library into compliance) has been enacted and was effective at the beginning of FY 2002. Second, during FY 2001 and 2000, the Library was not in compliance (as reported by the Office of Compliance) with the Congressional Accountability Act of 1995 requiring maintenance of specified safety standards.

### **Management's Assertion About the Effectiveness of Internal Control Over Safeguarding Collection Assets**

Although the valuation of the collection of heritage assets is not reported in the Library's balance sheet, the assets represent an important stewardship responsibility requiring a system of internal control to ensure accountability. To this extent, the Library includes in its annual financial statements a stewardship report and makes an assertion about the effectiveness of the internal control.

The results of the audit indicate that the Library fairly stated that it couldn't provide reasonable assurance that the internal control structure over safeguarding collection assets against unauthorized acquisition, use, or disposition was completely effective as of September 30, 2001 for the collections taken as a whole because of material internal control weaknesses. Based on the auditor's examination, the Library fairly asserted that newly acquired non-rare monographs (a major portion of the general collection) were under bibliographic, inventory, and preservation control when circulated outside the Library as of September 30, 2001. The Library could not assert that the newly acquired non-rare monographs were under completely effective internal control during internal processing and storage life cycles.

The Office of the Inspector General appreciates the courtesies and cooperation extended to the independent auditors and to our staff during the audit.

Attachment

cc: Deputy Librarian  
Director, Financial Services Directorate



## Independent Auditor's Report

Inspector General  
Library of Congress

In our audit of the Library of Congress (Library) for fiscal year 2001 and 2000, we found

- the financial statements are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles,
- no material weaknesses in internal control over financial reporting (excluding safeguarding collection assets) and compliance and its operation, although internal control should be improved,
- reportable noncompliance with laws and regulations we tested, and
- management fairly stated that (1) the Library cannot provide reasonable assurance that the internal control structure over safeguarding collection assets against unauthorized acquisition, use, or disposition was completely effective as of September 30, 2001, for all of the Library's collections; and (2) newly-acquired non-rare monographs (a major portion of the general collections of the Library) are under bibliographic, inventory and preservation controls when any item is circulated outside the Library and management cannot assert that inventory controls are fully implemented during the in-processing and in-storage life-cycles as of September 30, 2001.

The following sections discuss in more detail (1) these conclusions and our conclusions on Management's Discussion and Analysis and other supplementary information and (2) the scope of our audit.

### Opinion on Financial Statements

The financial statements including the accompanying notes present fairly, in all material respects, the financial position of the Library as of September 30, 2001 and 2000, and its related statements of net costs, changes in net position, budgetary resources, and financing for the years then ended in conformity with U.S. generally accepted accounting principles.

As discussed in Note 23 to the financial statements, *Budgetary Resources*, the Library changed its fiscal year 2001 presentation of the Combined Statement of Budgetary Resources to be more consistent with budget execution information reported in the Budget of the United States Government, and restated its presentation of fiscal year 2000 budgetary resources for consistency.

Centerpark I  
4041 Powder Mill Road, Suite 410  
Calverton, Maryland 20705-3106  
tel: 301-931-2050  
fax: 301-931-1710

[www.cliftoncpa.com](http://www.cliftoncpa.com)

### Consideration of Internal Control

We considered internal control over financial reporting and compliance.

We do not express an opinion on internal control over financial reporting and compliance because the purpose of our work was to determine our procedures for auditing the financial statements and to comply with OMB audit guidance, not to express an opinion on internal control. However, our work identified the need to improve certain internal controls, as described below. The weaknesses in internal control, although not considered material weaknesses, represent significant deficiencies in the design or operation of internal control, which could adversely affect the Library's ability to meet the internal control objectives listed in the objectives, scope, and methodology section.

A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that errors, fraud, or noncompliance in amounts that would be material to the financial statements may occur and not be detected promptly by employees in the normal course of performing their duties. Our internal control work would not necessarily disclose all material weaknesses.

\*\*\*\*\*

### REPORTABLE CONDITIONS

#### 1. SECURITY PRACTICES OVER INFORMATION TECHNOLOGY SYSTEMS NEED TO BE IMPROVED

There are several areas regarding the enterprise wide security program that need to be improved. This program should establish a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate, responsibilities may be unclear, misunderstood or improperly implemented or existing controls may be inconsistently applied. Our audit found that the Library's information systems environment remained threatened by weaknesses in several information protection control structures. The presence of these weaknesses increases the risk that the Library's data and equipment are not properly safeguarded. The details of the matters are as follows:

- **Entity-Wide Security Program is inadequate.** The Library of Congress does not have a documented entity-wide security program in accordance with the Computer Security Act of 1987 as interpreted by the Library's Computer Security Policy. The Library does not have a well-organized Information Security Management Structure to make decisions on how to manage and protect its diverse Information Technology Resources. The Library needs a Director of Information Technology Services whose responsibility per the Library Computer Security Policy includes amongst other duties, "...to develop, manage and coordinate the Library's security program." These are proactive measures that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems on an ad hoc basis, or after a violation has been detected.

- **Application change controls and system development require enhancement.** Certain controls over the modification of application software programs are deficient. These controls should be designed to ensure that only authorized programs and modifications are implemented. Without proper controls, there is a risk that security features could be inadvertently omitted or turned off, or that processing irregularities or malicious code could be introduced.
  - There were no written standards to control production programs as they progress through testing to production. The lack of controls may result in inefficient or inadequate testing or introducing production programs that do not meet management's criteria.
- **The Library does not maintain adequate controls of its test and production libraries.** Application Developers for one sub-system can move application modifications/upgrades from the test to the production environment without review of quality assurance. In other words, the same person who did the upgrade can carry out program migration into the production environment.
- **The Library's physical and logical access controls need to be enhanced.** Certain access controls require modification in order to provide a more secure environment. Access controls should provide reasonable assurance that the information technology resources (data files, application programs and computer facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. These controls include but are not limited to: controls over physical access to information technology resources, and controls that prevent unauthorized access to sensitive program and data files. The Library lacks management policies to manage access controls for applications and system software. There are no written standard access control policies. During our review of access controls, we found that:
  - Certain employees who had left the Library were still listed as active users of system resources and had not had their access rights revoked.
  - The security package that protects the financial application is obsolete and is no longer supported by the vendor.
  - No formal procedures have been developed addressing physical access to the data center. For example:
    - Ingress and egress to/from the Library's Data Center by visitors, third party contractors and housekeeping staff is not closely monitored. The visitors log usually had no visitor's names nor initial of the admitting party, it occasionally had time of entry but time of exit was rarely noted.
    - There was no maintenance log to verify that scheduled maintenance of the Library's data center equipment had been done. Procedures for assigning Data Center access badges to maintenance staff (AOC employees) and other third party contractors need to be formalized.

- Third parties should not be allowed to use the Data center as office space. If this cannot be avoided, such persons should be closely supervised. This is the case of certain contractors doing Windows 2000 upgrades to employee terminals. There were no records of the level of security granted them nor the serial number of the badges assigned to them.
- There are no procedures in place to safeguard new or unused keycards/badges.
- **Application security controls should be strengthened.** Application controls do not include a program for the certification and accreditation of sensitive applications. Management control over computer security was impaired by the lack of a process for the technical evaluation of the security of sensitive applications. Not addressing these control weaknesses increases the risk of unauthorized access to certain sensitive applications and data without being detected.
- **Segregation of duties should be enhanced.** Work responsibilities should be segregated so that one individual does not control all critical stages of a process. Often, segregation of duties is achieved by splitting responsibilities between two or more organizational groups. The extent to which duties are segregated depends on the size of the organization and the risk associated with its facilities and activities. Below is a summary of some of the control weaknesses noted at the Library of Congress.
  - The following incompatible authority is vested in the System Administrator of one of the Library's support sub-systems. Capacity to: customize configuration settings, set up users in the application, build profiles, set user passwords, add/modify/delete user profiles, add/modify/delete groups, add/modify/delete users and input fund data.
  - There is no hierarchical oversight or monitoring of the activity of System Administrators. Reviewing system-generated logs that record application access, usage and violation reports (where this feature is turned on) is equally the prerogative of the System Administrator or someone designated by this person.
  - System Administrators for certain sub-systems assign user passwords. These passwords while not secured in encrypted files cannot be changed by the users.
  - Users of certain Library Support sub-systems have the authority to (a) initiate purchase orders and (b) validate or approve these orders.
  - One of the new features incorporated in a sub-system upgrade allows users the possibility to modify purchase orders after these purchase orders have been approved and funds obligated. This is a potentially delicate feature, which should be discouraged. If it is imperative that it be incorporated in this upgrade, the assignment and use of this feature should be closely monitored.

Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed, improper program changes could be implemented, and that computer resources could be damaged or destroyed.

**Recommendations:**

We recommend the following:

- Senior management make security of its information technology resources a high priority and allocate adequate resources and personnel. Library management should develop an administrative structure to implement the security program throughout the organization and to ensure that Library Information Technology resources are restricted to authorized individuals and that critical data is protected.
- Implement more rigorous access regulations with regards to the main information processing facility of the Library. Regulate custody over unused keycards, restrict entry into the data center and supervise third parties who have been temporarily granted office space in the data center. In addition, deactivate the access privilege of users ID's who have left the Library's employment.
- Establish a program for the certification and accreditation of major application systems and general support systems in accordance with the Federal Information Processing Standards Publication (FIPS PUB) 102 "Guideline for Computer Security Certification and Accreditation," and
- Develop a written Systems Development Life Cycle methodology. Also, develop and implement controls for system software changes and prohibit developers from migrating test programs into the production environment without quality assurance review.
- Incompatible operational functions should be separated. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.
- Monitor hardware maintenance of environmental controls in the data center.

**2. THE LIBRARY LACKS A COMPREHENSIVE DISASTER RECOVERY PROGRAM**

The Library could lose the capability to process, retrieve, and protect electronic information. Losing the capability to process, retrieve and protect information maintained electronically can significantly impact the Library's ability to accomplish its mission. For this reason, The Library should have (1) an administrative structure to implement or maintain service continuity of Library operations, (2) procedures in place to protect Information Resources and minimize the risk of unplanned interruptions, and (3) a plan to recover critical operations should interruptions occur.

Some weaknesses noted at the Library of Congress include:

- The Library has not developed an enterprise-wide disaster recovery plan. The Library does not have critical policies and procedures usually found in government and private industry to protect information resources and minimize the risk of unexpected interruptions and to recover critical operations should interruptions occur.
- Formal data center emergency response and processing procedures have not been established. Training has not been provided to Library employees and third party contractors to respond to emergencies.
- The Library's present computer alternate processing location situated at the House of Representatives is not geographically segregated from the main processing center. Also, the Library does not have standard written policies for performing backups of data files, Application programs, and system files and placing them in off-site storage location. Tape backup and rotation standards have not been developed and documented.

The Library could lose the capability to process, retrieve, and protect information maintained electronically in the event of a disaster. Such an event would have a significant impact on its ability to accomplish its mission critical goals.

**Recommendations:**

We recommend that the Library:

- Develop management policies and an administrative structure to implement or maintain continuity of Library operations, and develop standard backup written policies for performing backups of data files, computer programs, and critical documents and placing them in off-site storage,
- Assess the criticality and sensitivity of computerized operations and identify supporting resources,
- Train staff to respond to emergencies, and

\*\*\*\*\*

Relevant comments from the Library's management responsible for addressing these internal control matters are provided as an attachment later in this section.

### **Compliance with Laws and Regulations**

Our tests for compliance with selected provisions of laws and regulations disclosed two instances of noncompliance that are reportable under *Government Auditing Standards* or OMB audit guidance:

- During fiscal years 2001 and 2000, the Library operated ten revolving gift funds beyond the scope of its authority. Legislation authorizing the Library's revolving fund was enacted into laws as approved in November 2000. The Act will be effective at the start of fiscal year 2002 and the Library will then be in compliance.
- During fiscal years 2001 and 2000, the Library was not in compliance with the "Congressional Accountability Act (CAA) of 1995." In the CAA, Congress made its facilities and employees subject to the same safety laws that applied outside the legislative branch. In 1997, other provisions of the CAA applied fire safety standards to Congressional buildings, including the Library. The Office of Compliance conducted a yearlong fire safety investigation that culminated in a report issued in January 2001 that identified numerous safety hazards in the Library's three Capitol Hill buildings.

Except as noted above, our tests for compliance with selected provisions of laws and regulations disclosed no other instances of noncompliance that would be reportable under *Government Auditing Standards* or OMB audit guidance. However, the objective of our audit was not to provide an opinion on overall compliance with laws and regulations. Accordingly, we do not express such an opinion.

### **Effectiveness Of Internal Controls Over Safeguarding Collection Assets**

We have examined management's assertion, which is presented in Section 4, that the Library cannot provide reasonable assurance that the Library of Congress' internal control structure over safeguarding of collection assets against unauthorized acquisition, use, or disposition was generally effective as of September 30, 2001. The control criteria include: bibliographical, inventory, preservation, and physical security controls as set forth in management's assertion.

Our examination was made in accordance with standards established by the American Institute of Certified Public Accountants and with *Government Auditing Standards*, issued by the Comptroller General of the United States, and accordingly included obtaining an understanding of the internal control structure over safeguarding of collection assets, testing and evaluating the design and operating effectiveness of the internal control structure, and such other procedures as we considered necessary in the circumstances. We believe our examination provides a reasonable basis for our opinion.

Because of inherent limitations in internal controls, unauthorized acquisitions, use or disposition of collection assets may occur and not be detected. Also, projections of any evaluation of internal controls over safeguarding of assets to future periods are subject to the risk that internal controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

In our opinion, management's assertion included in section 4 that, as a result of the material weaknesses in controls described in its report, it cannot provide reasonable assurance that the internal control structure was generally effective as of September 30, 2001 over safeguarding collection assets against unauthorized acquisition, use, or disposition is fairly stated, in all material respects, based upon the control criteria: bibliographical, inventory, preservation, and physical security controls. In addition, management's assertion that newly-acquired non-rare monographs (a major portion of the general collections of the Library) are under bibliographic, inventory and preservation controls when any item is circulated outside the Library and management cannot assert that inventory controls are fully implemented during the in-processing and in-storage life-cycles as of September 30, 2001, is fairly stated based upon the criteria described above.

### **Consistency of Other Information**

Our audit was conducted for the purpose of forming an opinion on the financial statements taken as a whole. Certain portions of the Library's Financial Statement Package are not a required part of the basic financial statements, but are supplementary information required by OMB Bulletin No. 01-09, *Form and Content of Agency Financial Statements*, and the Financial Accounting Standards Advisory Board's Statement of Federal Financial Accounting Standards No. 15, *Management's Discussions and Analysis*. This supplementary information is MD&A, stewardship information, and other accompanying information. Other accompanying information consists of the full Financial Statement Package except for the MD&A, stewardship information, the basic financial statements and notes thereto, and this auditor's report. We have applied certain limited procedures, which consisted principally of inquiries of management and selected tests of this information, such as comparing it for consistency with the financial statements and footnotes. Based on these limited procedures, we found no material inconsistencies with the financial statements or footnotes. However, we did not audit this information and express no opinion on it.

### **Objectives, Scope, and Methodology**

The Library's management is responsible for:

- (1) preparing the financial statements in conformity with U.S. generally accepted accounting principles,
- (2) establishing, maintaining, and assessing internal control to provide reasonable assurance that:
  - Financial reporting: Transactions are properly recorded, processed, and summarized to permit the preparation of financial statements and stewardship information in conformity with U.S. generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition.
  - Compliance with applicable laws and regulations: Transactions are executed in accordance with laws governing the use of budget authority and with other laws and regulations that could have a direct and material effect on the financial statements.
- (3) complying with applicable laws and regulations, and

- (4) establishing, maintaining, and assessing internal control over safeguarding of collections assets.

We are responsible for obtaining reasonable assurance about whether the financial statements are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

We are also responsible for (1) obtaining a sufficient understanding of internal control over financial reporting and compliance to plan the audit and for (2) testing compliance with selected provisions of laws and regulations that have a direct and material effect on the financial statements and laws for which OMB audit guidance requires testing, and (3) performing limited procedures with respect to certain other information appearing in the financial statements.

In order to fulfill these responsibilities, we (1) examined on a test basis, evidence supporting the amounts and disclosures in the financial statements, (2) assessed the accounting principles used and significant estimates made by management, (3) evaluated the overall presentation of the financial statements, (4) obtained an understanding of internal control related to financial reporting (excluding safeguarding assets), compliance with laws and regulations (including execution of transactions in accordance with budget authority), (5) tested relevant internal controls over financial reporting, and compliance, and evaluated the design and operating effectiveness of internal control, and (6) tested compliance with selected provisions of applicable laws and regulations.

We limited our internal control testing to controls over financial reporting and compliance and over safeguarding collection assets. Because of inherent limitations in internal control, misstatements due to error or fraud, losses, or noncompliance may nevertheless occur and not be detected. We also caution that projecting our evaluation to future periods is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with controls may deteriorate. In addition, we caution that our internal control testing may not be sufficient for other purposes.

We did not test compliance with all laws and regulations applicable to the Library. We limited our tests of compliance to those laws and regulations required by OMB guidance that we deemed applicable to the financial statements for the fiscal year ended September 30, 2001. We caution that noncompliance may occur and not be detected by these tests and that such testing may not be sufficient for other purposes.

We performed our work in accordance with auditing standards generally accepted in the United States of America, *Government Auditing Standards* issued by the Comptroller General of the United States, attestation standards established by the American Institute of Certified Public Accountants, and OMB audit guidance.

This report is intended solely for the information and use of the Library, the Library's Office of the Inspector General and Congress, and is not intended to be and should not be used by anyone other than these specified parties.

*Clifton Gunderson LLP*

Calverton, Maryland  
February 27, 2002

# Memorandum

**Library of Congress**  
**Office of the Librarian**  
*Deputy Librarian*

TO : Karl Schornagel  
Inspector General

FROM :   
Donald L. Scott  
Deputy Librarian of Congress

March 15, 2002

SUBJECT: Comments on the Audit of the Library of Congress

Thank you for the opportunity to review and comment on our audit report of the Library of Congress' consolidated financial statements for fiscal years 2001 and 2000. The audit report makes many good recommendations, and the Library is taking steps to address these recommendations.

I am pleased that the audit report reflects the Library's continued progress in ensuring accountability of our resources and the progress that has been made during fiscal year 2001 in the area of collections security. For the sixth consecutive year, the Library as received an unqualified audit opinion on the consolidated financial statements.

We recognize that while substantial progress has been made there is still much work to be done, especially in the areas of computer security, business continuity planning and collections security. We look forward to the challenge and to working cooperatively with your office and the Congress in continuing to improve the accountability of the Library's resources.