

Independent Auditor's Report

To the Inspector General
Library of Congress

We have audited the accompanying consolidated balance sheet of the Library of Congress (Library) as of September 30, 1999, and the related consolidated statements of net cost, changes in net position, and combined statement of budgetary resources for the year then ended (collectively the Financial Statements). These Financial Statements are the responsibility of the Library's management. Our responsibility is to express an opinion on these Financial Statements based on our audit.

We conducted our audit in accordance with generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin 98-08, *Audit Requirements for Federal Financial Statements*, as amended. These standards require that we plan and perform the audit to obtain reasonable assurance about whether the Financial Statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the Financial Statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the Financial Statements referred to above present fairly, in all material respects, the financial position of the Library of Congress as of September 30, 1999, and its net costs, changes in net position, and budgetary resources for the year then ended, in conformity with generally accepted accounting principles.

Our audit was made for the purpose of forming an opinion on the basic Financial Statements taken as a whole. The information contained in Management's Discussion and Analysis, the supplemental consolidating information, and the Required Supplementary Stewardship information is not a required part of the basic Financial Statements but is supplemental information (Section 4) required by OMB Bulletin 97-01, *Form and Content of Agency Financial Statements*. Such information has not been subjected to the auditing procedures applied in the audit of the basic Financial Statements, and, accordingly, we express no opinion on it.

In accordance with *Government Auditing Standards*, we have also issued our reports dated February 25, 2000 on our consideration of the Library's internal control over financial reporting, and our tests of its compliance with certain provisions of laws and regulations.

Clifton Sunderson L.L.C.

Greenbelt, Maryland
February 25, 2000

Independent Auditor's Report On Compliance With Laws and Regulations

To the Inspector General
The Library of Congress

We have audited the Financial Statements of the Library of Congress (Library) as of and for the year ended September 30, 1999, and have issued our report thereon dated February 25, 2000. We conducted our audit in accordance with generally accepted auditing standards; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 98-08, *Audit Requirements for Federal Financial Statements*, as amended.

The management of the Library is responsible for complying with laws and regulations applicable to the Library. As part of obtaining reasonable assurance about whether the Library's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and certain other laws and regulations specified in OMB Bulletin 98-08, as amended. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to the Library.

The results of our tests of compliance with the laws and regulations described in the preceding paragraph disclosed the following instance of noncompliance with the laws and regulations described in the preceding paragraph that are required to be reported under *Government Auditing Standards* and OMB Bulletin 98-08, as amended.

- The Library operates gift revolving funds beyond the scope of its authority. The Library has transmitted draft legislation to the appropriate authorizing committees on a yearly basis since 1991 to address this issue. This compliance issue has been the subject of GAO audit reports since 1980. GAO found that the Library's use of certain revolving gift funds exceeded its scope of authority under 2 U. S. C. 160 to accept gifts and use them to fulfill the donor's intent. Section 160 does not authorize the Library, without specific statutory authority, to set charges for goods and services provided through self-sustaining gift funds that (1) enlarge the funds beyond the scope of the donor's gift, (2) produce revenues for other activities, or (3) create a substantial surplus. During our 1999 audit work, we identified eleven revolving funds, ten of which did not have specific congressional authorization. The revolving funds had earned revenue of \$6 million.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit and, accordingly, we do not express such an opinion.

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. We caution that non-compliance may occur and not be detected by the tests performed and that such testing may not be sufficient for other purposes.

Clifton Sunderson L.L.C.

Greenbelt, Maryland
February 25, 2000

Independent Auditor's Report On Management's Assertion About The Effectiveness Of Internal Controls Over Financial Reporting

To the Inspector General
The Library of Congress

We have examined management's assertion, included in the accompanying management report on internal controls over financial reporting for the fiscal year ended September 30, 1999 (See Section 5), regarding the system of internal control designed by management to provide reasonable assurance that the following objectives are met:

- Financial reporting – transactions are properly recorded, processed, and summarized to permit the preparation of financial statements and stewardship information in conformity with generally accepted accounting principles and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; and
- Compliance with 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 and any other laws, regulations.

Our examination was made in accordance with: standards established by the American Institute of Certified Public Accountants (AICPA); *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 98-08, *Audit Requirements for Federal Financial Statements*, as amended and, accordingly, included obtaining an understanding of the internal control over financial reporting, testing and evaluating the design and operating effectiveness of the internal control, and such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion. As the Library is not subject to the requirements of the Federal Managers' Financial Integrity Act of 1982 (FMFIA), we did not test internal controls relevant to operating objectives as broadly defined by FMFIA, such as those controls relevant to ensuring efficient operations.

Because of inherent limitations in any internal control, errors or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

Management stated that because of the weaknesses described in its report, it cannot provide reasonable assurance that internal controls in place at September 30, 1999, met the objective that assets are safeguarded against loss from unauthorized acquisition, use, or disposition, but that internal controls were effective in assuring that transactions are properly recorded, processed, and summarized to permit the preparation of reliable financial statements and to maintain accountability for assets, and were effective in assuring material compliance with applicable laws and regulations.

Management made this assertion based upon criteria established under the Library's financial management policy, LCR 1510, which is based on the internal control standards and financial systems standards promulgated by the General Accounting Office.

In our opinion, management's assertion that because of the weaknesses described in its report, it cannot provide reasonable assurance that internal controls in place at September 30, 1999, met the objective that assets are safeguarded against loss from unauthorized acquisition, use, or disposition, but that internal controls were effective in assuring that transactions are properly recorded, processed, and summarized to permit the preparation of reliable financial statements and to maintain accountability for assets, and were effective in assuring material compliance with applicable laws and regulations, is fairly stated in all material respects, based upon criteria established under the Library's financial management policy, LCR 1510, which is based on the internal control standards and financial systems standards promulgated by the General Accounting Office.

As discussed in management's assertion, the following weaknesses existed in the design or operation of the internal control of the Library in effect at September 30, 1999. We consider these weaknesses, described below, to be reportable conditions under standards established by the AICPA and OMB Bulletin 98-08, as amended. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control over financial reporting that, in our judgment, could adversely affect the Library's ability to meet the internal control objectives described above. The reportable conditions we noted are as follows:

REPORTABLE CONDITIONS

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

Our examination found that the Library's systems environment remained threatened by weaknesses in several information protection control structures. The controls in place were inadequate to fully protect information systems' resources from unauthorized access, unauthorized use, or damage. The Library had not implemented security policies and procedures to ensure that Library resources were restricted to authorized individuals and that critical data was protected. 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:

- ***Internal networks structure needs to be strengthened.*** A Security firm hired by ITS to perform an analysis of the network architecture found high-risk vulnerabilities. Intruders can exploit the vulnerabilities to obtain unauthorized access to network utilities and services, which could compromise the integrity, confidentiality availability and reliability of the network. Computer networks can be very complex. The library networks are dynamic consisting of several operating systems that can have different configurations.
- ***The Library's logical access controls did not sufficiently restrict access.*** Logical access controls were inadequate to ensure the safekeeping of sensitive utilities and data sets. A number of logical access controls settings were not in place. Without modifications the system is vulnerable to unnoticed and/or un-logged activities which could impact accurate financial reporting.
- ***Application security controls should be strengthened.*** Application controls did 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.
- ***Application software, system software, and change controls were inadequate.*** The Library did not have controls in place for the management and maintenance of application and systems software. There were no written standards to control production programs as they progress through testing to final approval. The lack of controls may result in inefficient or inadequate testing or introducing production programs that do not meet management's criteria.

Recommendation:

We recommend the following:

- Implement the security firm's recommendations including more clearly define security policy, invest more in security assets and security training, and perform routine security audits;
- Develop and implement controls to ensure that the configuration of sensitive utilities and security software are set to minimize exposure to unauthorized access and un-logged activities. Perform risk assessments to determine the need for group access and compensating controls that minimize the risk exposure;

- Evaluate and review the implementation of security features available in the operating systems and applications to ensure that risks, security and compensating controls have been addressed;
- Establish a program for the certification and accreditation of major application systems and general support systems in accordance with 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 emergency system software changes.

2. THE LIBRARY LACKS A BUSINESS CONTINUITY PLAN

The Library did not have a formal disaster recovery plan. Without a plan detailing all aspects of the controls utilized during and after a disaster, the Library places itself at risk of extensive down time. The Library did not have an alternative data processing facility and the staff within the Data Center did not have any formal training on emergency procedures. In addition, certain systems and applications did not have off-site backups.

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.

Recommendation:

We recommend that the Library immediately develop and test a disaster recovery plan for its data center and other information technology facilities. In addition, we recommend that the Library rotate systems and applications backups to an off-site storage location.

A material weakness is a condition that precludes the entity’s internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis. We believe none of the reportable conditions described above is a material weakness.

The reportable conditions discussed above were considered in determining the nature, timing, and extent of audit tests applied in our audit of the 1999 financial statements, and this report does not affect our report dated February 25, 2000 on these financial statements.

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

In addition to the reportable conditions described above, we noted certain matters involving internal control and its operations that we reported to the management of the Library in a separate letter dated February 25, 2000.

Clifton Sunderson L.L.C.

Greenbelt, Maryland

February 25, 2000

Independent Auditor's Report On Management's Assertion About The Effectiveness Of Internal Controls Over Safeguarding Collection Assets

To the Inspector General
The Library of Congress

We have examined management's assertion, which is presented in Section 5, that it 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, 1999.

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 its assertion letter, the Library of Congress had defined the following control criteria for safeguarding collection assets against unauthorized acquisitions, use or disposition:

- Bibliographic controls, which include but are not limited to: cataloging, archival processing, and arrearage reduction;
- Inventory controls, which include but are not limited to: the automated circulation control system, manual shelf list, finding aids and other detailed descriptions, and registry of items lent for exhibition;

- Preservation controls, which include but are not limited to: use of surrogates (digital, microform, service copies of audiovisual materials); collections care programs; disaster preparedness; Top Treasures security; de-acidification; conservation of individual items; preservation treatment of processed items, preservation research and testing program to define actions for de-acidification, storage, audio preservation, studies of longevity of new digital media, etc.; and special Congressionally-mandated preservation programs such as the National Film Preservation Board and American Television and Radio Archive; and
- Physical security controls, which include but are not limited to: perimeter security (e.g., theft detection devices); secured receiving and holding areas for materials not yet accessioned into the research collections, including the Copyright Office; secured in-process working and holding areas; storage areas closed to the public and all staff except those who require daily access in order to perform their jobs; reader registration; security in reading rooms (cameras, police patrols, etc.); caging high risk collections; and secured loan stations.

The Library asserts that specific controls over items in the collection assets depend upon the individual format, demand for and condition of use, and the value and risk assessment for that item. The *Integrated Control-Integrated Framework*, issued by the Committee of Sponsoring Organizations of the Treadway Commission, would classify the aforementioned Library criteria as “control activities.” The Integrated Framework also includes the following elements of internal control reporting:

- Risk assessment and collections security plan – The Library must assess the risk of unauthorized acquisition, use, or disposition of the collection;
- Control environment – The Library must influence the control consciousness of its personnel by instituting an environment that makes internal control a priority;
- Information and communication – The Library must determine what information is needed by management to prevent or timely detect control failures and make that information readily available to management at all times; and
- Monitoring – The Library must establish policies and procedures for monitoring compliance with internal controls by personnel assigned to those tasks.

Adapting these elements to the *Internal Control-Integrated Framework’s* definition of internal controls over safeguarding of assets to fit the Library’s circumstances can be summarized as follows:

“Internal control over the safeguarding of collections against unauthorized acquisition, use, or disposition is a process, effected by the Library’s management and other personnel, designed to provide reasonable assurance that the risk of unanticipated loss (theft, mutilation, destruction, or misplacement) of collection items of significant market value, cultural or historical importance, or significant information value is reduced to an acceptable level.”

Applying this definition using the Library's control criteria, a weakness in safeguarding controls is significant enough that it should be included in the Library's assertion if it results in either:

- Significant risk of unanticipated loss (theft, mutilation, destruction, or misplacement) of collection items of significant market value, cultural or historical importance, or significant information value, or
- Significant risk that senior Library management does not have sufficient information about the extent to which the Library's objectives concerning the safeguarding of the collections are being achieved.

The Library has identified such weaknesses as material weaknesses based on guidance provided by the General Accounting Office.

Opinion on Management's Assertion

The Library continued in 1999 in the implementation stage of establishing a comprehensive risk assessment and collection security plan to identify the risks to the collection, the planned or established controls that must be in place to mitigate the risks, the policies and procedures required to enforce the controls and the information management needs to monitor the effectiveness of the controls. Until these tasks are completed, Library management will not have reasonable assurance that the risk of unanticipated loss (theft, mutilation, destruction, or misplacement) of collection items of significant market value, cultural or historical importance, or significant information value is reduced to an acceptable level.

In its assertion, management describes significant weaknesses in preservation controls, inventory controls, bibliographic controls, and physical security controls over collection assets as of September 30, 1999. Our recommendations for certain of these and other significant weaknesses identified by us during our examination are outlined in the following section, *Internal Control Weaknesses in Safeguarding of Collection Assets and Recommendations for Improvement*. Our current year recommendations and assessment of the Library's initiative are intended to build on the findings and recommendations made in fiscal year 1997 and 1998.

In our opinion, management's assertion that, as a result of the material weaknesses in controls described in its report, it cannot provide reasonable assurance that the internal control structure over safeguarding collection assets against unauthorized acquisition, use, or disposition, was generally effective as of September 30, 1999, is fairly stated based upon the criteria described above.

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

Clifton Sunderson L.L.C.

February 25, 2000
Greenbelt, Maryland

INTERNAL CONTROL WEAKNESSES IN SAFEGUARDING OF COLLECTION ASSETS AND RECOMMENDATIONS FOR IMPROVEMENT

1. A WEAK CONTROL ENVIRONMENT AND INCOMPLETE CONTROL ACTIVITIES EXISTED FOR THE SAFEGUARDING OF THE COLLECTION ASSETS

The Library's control environment was not conducive to effective security over the collections. At the same time that security ranks high among the Library's priorities, it also exists in natural tension with the Library's mission of making its resources "available and useful to the Congress and the American people". The Library maintains the world's largest collections, comprising nearly 119 million items. Compounding the complexity of developing security standards for collections of such large scale and diversity is the unrelenting growth of new materials. Securing the collections has traditionally been less important than being able to serve the public.

In its assertion, management describes a number of significant weaknesses in bibliographic controls, inventory controls, preservation controls, and physical security controls over collections as of September 30, 1999. Management also describes initiatives the Library has undertaken since September 30, 1997 to remedy some of these weaknesses.

During fiscal year 1999, planning was completed for the conversion of the card shelflist, and a contract was let for the conversion of the serial check-in file and holdings file. Procedures for in-process materials were revised to include the bar coding of new receipts as one of the first processing steps.

In preservation controls, the Library had inadequate temperature and humidity control in some collections storage areas; inadequate or insufficient space for appropriate storage of collections materials; insufficient space for reformatting the acetate negative collection; and insufficient funds for reformatting.

The Library has made progress in implementing many physical security measures, although it appears as though security awareness has not improved significantly. Many of the observations made were the same as those reported in prior audit reports, particularly with respect to controls within the work areas of the Capitol facilities. Risk assessment observations indicated inconsistencies in the levels of security in reading rooms, work areas where collections are processed, and among collection items in transit.

Recommendations:

We recommend the Library continue to take action on improving the control environment and implementing control activities. We support the need for the Library to fully implement the Integrated Library System (ILS) for inventory control. We recommend that facility requirements be considered in the overall collections risk assessment when considering preservation risk. We

recommend integration of the Library's overall physical security plan with the Library's risk assessments.

2. THE LIBRARY COLLECTION SECURITY PLAN HAD NOT BEEN FULLY IMPLEMENTED

The Library's Security plan was not fully implemented. Although the Library continued to implement actions outlined in the October 1997 Security Plan, the Library had not established control activities to mitigate the risks, the policies and procedures necessary to implement the necessary controls, the required management information needed to carry out its responsibilities, and the methods by which management will monitor the effectiveness of the established control procedures.

Measurements of the effectiveness of the Library's physical security controls hinge on the development of credible baselines. Conducting regular inventories and/or statistically valid random sampling efforts can create baselines capable of establishing trends in theft and mutilation. The Library had not conducted regular inventories or statistically valid random sampling efforts, and as a consequence no genuine baselines existed.

The Library has taken a number of recent initiatives to address prior findings related to collections security that will provide it a basis to continue implementing its security plan and for continuing to conduct its formal library wide risk assessments. Among these are:

- Through the work of the Collections Security Oversight Committee (CSOC), the Library developed minimum standards for preservation, bibliographic, and inventory controls. These standards were integrated with those for physical security allowing the Library to use one, internally consistent, approach for securing the collections and evaluating threats to the Heritage Assets.
- The Library completed additional risk assessments in 1999; fifteen have been completed in total.
- The Library completed its first random sampling plan in order to establish a baseline for selected collections. Execution of random sampling plans over time will yield baselines from which the effectiveness of controls can be measured.
- The Director of Acquisitions, Library Services, convener of the CSOC's Policy and Standards subcommittee, had established a methodology to track each division's plan addressing control weaknesses identified by the risk assessments.
- More than two-thirds of the physical security baseline standards established for the collections were met in fiscal year 1999.
- In fiscal year 1999, the Library took a major step in securing its collections, most particularly its general collections, through the implementation of the Integrated Library System. This off-the-shelf system replaces multiple legacy systems and brings all library

operations dealing with acquiring, cataloging, searching and lending the collection into one unified computer system.

The combination of the physical security minimal standard as established in the security plan with the mitigating opportunities identified as a result of the ongoing risk assessments will provide the Library with the capability of assessing the effectiveness of the control measure across the complete spectrum of collections security concerns.

Recommendations:

We recommend that the Library take action to fully develop and implement its security plan. The Library's draft security plan focuses on physical security and procedural standards and requirements for protecting the collections. We recommend that the Library take the necessary actions to fully develop and implement the programs that are essential to the full implementation of the security plan.

We also recommend that the Library continue conducting regular inventories and/or statistically valid random sampling projects in select divisions. These measuring projects will create valid baselines, which over time will yield trends in theft and mutilation enabling Library's management to evaluate the effectiveness of its Security Plan and controls in place protecting the collections.

3. THE LIBRARY LACKED EFFECTIVE MANAGEMENT INFORMATION FOR MONITORING OF THE COLLECTIONS ASSETS' INTERNAL CONTROLS

Collection security objectives were incorporated in annual performance plans of custodial chiefs in fiscal year 1999. Meaningful and regular management information about whether security goals are being established and met is essential to a strong control environment. The performance plans of security officials and custodial division chiefs, as well as those in other service units who are responsible for collections security, should include measurable objectives for assuring all collections controls are implemented and functioning. Now that the risk assessments are performed, it is known what tasks personnel should perform. Action plans were prepared, by the management in each division, in response to the Risk Assessments.

Recommendations:

We recommend monitoring the integration of the performance plan process with the Library's collection risk assessments. The major controls over safeguarding of collection assets have been identified from the risk assessments. Each division has developed measurable tasks that personnel should be performing to assure that those controls are functioning. Division management should be held accountable for monitoring personnel assigned to these tasks. Reporting these results should be fully integrated into the Library's annual performance plans in order that management receives the information needed to assess the effectiveness of the internal controls over the collection assets.