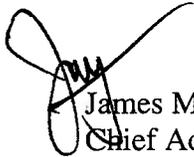


Office of Inspector General
U.S. House of Representatives
Washington, DC 20515-9990

MEMORANDUM

TO:  James M. Eagen, III
Chief Administrative Officer

FROM: James J. Cornell 
Inspector General

DATE: December 14, 2006

SUBJECT: Final Report - Audit Of The Financial Statements For The Year Ended
December 31, 2005 (Report No. 06-HOC-08)

The attached report presents the results of the audit of the U.S. House of Representatives' (House) annual financial statements for the year ended December 31, 2005. Once again, the House received an "unqualified opinion" on its financial statements. An "unqualified opinion" is the best rating given by auditors to financial statements. It means the auditors did not find any financially material discrepancies and found nothing to suggest the amounts on the financial statements were misstated. The Office of Inspector General contracted with Cotton & Company LLP, Certified Public Accountants, to perform the audit. Their report was compiled in November 2006. We have highlighted the results of the audit in the attached executive summary.

The results of the audit were discussed with your office throughout the audit, and you concurred with all but one of the reported internal control weaknesses and recommendations for corrective action. You partially concurred with one recommendation and we believe your office's alternative solution will satisfy the intent of the recommendation. Your response is included in the Management Comments section of the report on page 89.

If you have any questions or require additional information regarding this report, please call me or David Smith at (202) 226-1250.

Attachments



Financial Statements

Audit Report

*Audit Of The Financial Statements
For The Year Ended
December 31, 2005*

Report No. 06-HOC-08

December 14, 2006

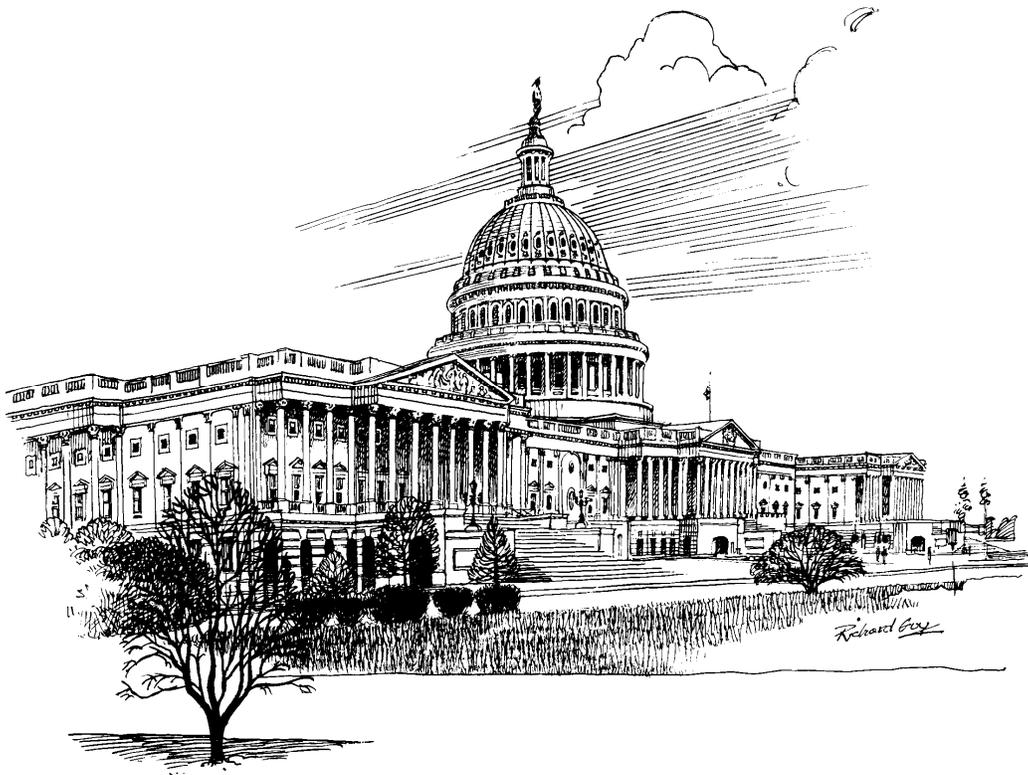


Table of Contents

Transmittal Memorandum

Executive Summary

Independent Auditor’s Report	1
Financial Statements	5
Statement of Financial Position	6
Statement of Operations	7
Statement of Cash Flows	8
Notes to the Financial Statements	9
Supplemental Financial Schedules	23
Independent Auditor’s Report on Compliance with Laws and Regulations	37
Independent Auditor’s Report on Internal Control	41
Management Comments	87
CAO Response to the 2005 Financial Statement Audit Report	

EXECUTIVE SUMMARY

Results Of Audit

The House continued to make progress during the past year in improving its financial management and operations. For the eighth year, the independent auditors expressed an “unqualified opinion” on the House’s financial statements; reporting that the financial statements fairly present, in all material respects, the financial position of the House and the results of its operations and cash flows in conformity with generally accepted accounting principles. In addition, the *Independent Auditor’s Report on Compliance with Laws and Regulations* identified no instances of noncompliance.

The *Independent Auditor’s Report on Internal Control* identified two internal control weaknesses--both of which are reportable conditions. One of these internal control weaknesses was previously reported for the year ended December 31, 2004. The second weakness incorporates a weakness from last year, but is broader in its scope.

During calendar year 2005, the House implemented or initiated corrective actions to address the 21 prior audit recommendations contained in last year’s report. Due to the House’s progress towards improving financial-related activities, we were able to close (i.e., fully implemented or otherwise resolved) 6 of the 21 prior recommendations. The closure of these recommendations resulted in the removal of one reportable condition, contained in last year’s report. The two remaining reportable conditions are associated with the financial information system and the financial reporting internal control framework.

Recommendations

This report contains 46 recommendations consisting of 15 prior recommendations, for which corrective actions are in varying stages of implementation, and 31 new recommendations.

Management Response

The CAO responded to the draft *Independent Auditor’s Report on Internal Control* on October 26, 2006. In his response, which is included in its entirety as an appendix to this report, the CAO concurred with the reported internal control weaknesses and all but one of the recommendations for corrective action. The CAO partially concurred with the recommendation to annually inventory capitalized internal-use software. As an alternative, the CAO proposed including capitalized internal use software on inventory listings that would be verified by each office using the software. The OIG believes this approach will satisfy the intent of the auditor’s recommendation.

Independent Auditor's Report

This Page Intentionally Left Blank



Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

INDEPENDENT AUDITOR'S REPORT

To the Inspector General
U.S. House of Representatives

Cotton & Company LLP has audited the accompanying Consolidated Statement of Financial Position of the U.S. House of Representatives as of December 31, 2005, and 2004, and the related Consolidated Statements of Operations and Cash Flows for the years then ended. These financial statements are the responsibility of the Members and administrative management of the House. Our responsibility is to express an opinion on these financial statements based on our audits.

We conducted our audits in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial statement audits contained in the *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated 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 audits provide 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 House as of December 31, 2005 and 2004, and the results of its operations and its cash flows for the years then ended December 31, 2005, and December 31, 2004, in conformity with accounting principles generally accepted in the United States of America.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The supplemental schedules, the Consolidating Statements of Financial Position, Operations, and Cash Flows, are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements. The supplemental schedules have been subjected to the auditing procedures applied in the audit of the basic consolidated financial statements and, in our opinion, such information is fairly stated in all material respects in relation to the basic consolidated financial statements taken as a whole.

In accordance with *Government Auditing Standards*, we have also issued reports dated May 15, 2006, on our consideration of the House's internal control over financial reporting and our tests of its compliance with applicable laws, rules, and regulations. Our reports on internal control and compliance are an integral part of an audit conducted in accordance with *Government Auditing Standards* and, in considering the results of the audits, those reports should be read together with this report.

COTTON & COMPANY LLP



Matthew H. Johnson, CPA
Partner

May 15, 2006
Alexandria, Virginia

Financial Statements

U.S. House of Representatives
Consolidated Statement of Financial Position
as of December 31, 2005 and December 31, 2004

	<u>2005</u> <u>Consolidated</u>	<u>2004</u> <u>Consolidated</u>
ASSETS		
Fund Balance with U.S. Treasury (Note 4)	\$ 1,122,063,296	\$ 1,058,766,878
Cash (Note 4)	9,091	1,459
Fund Balance with U.S. Treasury and Cash	<u>1,122,072,387</u>	<u>1,058,768,337</u>
Accounts Receivable, Net (Note 5)	612,666	235,323
Advances and Prepayments (Note 6)	8,308,915	8,944,880
Inventory	951,865	1,349,661
Property and Equipment, Net (Note 7)	<u>52,773,270</u>	<u>58,563,358</u>
Total Assets	<u>\$ 1,184,719,103</u>	<u>\$ 1,127,861,559</u>
LIABILITIES AND NET POSITION		
Accounts Payable (Note 9)	\$ 45,395,986	\$ 31,724,258
Capital Lease Liabilities (Note 8)	1,242,379	3,044,279
Accrued Funded Payroll and Benefits (Note 10)	7,820,285	7,560,399
Accrued Unfunded Annual Leave and Workers' Compensation (Note 10)	10,205,387	8,796,422
Deferred Credits (Note 11)	4,009,194	2,392,917
Unfunded Workers' Compensation Actuarial Liability (Note 12)	18,225,352	18,537,652
Other Liabilities	<u>294,159</u>	<u>102,059</u>
Total Liabilities	<u>87,192,742</u>	<u>72,157,986</u>
Unexpended Appropriations	1,056,666,770	1,010,204,361
Cumulative Results of Operations	<u>40,859,591</u>	<u>45,499,212</u>
Total Net Position (Note 13)	<u>1,097,526,361</u>	<u>1,055,703,573</u>
Total Liabilities and Net Position	<u>\$ 1,184,719,103</u>	<u>\$ 1,127,861,559</u>

U.S. House of Representatives
Consolidated Statement of Operations
for the Years Ended December 31, 2005 and December 31, 2004

	<u>2005</u>	<u>2004</u>
	<u>Consolidated</u>	<u>Consolidated</u>
REVENUE AND FINANCING SOURCES		
Revenue from Operations		
Sales of Goods	\$ 3,008,449	\$ 3,038,484
Sales of Services to Federal Agencies	6,226,875	5,657,051
Sales of Services to the Public	770,163	666,382
Interoffice Sales (Note 14)	0	0
Other Revenue	610,756	596,667
Total Revenue from Operations	<u>10,616,243</u>	<u>9,958,584</u>
Financing Sources		
Appropriations to Cover Expenses:		
Appropriations Received (Note 15)	1,204,077,790	1,149,428,934
Appropriations Yet To Be Received (Note 15)	2,405,838	3,590,661
Imputed Financing Source (Note 16)	53,798,438	51,550,355
Total Revenue and Financing Sources	<u>\$ 1,270,898,309</u>	<u>\$ 1,214,528,534</u>
EXPENSES		
Personnel Compensation	\$ 679,677,621	\$ 654,137,238
Benefits (Note 16)	280,020,618	264,071,089
Postage and Delivery	23,648,096	26,585,386
Repairs and Maintenance	51,733,169	54,363,907
Depreciation and Amortization (Note 7)	21,516,574	16,464,803
Rent, Utilities, and Communications	26,132,912	24,083,469
Telecommunications	29,371,375	24,496,635
Supplies and Materials	16,553,590	16,261,392
Travel and Transportation	34,998,183	31,346,396
Contract, Consulting, and Other Services	68,097,583	64,648,171
Printing and Reproduction	19,010,465	19,879,241
Subscriptions and Publications	10,336,035	9,536,413
Cost of Goods Sold	8,431,614	7,953,574
(Gain)/Loss on Disposal of Assets	216,608	350,960
Bad Debts	127,971	74,753
Interest on Capital Leases	240,136	126,156
Total Expenses	<u>\$ 1,270,112,550</u>	<u>\$ 1,214,379,583</u>
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	<u>\$ 785,759</u>	<u>\$ 148,951</u>
CHANGE IN NET POSITION		
Net Position, Beginning Balance	\$ 1,055,503,573	\$ 1,043,686,438
Adjustments (Note 8)	0	939,390
Net Position, Beginning Balance	1,055,503,573	1,044,625,828
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	785,759	148,951
Plus (Minus) Non-Operating Changes	41,237,029	10,928,794
Net Position, Ending Balance	<u>\$ 1,097,526,361</u>	<u>\$ 1,055,703,573</u>

U.S. House of Representatives
Consolidated Statement of Cash Flows
for the Years Ended December 31, 2005 and December 31, 2004

	<u>2005</u> <u>Consolidated</u>	<u>2004</u> <u>Consolidated</u>
CASH FLOWS FROM OPERATING ACTIVITIES		
Excess/(Deficiency) of Revenue and Financing Sources over Expenses	\$ 785,759	\$ 148,951
Adjustments affecting Cash Flow		
Appropriations Affecting Cash	(1,086,419,694)	(1,144,335,404)
(Increase)/Decrease in Accounts and Interoffice Receivable	(377,343)	(34,795)
(Increase)/Decrease in Advances and Prepayments	635,965	(4,438,161)
(Increase)/Decrease in Inventory	397,796	86,876
Increase/(Decrease) in Accounts and Interoffice Payable	13,671,728	5,241,292
Increase/(Decrease) in Other Accrued Liabilities	1,437,930	4,744,565
(Gain)/Loss on Disposal of Assets	216,608	350,960
Depreciation and Amortization	<u>21,516,574</u>	<u>16,464,803</u>
Net Cash Provided/(Used) by Operating Activities	<u>(1,048,134,677)</u>	<u>(1,121,770,913)</u>
CASH FLOWS FROM INVESTING ACTIVITIES		
Purchase of Property and Equipment	<u>(15,806,126)</u>	<u>(24,260,102)</u>
Net Cash Provided/(Used) by Investing Activities	<u>(15,806,126)</u>	<u>(24,260,102)</u>
CASH FLOWS FROM FINANCING ACTIVITIES		
Appropriations	1,135,073,378	1,166,754,493
Funds Returned to the U.S. Treasury	(7,753,623)	(5,706,603)
Principal Payment on Capital Lease Liabilities	<u>(74,902)</u>	<u>(316,664)</u>
Net Cash Provided/(Used) by Financing Activities	<u>1,127,244,853</u>	<u>1,160,731,226</u>
Net Cash Provided/(Used) by Operating, Investing, and Financing Activities	63,304,050	14,700,211
Fund Balance with U.S. Treasury and Cash, Beginning	<u>1,058,768,337</u>	<u>1,044,068,126</u>
Fund Balance with U.S. Treasury and Cash, Ending	<u>\$ 1,122,072,387</u>	<u>\$ 1,058,768,337</u>

Notes to the Financial Statements

NOTE 1 - DESCRIPTION OF THE REPORTING ENTITY

The U.S. House of Representatives (House) is one of two separate legislative chambers that comprise the Congress of the United States. The other is the U.S. Senate (Senate). All lawmaking powers of the Federal government are given to the Congress under Article I of the Constitution of the United States. The House and Senate jointly agree on a budget for the Legislative Branch and submit it to the President of the United States. The Members of the House serve two-year terms of office, which coincide with the sequential numbering of the entire Congress. These financial statements cover the years ended December 31, 2005 and 2004 and reflect the financial activities of the first session of the 109th Congress and the second session of the 108th Congress.

To help carry out its constitutional duties, the House creates committees of Members and assigns them responsibility for gathering information, identifying policy problems, proposing solutions, and reporting bills to the full chamber for consideration. The House appoints unelected officers to administer both legislative and non-legislative functions, which support the institution and its Members in carrying out its legislative duties. The consolidated comparative financial statements of the House provide financial information on the activities of all entities, which are subject to the authority vested in the House by the U.S. Constitution, public laws, and rules and regulations adopted by the membership of the House.

These financial statements reflect the organizational structure of the House under the 109th Congress. The following is a summary of the entity groupings as they appear in the calendar year 2005 consolidating financial statements:

House **Members** are elected from congressional districts of approximately equal population. The financial information aggregates transactions of the Member districts and Washington, D.C. offices, and includes 435 Representatives; four Delegates, one each, from the District of Columbia, Guam, Virgin Islands, and American Samoa; and one Resident Commissioner from Puerto Rico.

The **Committees** financial information aggregates transactions of the Standing and Special and Select Committees of the 109th Congress. Committees are organized at the beginning of each Congress according to their jurisdictional boundaries incorporated in the Rules of the House. The Committees of the House under the 109th Congress are:

Committee on Agriculture
Committee on Appropriations

Committee on Armed Services
Committee on the Budget
Committee on Education and the Workforce
Committee on Energy and Commerce
Committee on Financial Services
Committee on Government Reform
Committee on Homeland Security
Committee on House Administration
Committee on International Relations
Committee to Investigate the Preparation for and Response to Hurricane Katrina
Committee on the Judiciary
Committee on Resources
Committee on Rules
Committee on Science
Committee on Small Business
Committee on Standards of Official Conduct
Committee on Transportation and Infrastructure
Committee on Veterans' Affairs
Committee on Ways and Means
Permanent Select Committee on Intelligence

The House **Leadership Offices** financial information aggregates transactions of:

Speaker of the House
Majority and Minority Leaders
Majority and Minority Whips
Party Steering Committees, Caucus or Conference, which consist of Representatives of the same political party

The **Officers and Legislative Offices** financial information aggregates transactions of all legislative support and administrative functions provided to Members, Committees, and Leadership offices, including:

Chaplain
Chief Administrative Officer
Office of Emergency Planning, Preparedness and Operations
Clerk of the House
Office of the General Counsel
Office of Inspector General
Office of the Historian
Office of the Law Revision Counsel
Office of the Legislative Counsel
Parliamentarian
Sergeant at Arms

The **Joint Functions** financial information aggregates transactions of the joint activities of the House and the

Senate to the extent that the House funds these functions in whole or in part. House administrative management does not exert direct control over the expenditures of these functions. The joint functions in these statements include:

Attending Physician
Joint Committee on Taxation, which has members
from both the House and the Senate

Eliminations on the consolidating financial statements are used to negate the effect of financial transactions between House entities. Consolidated House financial information would be misleading if inter-entity transactions were not eliminated.

NOTE 2 - SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

A. Basis of Consolidation

The financial statements include the accounts and significant activities of the House. The consolidated financial statements do not include legislative agencies that support the House and that receive separate appropriations. These agencies are:

Library of Congress
Congressional Budget Office
Government Accountability Office
Government Printing Office
U.S. Botanic Garden
Architect of the Capitol
U.S. Capitol Police

Functions jointly shared between the House and the Senate are included in the consolidating financial statements to the extent their operations are funded by House appropriations. These consist of :

Attending Physician
Joint Committee on Taxation, which has
members from both the House and the Senate

All significant interoffice balances and transactions have been eliminated to arrive at consolidated financial information.

B. Basis of Accounting

The House, in accordance with generally accepted accounting principles, utilizes the accrual basis of accounting, which provides for the recognition of events as they occur, as opposed to when cash is received or disbursed. Therefore, revenues are recorded when earned and expenses are recorded when a liability is incurred, without regard to receipt or payment of cash. The accrual basis of accounting contributes significantly to the development of accurate cost information needed to report the financial position and results of operations.

C. Fund Balance with the U.S. Treasury and Cash

Funds available to the House to pay current liabilities and finance authorized purchases are held with the U.S. Treasury.

- Fund Balance with the U.S. Treasury includes House accounts, as well as the Congressional Use of Foreign Currency account, which is held at the U.S. Treasury and is maintained and administered by the Department of State on behalf of the House.
- For purposes of the Consolidated Statement of Cash Flows, funds held with the U.S. Treasury are considered cash.

D. Accounts Receivable

Accounts receivable consists of money owed the House by Federal agencies, Members, employees and/or vendors less an Allowance for Doubtful Accounts.

E. Advances and Prepayments

Advances consist of payments to Federal government entities for contractual services and for mailings that require address corrections or additional postage. Prepayments primarily consist of prepaid subscriptions for publications and data communication services.

F. Inventory

The *Gift Shop* and the *Supply Store* maintain an inventory of goods for sale. These entities are included with Officers and Legislative Offices in the consolidating financial statements. Inventories for sale are valued at the moving weighted average method.

The *Furniture Support Services*, also included with Officers and Legislative Offices, maintains inventories of such items as hardwood, carpet, leather, fabric, furniture components, and repair materials. These items are not for sale and are reflected in the financial statements at an estimated value based on the first in/first out inventory valuation method.

G. Property and Equipment

Property and equipment including computer purchases are capitalized if the unit acquisition cost is equal to or greater than \$25,000 and the item has a useful life greater than one year. Software is capitalized if the unit acquisition cost is equal to or greater than \$10,000 and the item has a useful life greater than one year. The costs of such items are recognized as assets when acquired. An appropriate portion of an asset's value is reduced and an expense recognized over the accounting periods benefited by the asset's use. See Note 7, Property and Equipment, for additional information on property and equipment held by the House.

The House has possession of numerous assets that may be of significant historical and artistic value. The House does not include these assets in the financial statements. The land and buildings occupied and used by Members, officers, and employees in Washington, D.C. are under the custody of the Architect of the Capitol and are not included in the financial statements of the House.

H. Leases

The House leases office space, vehicles, computers and other equipment. These leases are generally classified as operating leases. House regulations require that leases entered into by Members for space and vehicles be no longer than the elected term of the Member. The House also enters into leases, which are structured such that their terms effectively finance the purchase of the item. Such leases convey the benefits and risks of ownership and are classified as capital leases, if the net present value of the minimum lease payments due at lease inception meets House capitalization criteria. Items acquired by capital leases are recorded as House assets. The asset and corresponding liability are recorded at the net present value of the minimum lease payments at lease inception. The portion of capital lease payments representing imputed interest is expensed as interest on capital leases. See Note 8, Lease Commitments, for additional lease information.

I. Deferred Credits

The House receives advance payments from other Federal government entities for shared services, in advance of the delivery of these services. These advance payments are recorded as deferred credits. As the services are rendered the deferred credit account is drawn down and the appropriate revenue is recognized.

J. Revenue from Operations

Revenue is recognized when goods have been delivered or services rendered.

- Sales of goods consist of Gift Shop and Supply Store sales.
- Sales of services to the public are comprised of Photography sales, Child Care fees, and Attending Physician fees.
- Interoffice sales between House entities consist of computer services, telecommunications, office supplies, framing, recording, office equipment, photography, tape duplication charges, and are eliminated on the consolidating financial statements.
- Other revenue consists of Page School room and board, and vendor commissions.

K. Appropriations to Cover Expenses

Like other Federal government organizations, the House finances most of its operations with appropriations. The expenses of Members, Committees, and Leadership offices are entirely financed with appropriations. Other House entities require appropriations to the extent the revenue generated does not cover expenses. Appropriations are considered a financing source, not a revenue, since appropriations do not result from an earnings process.

L. Postage and Delivery

Postage and delivery consists of franked mail expenses and miscellaneous postage expenses. Members' postage includes the use of the Frank, which is charged to the Members' Representational Allowance. Miscellaneous postage expenses include courier charges, stamps, and rental of post office boxes.

M. Repairs and Maintenance

Repairs and maintenance include all expenses related to the maintenance and upkeep of House equipment in both Washington, D.C. and in Members' district offices, as well as related operating lease payments on various types of equipment. In addition, property and equipment purchases below the capitalization thresholds discussed in Note 2G, Property and Equipment, are classified as repairs and maintenance.

N. Depreciation and Amortization

The cost of capital assets is allocated ratably over an asset's useful life as depreciation or amortization expense. The House calculates depreciation and amortization expense based on the straight-line method over an asset's estimated useful life. Depreciation expense is applicable to tangible

assets such as furniture, equipment, and vehicles. Amortization expense is applicable to intangible assets such as software and capital leases. Assets acquired under capital leases are generally amortized over the lease term. However, if a lease agreement contains a bargain purchase option or otherwise transfers title of the asset to the House, the asset is amortized on the same basis as similar categories of owned assets.

O. Rent, Utilities, and Communications

Rent and utilities consist primarily of the rental of district offices by Members and any related utility payments. Communications costs consist of charges for news wire services, satellite fees, and external network access services.

P. Telecommunications

Telecommunications expense includes local and long distance telephone service in Washington, D.C. and in Members' district offices.

Q. Supplies and Materials

Supplies and materials include office supplies used by the House and medical supplies used by the Attending Physician. Supplies and materials do not include inventories held for sale by retail entities such as the *Gift Shop* and the *Supply Store*.

R. Travel and Transportation

Travel and transportation expenses include official travel by Members, Committees, and Leadership offices; travel by other House officers and employees and congressional delegations; freight and shipping costs; and expenses related to the lease and maintenance of vehicles.

S. Contract, Consulting, and Other Services

Contract, consulting, and other services include the cost of management services in House Postal Operations, annual audit fees, the cost of studies and analyses requested by Committees, as well as computer, recording, janitorial, and catering services.

T. Printing and Reproduction

This category primarily includes printing and reproduction of constituent communications. Also included are photography services, and printing and reproduction of

items such as informational publications and reference materials.

U. Subscriptions and Publications

Subscriptions and publications include the cost of periodicals and news services.

V. Cost of Goods Sold

Cost of goods sold includes the cost of products sold in the retail operations of the *Gift Shop* and the *Supply Store*, and the cost of services provided to federal and non-federal entities, such as the House postal facility.

W. Loss or Gain on Disposal of Assets

A loss is recognized when the net book value of the asset at the time of disposal exceeds any proceeds received. A gain is recognized when the net book value of the asset at the time of disposal is less than any proceeds received.

X. Annual Leave

Annual leave for the House Officers and their employees is accrued as earned, and the liability is reduced as leave is taken. The accrued annual leave balance as of September 30, 2005 is calculated according to Public Law 104-53, November 19, 1995, 109 Stat. 514. See Note 10, Accrued Payroll and Benefits and Leave, for additional information.

Y. Federal Employee and Veterans Benefits

This benefit expense includes the current cost of providing future pension benefits to eligible employees at the time the employees' services are rendered. Also included is the current period expense for the future cost of providing retirement benefits and life insurance to House employees. See Note 16, Benefits, for additional information.

Z. Use of Estimates

The preparation of financial statements requires management to make estimates and assumptions that affect the reported amount of assets and liabilities, as well as the disclosure of contingent assets and liabilities at the date of the financial statements, and the amount of revenue and expense reported during the period. Actual results could differ from those estimates.

NOTE 3 - INTRA-GOVERNMENTAL FINANCIAL ACTIVITIES

The House has significant intra-governmental financial activities with Executive and Legislative Branch entities. These financial activities include transactions and agreements to purchase goods and services.

Transactions with Executive Branch Agencies

The House’s most significant interagency transactions are with the:

- U.S. Postal Service for postage.
- Department of Defense for communication equipment
- U.S. Department of Labor (DOL) for unemployment and workers’ compensation.
- General Services Administration (GSA) for the use and upkeep of office space in certain Members’ district offices, office supplies and leased vehicles.
- U.S. Department of the Interior, U.S. Geological Survey, National Business Center for financial system contract and consulting services.
- U.S. Department of Transportation for transit benefits program.
- Other Executive Branch agencies for special studies as requested by House Committees.

Significant cash disbursements to Executive Branch agencies during the years ended December 31, 2005 and 2004 were approximately:

Disbursements to Executive Branch Agencies	2005	2004
U.S. Postal Service	\$ 19,447,000	\$ 28,190,000
Department of Defense	2,844,000	10,814,000
General Services Administration	4,542,000	4,748,000
U.S. Department of Labor	2,746,000	2,074,000
U.S. Department of Transportation	1,653,000	1,381,000
U.S. Department of the Interior	533,000	503,000
Other Executive Branch Agencies	10,000	430,000

The House also reports significant financial transactions with the U.S. Department of State, which maintains and

administers the Congressional Use of Foreign Currency account on behalf of Congress. This account, which was established in 1948 and made permanent in 1981, is authorized by legislation codified in Title 22, Sec. 1754 of the United States Code. The funds are available to Congressional Committees and delegations to cover local currency expenses incurred while traveling abroad. The fund balance related to the account is included in Fund Balance with U.S. Treasury under Officers and Legislative Offices.

Use of the foreign currency account for Congressional delegations and other official foreign travel of the House is authorized by either the Speaker of the House or the chairman of a Standing, Special and Select, or Joint Committee. Therefore, all foreign currency account financial activity is reported as Committee and Leadership office travel expense.

Foreign Currency Balance with the U.S. Department of State	2005	2004
Beginning Balance	\$ 26,366,887	\$ 11,344,688
Appropriation Received	17,000,000	23,500,000
Travel Expenses:		
Leadership	(1,151,607)	(1,687,864)
Committees	(7,988,135)	(6,789,937)
Ending Balance	<u>\$ 34,227,145</u>	<u>\$ 26,366,887</u>

Transactions with Legislative Branch Entities

The House pays for support services provided by other Legislative Branch entities. These entities receive their own appropriations and operate autonomously from the House’s administrative functions. The House received support services from the United States Senate in 2005. The House also receives support services from the Government Printing Office and the Architect of the Capitol.

Cash Disbursements to Legislative Branch Entities	2005	2004
Architect of the Capitol	\$ 225,000	\$ 307,000
Government Printing Office	119,000	152,000
Government Accountability Office	-	434,000
United States Senate	1,507,000	-

The House also receives payments for services provided to the Congressional Budget Office and the Architect of the Capitol and for the reimbursement of services shared with other Federal government entities. In 2005, the House shared services with the Library of Congress, and the United States Senate.

Cash Receipts from Legislative Branch Entities	2005	2004
Architect of the Capitol	\$ 336,000	\$ 270,000
Congressional Budget Office	92,000	-
Library of Congress	7,235,000	3,652,000
United States Senate	315,000	831,000

NOTE 4 - FUND BALANCE WITH THE U.S. TREASURY AND CASH

The House has appropriated and revolving fund balances with the U.S. Treasury. The balances, as of December 31, 2005 and 2004 were:

Fund/Cash Accounts Maintained by the House	2005	2004
Fund Balance with Treasury/Cash	\$ 1,087,836,151	\$ 1,032,401,450
Congressional Use of Foreign Currency	34,227,145	26,366,887
Total	<u>\$ 1,122,063,296</u>	<u>\$ 1,058,768,337</u>

The House usually receives the full amount of its appropriation at the beginning of each fiscal year.

Cash on Hand represents deposits in transit and amounts held in a commercial bank account as of December 31, 2005 with a balance of \$9,091.

NOTE 5 - ACCOUNTS RECEIVABLE

Accounts Receivable balances represent amounts owed the House by Federal agencies, Members, employees and/or vendors less an allowance for doubtful accounts. The Allowance for Doubtful Accounts was derived from the receivables amount owed to the House for more than six months.

Accounts Receivable	2005	2004
Accounts Receivable	\$ 907,075	\$ 360,845
Less: Allowance for Doubtful Accounts	(253,493)	(125,522)
Accounts Receivable, Net	<u>\$ 653,582</u>	<u>\$ 235,323</u>

NOTE 6 - ADVANCES AND PREPAYMENTS

Advances and prepayments are transfers of cash to cover future expenses or the acquisition of assets. These goods and/or services are delivered in increments that span several months. Advance payments are recorded as assets. As the goods and/or services are rendered, the Advance account is drawn down and the appropriate asset or expense is recognized. Prepayments are made for subscriptions and software licenses and are charged as expenses. At year-end, all such payments made for the previous, current and succeeding years are analyzed to determine the proper

expense and prepayment amounts applicable to the current accounting period for financial statement purposes. Advances and Prepayments are:

	2005	2004
Advances	\$ 1,265,261	\$ 3,198,368
Prepayments	7,043,654	5,746,512
Total	<u>\$ 8,308,915</u>	<u>\$ 8,944,880</u>

NOTE 7 – PROPERTY AND EQUIPMENT

Software, and vehicles and equipment, including computers, are capitalized if their acquisition cost equals or exceeds \$10,000 and \$25,000, respectively. Work in process consists of capitalized costs associated with assets received, but not placed in service as of December 31, 2005. Depreciation and

amortization expense is based on the straight-line method over an asset's estimated useful life.

Property and equipment as of December 31, 2005 and the related depreciation and amortization expense are:

2005 Classes of Property and Equipment	Service Life (Years)	Estimated Acquisition Value	Accumulated Amortization/ Depreciation	Estimated Net Book Value	Amortization/ Depreciation Expense
Work in Process	N/A	\$ 4,861,708	\$ -	\$ 4,861,708	\$ -
Computer Software and Hardware	3	83,296,734	64,410,038	18,886,696	14,574,172
Computer Software and Hardware	5	790,911	790,911	-	-
Equipment	5	35,369,928	23,571,631	11,798,297	4,740,699
Motor Vehicles	5	10,278,797	1,434,435	8,844,362	998,780
Furnishings and Other Equipment	10	1,738,469	1,583,817	154,652	61,829
Assets Under Capital Lease	10	3,234,787	646,956	2,587,831	323,479
Leasehold Improvements	10	7,934,730	2,389,244	5,545,486	712,617
Total		\$ 147,506,064	\$ 94,827,032	\$ 52,679,032	\$ 21,411,576

Property and equipment as of December 31, 2004 and the related depreciation and amortization expense are:

2004 Classes of Property and Equipment	Service Life (Years)	Estimated Acquisition Value	Accumulated Amortization/ Depreciation	Estimated Net Book Value	Amortization/ Depreciation Expense
Work in Process	N/A	\$ 15,503,938	\$ -	\$ 15,503,938	\$ -
Computer Software and Hardware	3	76,546,471	53,822,860	22,723,611	11,001,914
Computer Software and Hardware	5	790,911	790,911	-	-
Equipment	5	32,684,266	20,753,069	11,931,197	4,381,753
Motor Vehicles	5	-	-	-	-
Furnishings and Other Equipment	10	2,542,630	2,354,550	188,080	59,472
Assets Under Capital Lease	10	3,234,787	323,479	2,911,308	323,479
Leasehold Improvements	10	6,981,852	1,676,628	5,305,224	698,185
Total		\$ 138,284,855	\$ 79,721,497	\$ 58,563,358	\$ 16,464,803

NOTE 8 – LEASE COMMITMENTS**Capital Leases**

The House enters into leases, which are structured such that their terms effectively finance the purchase of the item. Such leases convey the benefits and risks of ownership and are classified as capital leases, if the net present value of the future minimum lease payments due at lease inception meets House capitalization criteria. Items acquired by capital leases are recorded as House assets. The asset and corresponding liability are recorded at the net present value of the future minimum lease payments due at lease inception. Assets under capital leases consist solely of building structures.

Future Capital Lease Payments Due as of December 31, 2005:

Year	
2006	\$ 422,998
2007	422,998
2008	422,998
2009	422,998
2010	422,998
Thereafter	1,268,995
Total Future Capital Lease Payments	\$3,383,985
Less: Imputed Interest	(685,248)
Net Capital Lease Liabilities	\$2,698,737
Unfunded Liability	\$2,698,737

Operating Leases

The House enters into various operating leases for temporary usage of office space, vehicles, hardware, and software. Leases that convey the benefits and risks of ownership, but

do not meet House capitalization criteria are also recognized as operating leases. Operating lease payments are recorded as expenses. Future operating lease payments are not accrued as liabilities. Members may lease office space in their districts through GSA or may directly lease space from the private sector. The Members' Congressional Handbook states that a Member cannot enter into a lease for office space beyond his/her elected term. Members and officers also enter into leases to rent vehicles for official business purposes. A Member may lease a vehicle for a period that exceeds the current congressional term, but the Member remains personally responsible for the lease liability if service to the House concludes prior to lease termination. House administration also leases hardware and software.

Future Operating Lease Payments Due as of December 31, 2005:

Year	Software and Hardware	Vehicles	Office Space	Parking	Total
2006	\$ 187,032	\$1,011,069	\$ 22,804,541	\$57,522	\$24,060,164
2007	-	-	-	-	-
Thereafter	-	-	-	-	-
Total	\$ 187,032	\$1,011,069	\$ 22,804,541	\$57,522	\$24,060,164

Lease expense for office space was \$22,558,436 and \$21,310,416 for the years ended December 31, 2005 and 2004, respectively. Lease expense for vehicles was \$1,604,368 and \$1,321,377 for the years ended December 31, 2005 and 2004, respectively.

NOTE 9 - ACCOUNTS PAYABLE

Accounts Payable balances represent amounts owed for the cost of goods and services received but not yet paid. Accounts Payable also includes amounts owed to DOL for unemployment compensation.

Accounts Payable	2005	2004
Vendor Payables	\$ 45,275,586	\$ 31,575,166
Unemployment Compensation	120,400	149,092
Total	\$ 45,395,986	\$ 31,724,258

NOTE 10 - ACCRUED PAYROLL AND BENEFITS AND LEAVE

The accrued annual leave balances are calculated according to Public Law 104-53, November 19, 1995, 109 Stat. 514 (i.e., the lesser of the employee’s monthly pay or the monthly pay divided by 30 days and multiplied by the number of days of accrued leave). Sick and other types of paid leave are expensed as they are taken. Accrued payroll and benefits include salaries and associated benefits earned in December 2005 and payable in January 2006.

The Members’ and Committees’ Congressional Handbooks allow offices to adopt personnel policies that provide for the accrual of annual leave and use of such leave. Leadership offices have also adopted similar policies. While leave is tracked from one pay period to the next, a consistent policy has not been formally adopted by these entities regarding the accrual and payment of leave time. Therefore, an accrued

leave liability for Members, Committees, and Leadership offices is estimated on the financial statements. Accrued annual leave and accrued payroll and benefits as of December 31, 2005 and 2004 were:

Accrued Leave, Payroll and Benefits, and Workers' Compensation	2005	2004
Funded		
Accrued Payroll and Benefits	\$ 7,820,285	\$ 7,560,399
Unfunded		
Accrued Annual Leave	7,810,964	6,739,723
Accrued Workers' Compensation	<u>2,394,423</u>	<u>2,056,699</u>
Total Unfunded	<u>\$ 10,205,387</u>	<u>\$ 8,796,422</u>

NOTE 11 - DEFERRED CREDITS

The House received payments in advance of receipt of shared services from the Library of Congress, the Senate and the Department of State. The deferred credit balance as of

December 31, 2005 and 2004 were \$4,009,194 and \$2,392,917, respectively.

NOTE 12 - UNFUNDED WORKERS’ COMPENSATION ACTUARIAL LIABILITY

The Federal Employees’ Compensation Act (FECA) provides income and medical cost protection to covered Federal civilian employees injured on the job, employees who have incurred a work-related occupational disease, and beneficiaries of employees whose death is attributable to a job-related injury or occupational disease. Claims incurred for the benefit of House employees under FECA are administered by DOL, which pays the initial claim and obtains reimbursement from the House. The unfunded workers’ compensation actuarial liability is an estimate based on actuarial calculations using

historical payment patterns to predict what costs will be incurred in the future. The liability is adjusted annually by applying actuarial procedures. Any upward or downward adjustment to the liability is recorded as an annual increase or decrease to benefits expense. In 2005, the actuarial liability was calculated by the House based on a model developed by DOL. The projected Unfunded Workers’ Compensation Actuarial Liabilities as of December 31, 2005 and 2004 were \$18,225,352 and \$18,537,652 , respectively.

NOTE 13 - NET POSITION

The components of Net Position are:

- Unexpended Appropriations - Appropriations are not considered expended until goods have been received or services have been rendered.
- Total Cumulative Results of Operations:

Cumulative Results of Operations - The net difference between expenses and revenue and financing sources including appropriations, revenues from operations and imputed financing sources.

Invested Capital - Funds used to finance capital assets such as computer hardware and software, vehicles, equipment, and inventory.

Future Funding Requirements - Known liabilities to be funded by future appropriations for accrued Annual Leave and Workers' Compensation.

Unexpended appropriations cancel at the end of the second fiscal year following the year in which appropriated. As required by law, these funds must be returned to the U.S. Treasury general account. Funds that were canceled and returned to the U.S. Treasury during calendar years 2005 and 2004 are:

Appropriations	2005	2004
2003	\$ 7,753,623	\$ -
2002	-	5,706,603
Total	\$ 7,753,623	\$ 5,706,603

Net Position as of December 31, 2005 and 2004 for Appropriated Funds and Revolving Funds, including the House Recording Studio, Net Expenses of Equipment, Page School, Restaurant, House Services, Barber and Beauty Shops, and Office Supply Service revolving funds are shown in the following table:

Net Position	Net Position December 31, 2005 Totals	Net Position December 31, 2004 Totals
Unexpended Appropriations	\$ 1,056,707,686	\$ 1,010,204,361
Cumulative Results of Operations:		
Cumulative Results of Operations	\$ 16,807,571	\$ 15,964,547
Invested Capital	50,998,972	56,868,739
Future Funding Requirements	(28,430,738)	(27,334,074)
Total Cumulative Results of Operations	39,375,805	45,499,212
Total Net Position	\$ 1,096,083,491	\$ 1,055,703,573

Changes in net position may include prior period adjustments, excesses or shortages of revenue and financing sources over expenses, and non-operating changes, such as investments in capital assets and inventory. Increases (or decreases) in non-operating changes result when amounts invested in capital assets and inventory exceed (or are less than) the amounts of liabilities to be funded by future

appropriations. The increase in Cumulative Results of Operations is primarily the result of purchases of Property, Plant and Equipment.

The Net Position table above reflects an additional cumulative results of operations line which further disaggregates activity other than invested capital or future funding requirements.

NOTE 14 - REVOLVING FUNDS, INTEROFFICE SALES, AND TRANSFERS

Some House entities transfer costs to Members, Committees, and other House offices for goods and services provided. These entities are primarily:

- House Support Services, which transfers costs of equipment to the Members and Committees,
- House Information Resources, which transfers telecommunication charges, and
- Office Supply Service, which transfers office supply purchases and flag sales.

Some House business-like entities operate as revolving funds. A revolving fund is a budgetary structure established by statute that authorizes certain government agencies to collect user fees or revenue to finance operating expenses. In 2005, the House operated revolving fund type activities for the House Recording Studio, Net Expenses of Equipment, Page School, Office Supply Service, Child Care Center, House Services, Restaurant, and Beauty and Barber Shops.

NOTE 15 - APPROPRIATIONS TO COVER EXPENSES

Appropriations Received include current and prior year funds necessary to finance House operating expenses such as personnel and benefits costs, contract services, and travel expenses. The House recognizes appropriations to cover expenses in the same period in which the associated expense is incurred. Appropriations to cover investments in capital

assets and inventory are recognized in the same period in which they are received.

Appropriations Yet To Be Received consist of expenses that are incurred in the current period, but will be funded by future appropriations. Such amounts include accrued actuarial liabilities, annual leave and workers' compensation expenses.

NOTE 16 - BENEFITS

House Members and employees are covered by either the Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS). Both Members and employees are eligible for retirement benefits under CSRS or FERS. A CSRS basic annuity, unreduced for age, debts to the fund, or survivor's benefits, is calculated by multiplying the highest 3 consecutive years' average salary by a percentage factor which is based on the length of Federal service. However, Members' benefits are different from those of employees. For example, a Member covered by CSRS is eligible to receive unreduced retirement benefits at age 60 if he or she has 10 years of Member service. An employee is eligible to receive reduced benefits at age 50 with 20 years of service or at any age with 25 years of service. The FERS basic benefit plan provides the same benefits for either Members or employees.

CSRS employees contribute a portion of their earnings to the Civil Service Retirement Fund. The House also contributes an amount to this fund. FERS employees, in addition to paying Social Security, contribute a portion of their base earnings to the FERS retirement fund. The House also contributes an amount toward the FERS retirement and Social Security funds.

Both FERS and CSRS employees can contribute to the Thrift Savings Plan (TSP). Effective July 2001, both FERS and CSRS employees' TSP contribution limits increase by one percent each year for five years to a maximum of 15% and 10% of the base pay of FERS and CSRS employees respectively, but not to exceed the IRS limit.

FERS employees also receive an automatic one percent House-paid contribution, as well as an additional House matching TSP contribution up to five percent of their basic pay. CSRS employee contributions to TSP do not receive matching House contributions. FERS employees could receive benefits from FERS, the Social Security System, and TSP. CSRS employees could receive benefits from CSRS and TSP.

Member and Employee Expenses	2005	2004
Retirement Plan Contributions	\$ 126,511,042	\$ 118,336,660
Federal Employee and Veterans' Benefits	53,798,438	51,550,355
Social Security	44,189,820	42,192,147
Health Insurance	40,406,925	37,589,913
Student Loan/Fitness Center Programs	8,171,831	7,334,082
Unemployment and Workers' Compensation	2,509,904	1,512,819
Annual Leave	1,071,241	666,697
Death Benefits	1,003,031	948,429
Transit Benefits	1,642,416	1,389,806
Life Insurance	1,028,270	976,854
Workers' Compensation Actuarial Adjustment	(312,300)	1,573,327
Total	<u>\$ 280,020,618</u>	<u>\$ 264,071,089</u>

Benefits costs for the past 3 years have averaged approximately \$262 million per year.

Federal-employing entities recognize their share of the cost of providing future pension benefits to eligible employees at the time the employees' services are rendered. This cost is included in Federal Employee and Veterans' Benefits expense. The pension expense recognized in the Statement of Operations is the current service cost for House employees less the amount contributed by the employee.

The measurement of the service cost requires the use of actuarial cost methods and assumptions, with the factors applied by the House provided by the Office of Personnel Management (OPM), the federal agency that administers the plan. The excess of the recognized pension expense over the amount contributed by the House represents the amount being financed directly through the Civil Service Retirement and Disability Fund administered by OPM.

The House does not receive an appropriation to fund this expense. Therefore, this portion of the pension expense is considered an imputed financing source to the House, and is included in the Imputed Financing Sources on the Statement of Operations. This amount was \$12,458,987 in 2005 and \$16,092,978 in 2004.

Federal-employing entities also recognize a current period expense for the future cost of post-retirement health benefits and life insurance for its employees while they are still employed. This cost is included in Federal Employee and Veterans' Benefits expense in the Statement of Operations. Employees and the House do not currently make contributions to fund these future benefits, and the House does not receive an appropriation to fund this expense. Therefore, this portion of the post-retirement health benefits and life insurance is considered an imputed financing source to the House, and is included in Imputed Financing Sources on the Statement of Operations. This amount was \$41,339,451 in 2005 and \$35,457,377 in 2004.

Federal Employee and Veterans' Benefits (Imputed Financing Source)	2005	2004
Current Service Cost - Federal Employees Health Benefits	\$ 41,239,133	\$ 35,362,210
Current Service Cost - Federal Pensions	12,458,987	16,092,978
Current Service Cost - Federal Employees Group Life Insurance	100,318	95,167
Total	<u>\$ 53,798,438</u>	<u>\$ 51,550,355</u>

NOTE 17 - EMERGENCY PREPAREDNESS

The House continues to develop contingency plans to ensure the continuation of all House Operations in the event of an emergency evacuation.

Approximately \$24.9 million and \$28.8 million were expended in 2005 and 2004, respectively.

NOTE 18 - CONTINGENCIES

The House is currently involved in a lawsuit, the probable outcome of which is unfavorable. The precise amount is

unknown based on the best information available as of the reporting date.

This Page Intentionally Left Blank

Supplemental Financial Schedules

This Page Intentionally Left Blank

Organization and Composition of Financial Statements

This Page Intentionally Left Blank

**U.S. House of Representatives
Organization and Composition of
Consolidating Financial Statements**

Members

Representatives, Delegates and Resident
Commissioner
Members' Allowances and Expenses

Legislative Computer Systems
Office of Legislative Operations
Legislative Resource Center
Official Reporters
Office of Publication Services
Capitol Service Groups

Committees

Committee on Agriculture
Committee on Appropriations
Committee on Armed Services
Committee on the Budget
Committee on Education and the Workforce
Committee on Energy and Commerce
Committee on Financial Services
Committee on Government Reform
Committee on Homeland Security
Committee on House Administration
Committee on International Relations
Committee to Investigate the Preparation for and
Response to Hurricane Katrina
Committee on the Judiciary
Committee on Resources
Committee on Rules
Committee on Science
Committee on Small Business
Committee on Standards of Official Conduct
Committee on Transportation and Infrastructure
Committee on Veterans' Affairs
Committee on Ways and Means
Permanent Select Committee on Intelligence

Office of the Sergeant at Arms
Immediate Office
Chamber Security
Capitol Guide Service and Congressional Special
Services Office
House Garages and Parking Security

Chief Administrative Officer (CAO)
Immediate Office
Press Gallery
Periodical Press Gallery
Radio/TV Correspondents' Gallery
CAO Business Improvement Team

House Information Resources
Client Services Group
Communications Group
Information Management

Office of Human Resources
Office of Employee Assistance
ADA Services
Office of Personnel and Benefits
Child Care
Office of Administration
Outplacement Services
Office of Training
Payroll
Office of Member Services

Leadership Offices

Office of the Speaker
Office of the Majority Leader
House Majority Whip
Office of the Democratic Leader
Democratic Whip
House Republican Conference
House Republican Policy Committee
Democratic Caucus

House Support Services (HSS)
Contractor Management
Furniture Support Services
House Office Service Center
First Call Customer Service Center
House Gift Shop
Mail List/Processing/ Mass Mail
Office Supply Service
Office Services
Special Events

Officers and Legislative Offices

Office of the Clerk
~~Immediate Office~~
~~Office of History and Preservation~~
~~Office of House Employment Counsel~~
~~House Page Program~~

House Recording Studio	House Recording Studio
Operations Support Center	Page School Revolving Fund
Acquisition and Account Management	
Central Receiving/Warehouse	Office of the Chaplain
Logistics and Distribution	Office of Interparliamentary Affairs
Vendor Management	Parliamentarian
Production Management	Office of the Parliamentarian
Photography	Compilation of Precedents
	Office of the Law Revision Counsel
Office of Finance and Procurement	Office of the Legislative Counsel
Accounting	Office of the General Counsel
Budget	Office of Inspector General
Financial Counseling	Office of Emergency Planning, Preparedness and
Financial Systems	Operations
Procurement	Office of House Historian
	Technical Assistants to the Attending Physician
Revolving Funds	Congressional Executive Commission on the
Child Care Center	People's Republic of China
House Services	Commission on Security and Cooperation in Europe
House Beauty Shop	
House Barber Shop	
House Restaurant	
Stationery	
	Joint Functions
	Office of the Attending Physician
	Joint Committee on Taxation

Consolidating Statements

U.S. House of Representatives
Consolidating Statement of Financial Position
as of December 31, 2005

	<u>Members</u>	<u>Committees</u>
ASSETS		
Fund Balance with U.S. Treasury	\$ 506,764,522	\$ 116,223,325
Cash	<u>0</u>	<u>0</u>
Fund Balance with U.S. Treasury and Cash	506,764,522	116,223,325
Accounts Receivable, Net	441,254	56,968
Interoffice Receivable	59,555	0
Advances and Prepayments	3,106,944	606,300
Inventory	0	0
Property and Equipment, Net	<u>380,630</u>	<u>3,321,144</u>
Total Assets	<u>\$ 510,752,905</u>	<u>\$ 120,207,737</u>
LIABILITIES AND NET POSITION		
Accounts Payable	\$ 15,766,497	\$ 1,140,803
Interoffice Payable	1,508,670	146,864
Capital Lease Liabilities	0	0
Accrued Funded Payroll and Benefits	7,803,307	9,230
Accrued Unfunded Annual Leave and Workers' Compensation	4,738,801	1,471,390
Deferred Credits	0	0
Unfunded Workers' Compensation Actuarial Liability	0	0
Other Liabilities	<u>0</u>	<u>0</u>
Total Liabilities	<u>29,817,275</u>	<u>2,768,287</u>
Unexpended Appropriations	485,322,151	115,609,201
Cumulative Results of Operations	<u>(4,386,521)</u>	<u>1,830,249</u>
Total Net Position	<u>480,935,630</u>	<u>117,439,450</u>
Total Liabilities and Net Position	<u>\$ 510,752,905</u>	<u>\$ 120,207,737</u>

<u>Leadership Offices</u>	<u>Officers and Legislative Offices</u>	<u>Joint Functions</u>	<u>Eliminations</u>	<u>Combined</u>
\$ 18,102,380	\$ 470,841,893	\$ 10,131,176	\$ 0	\$ 1,122,063,296
0	9,091	0	0	9,091
<u>18,102,380</u>	<u>470,850,984</u>	<u>10,131,176</u>	<u>0</u>	<u>1,122,072,387</u>
21,633	92,443	368	0	612,666
0	1,801,213	0	(1,860,768)	0
122,270	4,310,593	162,808	0	8,308,915
0	951,865	0	0	951,865
304,077	47,582,077	1,185,342	0	52,773,270
<u>\$ 18,550,360</u>	<u>\$ 525,589,175</u>	<u>\$ 11,479,694</u>	<u>\$ (1,860,768)</u>	<u>\$ 1,184,719,103</u>
\$ 115,403	\$ 28,329,343	\$ 43,940	\$ 0	\$ 45,395,986
51,078	146,510	7,646	(1,860,768)	0
0	1,242,379	0	0	1,242,379
1,192	6,021	535	0	7,820,285
188,630	3,765,763	40,803	0	10,205,387
0	4,009,194	0	0	4,009,194
0	18,225,352	0	0	18,225,352
0	294,159	0	0	294,159
<u>356,303</u>	<u>56,018,721</u>	<u>92,924</u>	<u>(1,860,768)</u>	<u>87,192,742</u>
18,078,610	427,526,427	10,130,381	0	1,056,666,770
115,447	42,044,027	1,256,389	0	40,859,591
<u>18,194,057</u>	<u>469,570,454</u>	<u>11,386,770</u>	<u>0</u>	<u>1,097,526,361</u>
<u>\$ 18,550,360</u>	<u>\$ 525,589,175</u>	<u>\$ 11,479,694</u>	<u>\$ (1,860,768)</u>	<u>\$ 1,184,719,103</u>

U.S. House of Representatives
Consolidating Statement of Operations
for the Year Ended December 31, 2005

	<u>Members</u>	<u>Committees</u>
REVENUE AND FINANCING SOURCES		
Revenue from Operations		
Sales of Goods	\$ 0	\$ 0
Sales of Services to Federal Entities	0	0
Sales of Services to the Public	0	0
Interoffice Sales	0	0
Other Revenue	0	0
Total Revenue from Operations	<u>0</u>	<u>0</u>
Financing Sources		
Appropriations to Cover Expenses:		
Appropriations Received	755,611,533	190,757,443
Appropriations Yet To Be Received	1,763,477	557,935
Imputed Financing Source	34,733,507	10,364,889
Total Revenue and Financing Sources	<u>\$ 792,108,517</u>	<u>\$ 201,680,267</u>
EXPENSES		
Personnel Compensation	\$ 452,121,009	\$ 123,717,485
Benefits	185,133,186	51,801,812
Postage and Delivery	23,224,468	23,663
Repairs and Maintenance	25,164,219	4,402,193
Depreciation and Amortization	400,221	1,507,263
Rent, Utilities, and Communications	24,399,128	75,019
Telecommunications	14,401,949	1,603,977
Supplies and Materials	9,572,276	1,379,694
Travel and Transportation	22,367,323	9,363,769
Contract, Consulting, and Other Services	8,533,845	6,294,860
Printing and Reproduction	18,688,837	130,900
Subscriptions and Publications	8,079,356	1,268,458
Cost of Goods Sold	0	0
(Gain)/Loss on Disposal of Assets	22,700	111,174
Bad Debts	0	0
Interest on Capital Leases	0	0
Total Expenses	<u>\$ 792,108,517</u>	<u>\$ 201,680,267</u>
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	<u>\$ 0</u>	<u>\$ 0</u>
CHANGE IN NET POSITION		
Net Position, Beginning Balance	\$ 456,256,071	\$ 110,397,423
Adjustments	0	0
Net Position, Beginning Balance	456,256,071	110,397,423
Excess (Shortage) of Revenue and Financing Sources over Total Expenses	0	0
Plus (Minus) Non-Operating Changes	24,679,559	7,042,027
Net Position, Ending Balance	<u>\$ 480,935,630</u>	<u>\$ 117,439,450</u>

Leadership Offices	Officers and Legislative Offices	Joint Functions	Eliminations	Combined
\$ 0	\$ 3,008,449	\$ 0	\$ 0	\$ 3,008,449
0	6,226,875	0	0	6,226,875
0	658,314	111,849	0	770,163
0	32,882,759	0	(32,882,759)	0
0	610,756	0	0	610,756
0	43,387,153	111,849	(32,882,759)	10,616,243
26,249,544	218,214,694	13,244,576	0	1,204,077,790
122,479	(70,980)	32,927	0	2,405,838
1,338,105	6,761,801	600,136	0	53,798,438
<u>\$ 27,710,128</u>	<u>\$ 268,292,668</u>	<u>\$ 13,989,488</u>	<u>\$ (32,882,759)</u>	<u>\$ 1,270,898,309</u>
\$ 15,965,121	\$ 80,709,160	\$ 7,164,846	\$ 0	\$ 679,677,621
6,746,467	33,218,309	3,120,844	0	280,020,618
15,754	378,719	5,492	0	23,648,096
787,324	20,907,473	471,960	0	51,733,169
224,262	18,922,103	462,725	0	21,516,574
64,960	1,593,370	435	0	26,132,912
817,020	12,441,621	106,808	0	29,371,375
783,899	4,343,795	473,926	0	16,553,590
1,453,431	1,777,328	36,332	0	34,998,183
403,870	51,011,148	1,853,860	0	68,097,583
87,362	99,466	3,900	0	19,010,465
323,634	488,076	176,511	0	10,336,035
0	41,314,373	0	(32,882,759)	8,431,614
37,024	45,710	0	0	216,608
0	127,971	0	0	127,971
0	240,136	0	0	240,136
<u>\$ 27,710,128</u>	<u>267,618,758</u>	<u>\$ 13,877,639</u>	<u>\$ (32,882,759)</u>	<u>\$ 1,270,112,550</u>
<u>\$ 0</u>	<u>\$ 673,910</u>	<u>\$ 111,849</u>	<u>\$ 0</u>	<u>\$ 785,759</u>
\$ 17,089,291	\$ 460,732,722	\$ 11,028,066	\$ 0	\$ 1,055,503,573
0	0	0	0	0
17,089,291	460,732,722	11,028,066	0	1,055,503,573
0	673,910	111,849	0	785,759
1,104,766	8,163,822	246,855	0	41,237,029
<u>\$ 18,194,057</u>	<u>\$ 469,570,454</u>	<u>\$ 11,386,770</u>	<u>\$ 0</u>	<u>\$ 1,097,526,361</u>

U.S. House of Representatives
Consolidating Statement of Cash Flows
for the Year Ended December 31, 2005

	<u>Members</u>	<u>Committees</u>
CASH FLOWS FROM OPERATING ACTIVITIES		
Excess/(Deficiency) of Revenue and Financing Sources over Expenses	\$ 0	\$ 0
Adjustments affecting Cash Flow		
Appropriations Affecting Cash	(547,015,822)	(144,901,759)
(Increase)/Decrease in Accounts and Interoffice Receivable	(425,615)	(50,088)
(Increase)/Decrease in Advances and Prepayments	21,496	126,241
(Increase)/Decrease in Inventory	0	0
Increase/(Decrease) in Accounts and Interoffice Payable	6,893,365	(231,379)
Increase/(Decrease) in Other Accrued Liabilities	1,145,485	330,133
(Gain)/Loss on Disposal of Assets	22,700	111,174
Depreciation and Amortization	400,221	1,507,263
	<u>(538,958,170)</u>	<u>(143,108,415)</u>
Net Cash Provided/(Used) by Operating Activities		
CASH FLOWS FROM INVESTING ACTIVITIES		
Purchase of Property and Equipment	<u>(97,010)</u>	<u>(805,334)</u>
Net Cash Provided/(Used) by Investing Activities	<u>(97,010)</u>	<u>(805,334)</u>
CASH FLOWS FROM FINANCING ACTIVITIES		
Appropriations	557,995,569	149,057,836
Funds Returned to the U.S. Treasury	(1,574,030)	(617,164)
Appropriated Funds Allocated	15,166,789	3,195,175
Principal Payment on Capital Lease Liabilities	<u>0</u>	<u>0</u>
Net Cash Provided/(Used) by Financing Activities	<u>571,588,328</u>	<u>151,635,847</u>
Net Cash Provided/(Used) by Operating, Investing, and Financing Activities	32,533,148	7,722,098
Fund Balance with U.S. Treasury and Cash, Beginning	<u>474,231,374</u>	<u>108,501,227</u>
Fund Balance with U.S. Treasury and Cash, Ending	<u>\$ 506,764,522</u>	<u>\$ 116,223,325</u>

Leadership Offices	Officers and Legislative Offices	Joint Functions	Eliminations	Combined
\$ 0	\$ 673,910	\$ 111,849	\$ 0	\$ 785,759
(32,716,748)	(350,621,166)	(11,164,199)	0	(1,086,419,694)
(11,964)	315,192	(223)	(204,645)	(377,343)
(25,544)	580,963	(67,191)	0	635,965
0	397,796	0	0	397,796
(138,810)	6,950,702	(6,795)	204,645	13,671,728
90,535	(146,965)	18,742	0	1,437,930
37,024	45,710	0	0	216,608
224,262	18,922,103	462,725	0	21,516,574
<u>(32,541,245)</u>	<u>(322,881,755)</u>	<u>(10,645,092)</u>	<u>0</u>	<u>(1,048,134,677)</u>
<u>(95,020)</u>	<u>(14,271,865)</u>	<u>(536,897)</u>	<u>0</u>	<u>(15,806,126)</u>
<u>(95,020)</u>	<u>(14,271,865)</u>	<u>(536,897)</u>	<u>0</u>	<u>(15,806,126)</u>
18,666,118	398,472,933	10,880,922	0	1,135,073,378
(902,882)	(4,199,469)	(460,078)	0	(7,753,623)
16,013,028	(35,104,202)	729,210	0	0
0	(74,902)	0	0	(74,902)
<u>33,776,264</u>	<u>359,094,360</u>	<u>11,150,054</u>	<u>0</u>	<u>1,127,244,853</u>
1,139,999	21,940,740	(31,935)	0	63,304,050
<u>16,962,381</u>	<u>448,910,244</u>	<u>10,163,111</u>	<u>0</u>	<u>1,058,768,337</u>
<u>\$ 18,102,380</u>	<u>\$ 470,850,984</u>	<u>\$ 10,131,176</u>	<u>\$ 0</u>	<u>\$ 1,122,072,387</u>

This Page Intentionally Left Blank

**Independent Auditor's
Report on Compliance with
Laws and Regulations**

This Page Intentionally Left Blank



Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

**INDEPENDENT AUDITOR'S REPORT ON
COMPLIANCE WITH LAWS AND REGULATIONS**

To the Inspector General
U.S. House of Representatives

Cotton & Company LLP has audited the financial statements for the U.S. House of Representatives (House) as of December 31, 2005 and for the year ended, and have issued our reports thereon dated May 15, 2006. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Compliance with laws, rules, and regulations is the responsibility of the Members and administrative management of the House. As part of obtaining reasonable assurance about whether the House's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws and House rules and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. Providing an opinion on compliance with those provisions was not, however, an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.

Compliance with laws, rules, and regulations for the House is significantly different than for Executive Branch departments and agencies. First, many of the laws that apply to the Executive Branch, such as the Federal Managers' Financial Integrity Act of 1982, Government Management Reform Act of 1994, and Chief Financial Officers Act of 1990, do not apply to the House. Second, Executive Branch departments and agencies are subject to regulations that implement their authorizing statutes and to regulations imposed by other agencies, such as the Office of Management and Budget and the Office of Personnel Management. The House is subject to specific laws and its own rules and to regulations contained in its *Members' Congressional Handbook and Committees' Congressional Handbook*.

The sole, official purpose of this report is for informational use by Members of the U.S. House of Representatives, Office of the Chief Administrative Officer, and Office of Inspector General. It is not intended to be, and should not be, used by anyone other than these specified parties in an official capacity.

COTTON & COMPANY LLP

A handwritten signature in black ink, appearing to read "Matthew H. Johnson".

Matthew H. Johnson, CPA
Partner

May 15, 2006
Alexandria, Virginia

This Page Intentionally Left Blank

Independent Auditor's Report on Internal Control

This Page Intentionally Left Blank



Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL

To The Inspector General
U.S. House of Representatives

Cotton & Company LLP has examined the effectiveness of U.S. House of Representatives internal control over financial reporting as of December 31, 2005, based on *Standards for Internal Control in the Federal Government*, issued by the Comptroller General of the United States. House management is responsible for maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on the effectiveness of internal control based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and *Government Auditing Standards*, issued by the Comptroller General of the United States, and, accordingly, obtained an understanding of internal control over financial reporting; tested and evaluated design and operating effectiveness of the internal control; and performed such other procedures as considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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

In our opinion, the House of Representatives maintained, in all material respects, effective internal control over financial reporting as of December 31, 2005, based on *Standards for Internal Control in the Federal Government*.

We did note certain matters involving internal control and its operations that we consider reportable conditions under standards issued by AICPA. Reportable conditions are matters coming to our attention related to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the House's ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements. These conditions are:

- ? Weaknesses in the financial information system reduced the integrity of financial data and reporting.
- ? The financial reporting internal control framework was inadequate.

Material weaknesses are reportable conditions 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 misstatements in an amount that would be material in relation to the financial statement being audited may occur and not be detected within a

timely period by employees in the normal course of performing their assigned functions. We consider neither of these reportable conditions to be a material weakness. Additional details on the reportable conditions shown above are attached to this report.

The sole, official purpose of this report is for informational use by Members of the U.S. House of Representatives, Office of the Chief Administrative Officer, and Office of Inspector General. It is not intended to be, and should not be, used by anyone other than these specified parties in an official capacity. This report is however, available to the public for informational purposes only.

COTTON & COMPANY LLP



Mathew H. Johnson, CPA, CISA, CGFM

May 15, 2006
Alexandria, Virginia

**STATUS OF INTERNAL CONTROL WEAKNESSES
CALENDAR YEAR 2005 FINANCIAL STATEMENT AUDIT**

Cotton & Company LLP assessed the status of weaknesses identified in the Calendar Year (CY) 2004 Independent Auditor's Report on Internal Control. Implementation of the new, non-member payroll system, Paylinks, has successfully addressed a longstanding audit recommendation that the payroll system needs to be replaced. While the House continues to make progress toward implementing recommendations for other conditions, weaknesses still exist, and we recommend that the Chief Administrative Officer (CAO) continue to implement past recommendations.

Our criteria for assessing control weaknesses are provided below along with a summary status of control weaknesses and detailed descriptions of these weaknesses.

CRITERIA

In determining the status of new and existing internal control weaknesses, we applied the following criteria:

Substantial Progress	New financial system and/or new policies and procedures put in place <i>substantially</i> address the <i>more significant</i> recommendations made in the prior audit.
Some Progress	New financial system and/or new policies and procedures put in place <i>partially</i> address the <i>more significant</i> recommendations made in the prior audit.
Limited Progress	Steps taken to address <i>less significant</i> recommendations; more significant recommendations addressed only with <i>proposals</i> or <i>remain open</i> .
New Condition	Newly identified weakness.

We based our assessment of the status of prior recommendations on a review of the House's progress toward implementation. The following criteria were used to assess that progress:

Closed	The House fully implemented recommended corrective actions, or changes in House operations remedied or eliminated the need for recommended corrective action.
Substantial Progress	The House has <i>substantially</i> addressed the <i>more significant</i> aspects of the recommendation.
Some Progress	The House has <i>partially</i> addressed the <i>more significant</i> aspects of the recommendation.
Limited Progress	The House has made progress on the <i>less significant</i> aspects of the recommendation.
Not Started	The House has taken <i>no action</i> to implement the recommendation.

SUMMARY STATUS OF INTERNAL CONTROL WEAKNESSES

The following matrix provides a summary of new and existing internal control weaknesses:

Weakness	Status as of April 28, 2006			
	Substantial Progress	Some Progress	Limited Progress	New Condition
1 Weaknesses in the financial information system reduced the integrity of financial data and reporting. <i>(Reportable Condition)</i>			X	
2 The financial reporting internal control framework was inadequate. <i>(Reportable Condition)</i>			X	

STATUS OF PRIOR-YEAR RECOMMENDATIONS

With the implementation of Paylinks in CY 2005, we removed the prior-year reportable condition pertaining to replacement of the non-member payroll system. One other recommendation is, however, still not fully resolved. We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
05-HOC-07, 1.2 Develop a proposal, for Committee on House Administration approval, which corrects the payroll inefficiency of preparing and processing supplemental payroll.	Limited Progress The CAO and CHA are researching alternative procedures which will minimize the number of supplemental monthly payroll payments.	CONCURE The CAO concurs with this recommendation which corrects the payroll inefficiency in preparing and processing supplemental payroll. The CAO will work together with the OIG and OIG contract support to help analyze the various pay cycle options and their impact on reports and other payroll-related processes. The OIG support is intended to provide valuable advisory support to the CAO. Based on the findings, the CAO will develop a proposal to correct the payroll inefficiency in preparing and processing supplemental payroll. The CAO intends to develop the proposal by April 30, 2007.

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

05-HOC-07, 1.1

Replace the non-member payroll and Human Resources systems.

05-HOC-07, 1.3

Develop adequate controls to manage and account for annual and sick leave for applicable employees.

DISCUSSION OF INTERNAL CONTROL WEAKNESSES**Weakness 1: Weaknesses in the financial information system reduced the integrity of financial data and reporting.**

Summary Status: **Reportable Condition**
 Prior Condition
 Limited Progress

As part of the CY 2005 financial statement audit, we reviewed physical, logical, and management controls over CAO information systems that process and report information on the annual financial statements. We reviewed controls used to secure and safeguard financial information traveling over the CAO network and residing on House financial systems. Our audit was limited to the CAO portion of the House network (general support system) and related financial information systems.

We relied upon industry best practices, such as Control Objectives for Information and Related Technology (CobiT) and the Center for Internet Security (CIS), for review criteria. CobiT provides a framework to help meet multiple needs of management by bridging gaps among business risks, control needs, and technical issues. It provides a framework of generally accepted information system management and automated control practices and procedures that can be applied across a variety of domains and systems. The CobiT mission is to research, develop, publicize, and promote an authoritative, up-to-date, international set of generally accepted information technology (IT) control objectives for daily use by business managers and auditors. The CAO has accepted CobiT as an authoritative source of IT control and guidance.

In conducting our review, we examined internal control over IT for both the general support system and individual financial applications using Federal *Information System Controls Audit Manual* (FISCAM), an accepted IT audit methodology developed by the Government Accountability Office (GAO). We examined controls in the following six areas:

- ? **Entity-wide security program planning and management controls** to provide a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of computer-related controls.
- ? **Access controls** to limit or detect access to computer resources (data, program, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.
- ? **System software controls** to limit and monitor access to powerful programs and sensitive files that control computer hardware and secure applications supported by the system.
- ? **Service continuity controls** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed, and critical and sensitive data are protected from destruction.

-
- ? **Application software development and program change controls** to prevent implementation of unauthorized programs or modifications to existing programs.
 - ? **Segregation-of-duty controls** to provide policies, procedures, and organizational structure to prevent one individual from controlling key aspects of computer-related operations and thereby conducting unauthorized actions or gaining unauthorized access to assets or records. These controls must be applied within an application and at the mainframe and network system level.

The financial and related information systems included in our audit are below:

- ? Federal Financial System (FFS)
- ? Procurement Desktop (PD)
- ? Fixed Asset and Inventory Management System (FAIMS)
- ? Lawson Financial (Paylinks)
- ? House CAO Network

We also reviewed management actions to address prior-year recommendations. Although CAO made some progress in addressing prior-year weaknesses, 14 of 16 recommendations remain open.

Our audit identified weaknesses in all FISCAM control areas. Although none of the weaknesses discussed in this report by itself represents a reportable condition, they collectively comprise a reportable condition.

Weaknesses in each of the six FISCAM areas are discussed below.

Entity-Wide Security Program Planning and Management

CAO's information system security program policies and procedures covering its network and financial applications need improvement. We identified the following entity-wide weaknesses during our CY 2005 audit:

1. Security Awareness Training

In our CY 2004 financial statement audit report, we noted that CAO did not have a security awareness training program in place to ensure that all CAO personnel received annual security awareness training. We recommended that the CAO:

Ensure full attendance at annual security awareness training by all CAO employees and implement procedures to track attendance of the training program.

CAO implemented a security awareness training program and took steps to ensure that personnel attended training. It had not, however, instituted controls to ensure that new CAO employees and contractors attend security awareness training before being granted network access.

House Information Security Policy (HISPOL) 002.0, *General Information Security Guidelines for Protecting Systems from Unauthorized Use*, states:

Offices must keep appropriate records to institute a process of security training that users must complete before being granted access to systems, and periodically thereafter.

In addition, CobiT DS7.3, *Security Principles and Awareness Training*, states:

All personnel must be trained and educated in system security principles, including periodic updates with special focus on security awareness and incident handling.

We conducted tests to determine if new employees and contractors completed security awareness training before being granted network access. Our testing determined the following:

- ? As of the date of testing, the House had hired 30 new employees during CY 2005. None of the 30 employees tested completed security awareness training before being granted network access, as required by HISPOL 002.
- ? Of the 30 new CAO employees tested, 8 had not completed security awareness training as of December 31, 2005.
- ? Of the 22 new CAO employees who completed security awareness training in CY 2005, training was completed an average of 87 days after hire dates.
- ? CAO did not require contractors to take security awareness training.

2. Certification and Accreditation

CAO had not developed and put in place a formal certification and accreditation process. Security certification and accreditation are important activities that support a risk management process and should be an integral part of an agency's information security program. Our review of the draft Compliance Program did not identify policies or procedures that would specifically support or address steps in a certification and accreditation process.

The four certification and accreditation phases are:

- ? **Initiation Phase.** The purpose of this phase is to obtain authorizing official and senior agency information security officer agreement with the contents of the system security plan (SSP), including the system's documented security requirements, before the certification agent begins the assessment of security controls in the information system. This phase consists of three tasks:
 - ? Preparation
 - ? Notification and Resource Identification
 - ? System Security Plan Analysis, Update, and Acceptance

-
- ? **Security Certification Phase.** The purpose of this phase is to determine the extent to which security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting system security requirements. This phase also addresses specific actions taken or planned to correct security control deficiencies and reduce or eliminate known vulnerabilities in the information system.

Upon successful completion of this phase, the authorizing official will have the information needed from the security certification to determine risk to agency operations, assets, and individuals—and thus, will be able to render an appropriate security accreditation decision for the information system. This phase consists of two tasks:

- ? Security Control Assessment
- ? Security Certification Documentation

- ? **Security Accreditation Phase.** The purpose of this phase is to determine if remaining known vulnerabilities in the information system pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the information system owner will have:

- ? Authorization to operate the information system;
- ? Interim authorization to operate the information system under specific terms and conditions; or
- ? Denial of authorization to operate the information system.

This phase consists of two tasks:

- ? Security Accreditation Decision
- ? Security Accreditation Documentation

- ? **Continuous Monitoring Phase.** The purpose of this phase is to provide ongoing oversight and monitoring of security controls in the information system and inform the authorizing official when changes occur that may impact system security. This phase consists of three tasks:

- ? Configuration Management and Control
- ? Security Control Monitoring
- ? Status Reporting and Documentation

Completing security accreditation ensures that an information system will be operated with appropriate management review, have ongoing monitoring of security controls, and be reaccredited in accordance with policy. House policy requires risk assessments every 2 years or when major changes occur to a system.

Activities within the four phases include:

- ? Conducting system-level risk assessments to identify necessary operational, physical, and logical system controls.

-
- ? Agreeing on information documented in SSPs.
 - ? Conducting security control assessments to determine if documented security controls are operating as intended.
 - ? Mitigating identified weaknesses.
 - ? Updating SSPs accordingly.

Finally, the certification and accreditation process requires that management approve the system for operation in production by signing certification and accreditation statements.

We identified the following weaknesses that would be addressed with a formal security certification and accreditation process:

- o System owners have not been specifically identified and were not required to and did not sign off on systems before they were placed into production. System owners have not been identified and documented in SSPs for Paylinks, Procurement Desktop, and the network.
- o CAO had not developed and documented a SSP for its general support system (network).
- o The Paylinks SSP was not developed and finalized before Paylinks was placed into production. The final SSP is dated December 1, 2005. Security requirements should have been identified during the requirements-and-development phase of the Paylinks implementation project and documented in the SSP. The Paylinks SSP also did not include all information required by House Information Security Publication 24, *Guidelines for Developing System Security Plans.* Specific information missing from the Paylinks SSP is identified below:
 - ? The System Identification section did not include the level of information sensitivity.
 - ? The System Identification section did not include the individual or office responsible for the system.
 - ? The System Name section did not identify the system as a major application.
 - ? The General Description and Purpose section did not include the determination and description of the criticality of the system.
 - ? The Information Sensitivity section did not describe the sensitivity of the system and the information it processes. (If the system is designated sensitive, this section should also describe the estimated magnitude of harm that may result from loss or unauthorized use of the system or its information.)
 - ? The Assignment of Security Responsibility section did not document application security responsibility. (House Information Resources (HIR) is listed with security responsibility; however, HIR security is not responsible for Paylinks application security.)

-
- ? The System Interconnection section did not include sensitivity level of data processed by external systems, short discussions of major concerns or considerations in determining interconnection, or name and title of authorizing management official(s) and date of authorization.
 - ? The Risk Assessment section did not provide the estimated completion date of a Human Resources Paylinks risk assessment.
 - ? The Planning for Security in the Systems Development Life Cycle section did not outline the structured process of planning adequate and cost-effective security protection for the system throughout the system development life cycle (SDLC).
 - ? The Production Input and Output Controls section did not document control mechanisms used in processing, storing, and disposing of information media.
 - ? The Software and Maintenance Controls Data Integrity/Validation Controls section did not document how to manage emergency software fixes, software owner, and copyright information.
 - ? The Documentation section was not included to identify all completed system documentation and physical locations of such documentation or identify system documentation not yet completed along with estimated completion dates.
 - ? The User Identification and Authentication section did not include password change frequency and the process for authenticating UNIX accounts.
 - ? The Logical Access Controls section did not include policies regulating how users can delegate access permissions or make copies of files or information accessible to other users and how often Access Control Lists are reviewed to identify and remove users who have left the organization or whose duties no longer require system access.
 - ? The Audit Trail section described logging and monitoring events at the operating-system level, but did not address logging and monitoring of application and database activities or describe which activities should be logged and monitored on a regular basis.
- o Risk assessments or security audits (other than operating-system level) were not performed on Paylinks before it was placed in production. Specifically, security audits were not performed at the database, application, and management levels.
 - o Procurement Desktop, FAIMS, FFS, Paylinks, and the network have not been formally certified and accredited.

HISPOL 002.1, Section 2.4, System Security Plan, states:

Prior to authorization for connection to networks or operation of major applications, each system's security policy and procedural rules should be developed and documented. The security policy and procedural rules should be implemented, and processes defined to monitor security to ensure reasonable and effective management of the system and compliance with the system security plan.

HISPOL 003.0 states:

Audits are conducted on new systems prior to implementation and on existing systems every two years. Systems that undergo major modifications will also be reviewed prior to implementation. If an audit reveals significant vulnerabilities, corrective action must be taken within the time period specified by the HIR Information Systems Security Office.

3. Rules of Behavior

CAO personnel and contractors with access to the House network and financial applications were not required to sign system rules of behavior. HISPOL 002.0 documents Principles of Behavior for General Use of House Information Systems and Principles of Behavior for Special Circumstances and provides House network users with general House Information Security Rules of Behavior. Further, it is published on the House intranet, and security awareness training includes a recommendation that HISPOLs and HISPUBs be followed. The House did not, however, require its employees and contractors to provide signed statements acknowledging that they had received, read, and agreed to the House Network Rules of Behavior (the House's Principles of Behavior).

While CAO has made improvements in this area, we recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>1. Develop, document, and implement procedures to ensure that all new CAO employees and contractors complete security awareness training within 30 days after being granted access to the network and financial applications.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation for all employees and contractors utilizing the House network and CAO supported financial applications to receive security awareness training. The CAO provides annual security awareness training online and through the House Learning Center. Most users take advantage of the online option, which requires a network account. To ensure timely completion of the training by new network account holders, the CAO will modify the notification process and ensure new employees complete security awareness training within 30 days after receiving a network account. The CAO will implement this modification for CAO employees by December 31, 2006. Contingent on availability of funding through the CAO unfunded process, the CAO will incorporate contractors into this process by May 31, 2007.</p>

Recommendation	Status of Recommendation	Management Response
<p>2. Develop, document, and implement a formal certification and accreditation program to achieve:</p> <ul style="list-style-type: none"> ? Certification and accreditation of the general support system and all major financial applications. ? Recertification every 3 years or when major changes occur. ? Development of a SSP for the House general support system (network) to include requirements identified in HISPUB 024. ? Identification of system owners and administrators including security administrators. <p>Developing and fully implementing a formal certification and accreditation process should help resolve prior-year recommendations.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation to establish a formal certification and accreditation program and to certify the general support system (network) and financial systems. The CAO has established the Security Compliance Program, documented in House Information Security Policy 007, which requires initial certification and subsequent two-year recertification of systems. The CAO is in the process of completing formal certification of all financial systems, including cited deliverables. Given the complexity of the House network, the CAO will complete its certification in phases. The first phase will include a baseline System Security Plan and a plan for completing the remaining phases. The CAO will have taken the appropriate actions to close this recommendation by August 31, 2007.</p>
<p>3. Require all CAO employees and contractors users of the Network/Financial systems to read and sign expected rules of behavior annually as part of security awareness training. Signed statements should be retained for future use if necessary.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation to require CAO employees and contractors that have been provided access to the CAO network and/or a CAO supported financial system to read and sign expected rules of behavior. Such documentation of users' acceptance of rules of behavior is outlined in the System Security Plan for each specific financial system. The CAO is in the process of acquiring user documentation for each financial system and the general support system. Once completed, the CAO believes these actions will sufficiently mitigate the risk identified. The CAO will explore ways to require all employees and contractors to read and sign expected rules of behavior annually as resources become available. The CAO will have acquired all user documentation for the aforementioned systems by May 31, 2007.</p>

The following audit recommendations were made in past Office of the Inspector General (OIG) audit reports. Based on tests conducted during CY 2005, the underlying weakness of these recommendations still exists. To resolve them, we recommend that CAO continue to implement the partially resolved recommendations.

Recommendation	Status of Recommendation	Management Response
<p>03-HOC-05 3.02 Establish a compliance program that would monitor and report on CAO business units' compliance with HISPOL and CAO policies for implementing computer security controls at the financial application level.</p>	<p>Limited Progress Management established a three-phase approach to the recommendation. Phase 1 of the CAO compliance program was funded and ended January 31, 2004. The second phase has started and will be completed in CY 2005.</p>	<p>CONCUR. The CAO concurs with the recommendation and has completed the implementation and deployment of the Security Compliance Program. The final phase of the program was to develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.</p>
<p>04-HOC-07, 2.02 Develop, document, and put in place procedures to ensure compliance with HISPOL 003.0. These procedures should include risk assessments performed at all levels (application, database, and server) before new systems are installed and when enhancements are made to existing systems. In addition, this would include developing a schedule of risk assessments for existing and new financial systems and developing procedures to identify, implement, and track corrective actions designed to resolve weaknesses identified in the risk assessment.</p>	<p>Limited Progress Policies and procedures have not been finalized and put in place. Risk assessments at the application level are occurring; however, we determined they are not being done consistently or effectively to ensure controls are in place and effective.</p>	<p>CONCUR. The CAO concurs with the recommendation and has completed the implementation and deployment of a Security Compliance Program. The final phase of the program was to develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.</p>
<p>04-HOC-07, 2.03 Develop procedures to ensure that system-specific security plans are developed and updated as needed to reflect changes to software, hardware, and business operations.</p>	<p>Limited Progress CAO developed and documented HISPUB 024, which identifies the information that should be included in a SSP. Procedures are not, however, in place for ensuring that security plans are developed in a timely manner and address all areas identified in HISPUB 024. A security plan has not been developed for the network, and the Paylinks security plan, which was put in place after Paylinks was in production, does not address all areas of HISPUB 024.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications required to establish system security plans for financial systems. The Paylinks system security plan has been developed and approved in this format. The CAO is currently in the process of revising existing security plans for financial systems with the new format and content, and developing a baseline System Security Plan for the general support system (network). These activities will be completed by August 31, 2007.</p>

Recommendation	Status of Recommendation	Management Response
<p>05-HOC-07, 2.02 Modify HISPUB 024 (pending) to require CAO SSPs to identify specific individuals as system and data owners.</p>	<p>Not Started HISPUB 024 does not require specific individuals be identified as system owners and our review of SSPs noted that specific individuals have not been identified.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of specific system and data owners. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.</p>
<p>05-HOC-07, 2.03 Modify HISPUB 024 to include guidance on what expected behaviors should be documented within CAO SSPs. CAO should fully implement all requirements identified in HISPUB 024 by updating CAO SSPs to comply with HISPUB 024.</p>	<p>Limited Progress The Paylinks SSP did not address HISPUB 24 in all areas.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of expected behaviors. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.</p>

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

<p>04-HOC-07, 2.01 Ensure full attendance at annual security awareness training sessions by all CAO employees and implement procedures to track attendance of the training program..</p>
--

Access Controls

Access controls over CAO major applications and the general support system were inadequate. We identified the following weaknesses:

1. Paylinks User Access Request Forms

Controls were inadequate to ensure that Paylinks access authorizations were documented on standard forms, maintained on file, approved by senior managers, and securely transferred to security personnel. Management did not document and put in place access authorization policy or procedures for the Paylinks

application before it was placed in production. As a result, we noted the following user account administration issues:

- ? Access request forms were not used to grant initial users of Paylinks access to the application. Management did not start using access request forms until the end of October 2005. Of the 45 individuals selected in our sample, 12 had completed access request forms. In addition, 55 of the 81 accounts in Paylinks at the time of our testing did not include access request forms. All individuals with access to Paylinks should have an access request form on file that shows approved access within the system.
- ? Management did not adhere to account administration procedures documented in the Paylinks SSP. Section 7.1.1, *Application User Request Form* states:

The HR PAYLINKS Application Manager requires the supervisor of each user to fill out an application user request form prior to being given access to the system.

Requests were emailed or conveyed by telephone to the administrator, who then filled out the form and processed the request. In addition, the only signature spaces on the access request form were for network, UNIX, and Lawson administrators. The access request form did not have space for the supervisor to sign when completing the form.

- ? Management had not identified a security administrator for Paylinks to review and approve all access requests and ensure that individual access in the application agreed with access requested and approved on access request forms.

2. **Periodic Account Reviews**

Controls were not adequate to ensure that Paylinks accounts were periodically reviewed and inactive user accounts monitored and removed when not needed. Management had not developed, documented, and put in place policies and procedures to ensure that owners periodically review Paylinks access authorizations to determine if they remain appropriate and ensure that inactive user accounts are monitored and removed when not needed.

3. **Terminated Employees**

Controls were not adequate to ensure that termination and transfer procedures included prompt revocation of system network access. Network accounts were not consistently disabled or deleted even though monthly notifications were sent out to notify system administrators of employee departures or retirements.

Our network account testing identified 4 of 28 accounts tested (or 14 percent) that had not been disabled or deleted as of the test, October 15, 2005. The accounts identified were open for an average of 45 days from the employee's departure date to our test date.

4. **Warning Banners**

Controls were not adequate to ensure that the opening screen viewed by CAO users (both internally and via remote access) provided a warning that the system is for authorized use only, and that user activity will be monitored. The CAO did not consistently implement use of logon warning banners. We observed computers in HIR logged onto a House server without warning banners.

HISPOL 002.0, *General Information Security Guidelines for Protecting Systems from Unauthorized Use*, specifically requires implementation of logon warning banners to notify individuals that House systems are to be used for official business only, unauthorized system use may violate House rules or United States Code, and disciplinary sanctions could result from unauthorized actions. In addition, the CAO's server checklists have specific steps for determining if a warning banner has been implemented on each server audited. This checklist, if completed properly, would have identified and corrected this weakness.

5. **Database Weaknesses**

Controls were not adequate to ensure that databases supporting House financial applications were securely configured to prohibit unauthorized or malicious activities. CAO had not developed, documented, and put in place specific procedures for auditing databases and implementing standard security configuration baselines that documented accepted database security settings. We identified the following high-risk weaknesses when performing detailed reviews of the Paylinks and PD Oracle databases:

Paylinks Oracle Database

- ? Strong passwords were not being used as required by House policy. We identified default and weak passwords.
- ? The most recent security patches had not been applied.
- ? Logging was not activated.

Procurement Desktop Oracle Database (8i)

- ? The version of Oracle being use, (8i), was unsupported.
- ? The most recent security patches had not been applied.
- ? Strong passwords were not being used, as required by House policy:
 - ? Default or weak passwords were identified.
 - ? Clear Text passwords were identified.
 - ? Old passwords were identified for 248 accounts.
 - ? Default or easily-guessed passwords for privileged accounts were identified.

6. Logging, Monitoring, and Incident Response

Controls were not adequate to ensure that unauthorized or malicious activities in Paylinks were logged, reviewed, and responded to in a timely manner. Logging, monitoring, and incident response policies and procedures for Paylinks have not been sufficiently identified, documented, and put in place. We identified the following logging and monitoring issues related to Paylinks:

- ? When Paylinks was placed into production, logging and monitoring controls were in place at the network level (Secure Enclave). Management had not, however, put in place logging, monitoring, and incident response controls for the database and application. The Paylinks SSP did not identify or discuss logging and monitoring at the application and database levels. Logging and monitoring controls identified in the SSP were related to Secure Enclave.

During our audit period, management enabled logging at the application level. Logs files were, however, too large and unorganized for management to effectively review them on a periodic basis. We did note that management was in the process of identifying and purchasing automated software to aid in the review of logs. This effort was incomplete as of December 31, 2005.

Management had not assigned responsibility for review of database and application logs. The review of logs is traditionally performed by system security administrators. Management had not identified a system security administrator for Paylinks.

U.S. House of Representatives Chief Administrative Officer IT Systems Audit Log Review Policy states:

Systems or security administrators should review audit and exception logs weekly, or more frequently in the case of mission-critical IT systems, for anomalous events such as unusual activity on user accounts, misuse of administrative privileges, and unauthorized access to sensitive files. Anomalous events should be referred to the HIR Security Office for further investigation as needed. The Security Office will conduct a semi-annual random review of audit logs for CAO-supported IT systems.

In addition, CobiT states:

IT security administration should ensure that security activity is logged and any indication of imminent security violation is reported immediately to all who may be concerned, internally and externally, and is acted upon in a timely manner.

Management controls should guarantee that sufficient chronological information is being stored in operations logs to enable the reconstruction, review and examination of the time sequences of processing and the other activities surrounding or supporting processing.

IT security administration should ensure that violation and security activity is logged, reported, reviewed and appropriately escalated on a regular basis to identify and

resolve incidents involving unauthorized activity. The logical access to the computer resources accountability information (security and other logs) should be granted based upon the principle of least privilege, or need-to-know.

Without effective logging, monitoring, and incident response controls in place, management cannot ensure that financial data processed and stored in Paylinks are accurate and authorized.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>4. a. Develop procedures to ensure that access request forms are used for granting access to Paylinks in accordance with procedures documented in the Paylinks SSP.</p> <p>b. Complete user access request forms for all individuals in Paylinks who do not have an access request form. Access request forms should document the access level each user has been authorized.</p> <p>c. Update the Paylinks user access request form to include a space for the requesting supervisor and security administrator to sign and clearly show what access in Paylinks the user has been authorized in the system.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. The CAO updated the user account request forms as requested, recertified each individual with a current user account, and follows the aforementioned procedure for new account assignment. The CAO believes we have taken appropriate action to close this recommendation.</p>
<p>5. Develop, document, and put in place policies and procedures to ensure that Paylinks accounts are periodically reviewed and disabled or deleted when no longer needed.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. The CAO has updated the Paylinks System Security Plan and Paylinks Access Control Manual to reflect the policies and procedures for review of user accounts. The CAO certified all current users of Paylinks. Further, the CAO will continue the User Account Management process to assist individual system owners in monitoring of user access to CAO maintained systems. The CAO believes we have taken appropriate action to close this recommendation.</p>

Recommendation	Status of Recommendation	Management Response
<p>6. Take steps to ensure logon warning banners are in place and operating effectively for all CAO network users.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO will ensure logon warning banners are in place for all CAO network users by November 30, 2006.</p>
<p>7. a. Develop policies and procedures to ensure that standard security configuration baselines are developed, tested, and implemented for all CAO financial applications before placing them into production.</p> <p>b. When management must configure a database against industry best practice for functionality reasons, clearly document this in the security baseline.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation to ensure standard security configuration baselines are developed, tested and implemented for all CAO financial applications. The House has established policy guidelines for systems connected to the House network. The CAO maintains systems within this policy by utilizing established standards, or baselines, and regularly testing these baselines against House approved Information Security Checklists. Further, the CAO maintains systems within strict configuration management practices documenting system configuration and change to the standard baseline required by each application. This is documented and tracked within the configuration management procedures for each system. The CAO believes these actions mitigate the risk identified; however, the CAO will take action to ensure these operational procedures are properly documented and maintained to further ensure mitigation of this risk. The CAO will document standard security configuration baselines for all financial systems by June 29, 2007.</p>
<p>8. Update Paylinks SSP to address logging and monitoring at the application and database levels. The SSP should identify what information or activities are to be logged, how long logs are to be retained, who has access to logs, and who should review logs.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation and has updated the Paylinks System Security Plan to address logging and monitoring of the system at the application and database levels. The System Security Plan is currently compliant with HISPUB 007.2.1, System Security Plan Template for Major Applications. The CAO believes we have taken appropriate action to close this recommendation.</p>

The following audit recommendations were made in past OIG audit reports. Based on tests conducted during CY 2005, the underlying weaknesses of these recommendations still exist. To resolve them, we recommend that the CAO continue to implement the partially resolved recommendations.

Recommendation	Status of Recommendation	Management Response
<p>05-HOC-07, 2.04 Take steps to ensure that all CAO network access requests are documented and retained for future reference.</p>	<p>Not Started HIR has not developed, documented, or implemented policies and procedures requiring network access requests be documented and retained.</p>	<p>CONCUR. The CAO concurs with the recommendation. The CAO intends to establish and implement a procedure for granting network access including documenting and retaining access requests. The CAO intends to take required action by May 31, 2007.</p>
<p>05-HOC-07, 2.05 Modify existing procedures to ensure that CAO system administrators are notified immediately when employees leave or are terminated from employment with the House.</p> <p>Assign responsibility for quarterly review of all CAO network accounts and require all reviews be documented for future reference. Reviewers should look for active accounts that have not been used in a specified period of time. These accounts should be followed up to determine if they are still necessary and disabled or deleted if not.</p>	<p>Limited Progress Policy was developed, documented, and finalized but not implemented.</p>	<p>CONCUR. The CAO concurs with the recommendation. The procedures to notify systems administrators have been established and implemented. Because of the natural tie between network accounts and email accounts, the CAO will conduct review and recertification of all CAO network users in conjunction with deployment of Exchange 2003. The CAO intends to establish and implement a procedure for granting network access including documenting and retaining access requests. The CAO intends to take required action by May 31, 2007.</p>
<p>05-HOC-07, 2.06 Identify and document specific activities that security administrators should be logging and reviewing on a weekly basis such as failed logon attempts, changes to security profiles, and unsuccessful attempts to access unauthorized systems or data by users and outsiders.</p>	<p>Limited Progress HISPUB 024 has a section for logging however this only partially addresses our recommendation that specific activities be identified that administrators should be logging and reviewing.</p> <p>Our recommendation is referring to specific activities the CAO requires to be logged, such as failed logon attempts. These activities should be identified in a CAO-wide policy. Security plans would include these activities and additional system-specific activities based on specific risks to the system.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of expected behaviors. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.</p>

Recommendation	Status of Recommendation	Management Response
<p>05-HOC-07, 2.07 Finalize and implement HISPUB 022.0, Computer Security Incident Management. Effective implementation would include taking steps to ensure that all CAO system administrators are aware of the HISPUB and fully understand their roles and responsibilities for identifying and reporting potential security incidents.</p>	<p>Limited Progress HISPUB 022.0 has not been approved and implemented.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. The CAO has coordinated the revisions with systems administrators and will provide formal notification when the Committee has approved the revised documents. The CAO believes we have taken appropriate action to close this recommendation.</p>
<p>05-HOC-07, 2.08 Develop and implement policies and procedures to ensure that CAO system administrators are notified, and access is removed on the same day an employee leaves or is terminated from the House.</p>	<p>Substantial Progress Policy has been finalized, but not implement at time of our audit.</p>	<p>CONCUR. The CAO concurs with the recommendation to notify systems administrators when employees depart and promptly remove access. The CAO has implemented the associated procedures. Further, the CAO re-emphasized the importance of adhering to this policy with systems administrators and Information Technology management. The CAO believes these actions mitigate the identified risk and believes we have taken the appropriate action required to close this recommendation.</p>
<p>05-HOC-07, 2.09 Document policies and procedures for granting emergency and temporary access. Monitor emergency and temporary access, and automatically terminate access after a predetermined period when possible.</p>	<p>Not Started No policies or procedures (draft or final) were provided for review.</p>	<p>CONCUR. The CAO concurs with the recommendation and intends to document the requested policies and procedures for granting temporary and emergency access by May 31, 2007.</p>

Systems Software Controls

Management had not developed, documented, and implemented security configuration baselines for the Windows and UNIX operating systems supporting Paylinks, and controls over these systems are inadequate. A security configuration baseline documents management-approved security controls of a production system by documenting the details of system-unique hardware and software configurations. A security configuration baseline also documents any risky settings or services that are used for business purposes and compensating controls that are in place.

Management should conduct periodic audits of the production system against the security configuration baseline, and document deviations from the approved baseline. HIR operating system checklists do not qualify as a security configuration baseline for an individual system because the checklists provide only a generic list of recommended security settings for a system software component, such as an operating system or web server.

With the assistance the OIG, we performed detailed scans of the Paylinks UNIX and Windows operating systems. These scans identified weaknesses in the UNIX operating systems, some of which were high-risk items. We also reviewed audit checklists completed by HIR on these servers. The checklists were not always completed in accordance with House procedures, and security audits were not always appropriately documented. Also, the checklists did not always reflect the current UNIX operating system configuration.

For example, we identified one server that HIR approved and certified as compliant. Detailed scans revealed, however, a significant "high risk" weakness that should have prevented the server from being certified as compliant. Currently, when HIR security approves a completed audit, the system is approved for production.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
9. Ensure that security audits are performed in accordance with House Information Security Policy 007.	New Recommendation	<p>CONCUR.</p> <p>The CAO concurs with the recommendation and has implemented the Security Compliance Program as described in House Information Security Policy 007. The most mature segment of the Compliance Program ensures servers are audited prior to being placed on the network and whenever a major change occurs, and every two years thereafter. When fully mature, the newest segment of the Compliance Program will ensure database audits are conducted on applications prior to production. Currently, the affected CAO business units are working to audit and improve existing databases and to ensure appropriate security controls are included in the databases that are in development. The CAO will have taken appropriate actions to complete this recommendation by August 31, 2007.</p>

Recommendation	Status of Recommendation	Management Response
<p>10. Develop and document standard security configuration baselines for all operating systems supporting CAO financial applications. Standard security configurations should be documented and clearly show how the operating system is intended to be configured. When risky or sensitive settings or processes must be used, management should clearly document reasons in the standard security configuration baseline.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation to ensure standard security configuration baselines are developed, tested and implemented for all CAO financial applications including the operating system. The House has established policy guidelines for systems connected to the House network. The CAO maintains systems within this policy by utilizing established standards, or baselines, and regularly testing these baselines against House approved Information Security Checklists. Further, the CAO maintains systems within strict configuration management practices documenting system configuration and change to the standard baseline required by each application. This is documented and tracked within the configuration management procedures for each system. The CAO believes these actions mitigate the risk identified; however, the CAO will take action to ensure these operational procedures are properly documented and maintained to further ensure mitigation of this risk. The CAO have properly documented standard security configuration baselines for all operating systems supporting financial systems by June 29, 2007.</p>

The following audit recommendations were made in prior-year OIG audit reports. Based on tests conducted during CY 2005, underlying weaknesses of these recommendations still exist. To resolve them, we recommend that CAO continue to implement these recommendations.

Recommendation	Status of Recommendation	Management Response
<p>05-HOC-07, 2.10 Modify existing HISPUBs and develop additional policies and procedures where necessary to ensure that all blank or default passwords are identified and changed before any CAO financial system is placed into production. Include specific steps in House audit checklists for determining if blank or default passwords exist.</p>	<p>Limited Progress Audit procedures performed during our audit determined that blank and default passwords still exist in financial systems. The CAO's server checklists are not being correctly used and, therefore, are not providing assurance that default and blank passwords are changed or disabled.</p>	<p>CONCUR. The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. The CAO has also audited all financial systems under the revised policy. The CAO believes we have taken required action to close this recommendation.</p>

Service Continuity

The House had not developed, documented, and tested data center emergency procedures for the Ford data center. The House did have procedures to follow in the event of a fire, but these did not identify data center personnel responsibilities or discuss activities that personnel may need to conduct within the data center, such as shutting down equipment during an emergency. Without adequately documented and tested procedures in place, management cannot ensure that data center personnel will understand their roles and responsibilities and perform necessary tasks in the event of an emergency.

CobiT suggests that management:

Define, implement and maintain standard procedures for IT operations and ensure the operations staff is familiar with all operations tasks relevant to them. Operational procedures should cover shift handover (formal handover of activity, status updates, operational problems, escalation procedures and reports on current responsibilities) to ensure continuous operations.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>11. Develop, document, and test emergency procedures for the Ford data center.</p> <p>Ensure that procedures include specific steps to take in the data center during an emergency and identify who is responsible for taking such steps. Address activities such as emergency shut down of systems and responding to fires or water leaks.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. Currently the CAO is renovating the Ford Data Center and operating at partial capacity. In an effort to mitigate this risk, individual system owners have established and tested emergency fail over procedures. To prepare for full capacity operations, the CAO is establishing, documenting, and testing emergency procedures for the Ford Data Center as part of the reconstitution phase of the renovation. The CAO will have these procedures in place by November 30, 2007.</p>

The following audit recommendation was made in a prior-year OIG audit report. Based on tests conducted during CY 2005, the underlying weakness of this recommendation still exists. To resolve it, we recommend that the CAO continue to implement the partially resolved recommendation.

Recommendation	Status of Recommendation	Management Response
<p>02-HOC-06, 4.5</p> <p>Coordinate contingency planning and recovery policies and procedures to ensure a comprehensive approach that includes the network, mainframe computer, FFS, PD, and all critical financial systems.</p>	<p>Limited Progress</p> <p>HIR is developing a new alternative recovery site and new recovery procedures and processes.</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation and is in the process of developing recovery procedures and processes for the alternative site. The CAO will have taken the necessary action to close this recommendation by December 31, 2007.</p>

Application Software Development and Program Change Control

During CY 2005, the House implemented a new staff payroll system, Paylinks. Application development and program change controls were not, however, adequate to ensure that major applications were sufficiently developed and tested before being placed into production. This implementation did not follow House SDLC policies and procedures and, as a result, significant errors in the monthly processing of payroll occurred.

To investigate and correct these errors, Office of Finance and Procurement (OFP) staff members were diverted from their regular daily responsibilities, which resulted in issues and errors in non-payroll areas as well. Further, because of problems associated with Paylinks, House management reversed its decision to change its financial reporting from calendar year to fiscal year, anticipating that problems with Paylinks would impact the House's ability to prepare timely and accurate financial statements. The House is currently identifying systems requirements for the FFS replacement, but poor planning and implementation of Paylinks raises concerns regarding the sufficiency of FFS replacement system planning.

We reviewed support for development, testing, and implementation of Paylinks and identified several instances in which security was not adequately incorporated into the system development process, as required by CAO's SDLC policy and SDLC Handbook. In addition, several items in the Paylinks production issues log suggest that adequate SDLC procedures were not implemented and followed. Specific issues we identified are discussed in the following sections.

1. Documenting Changes

Controls were inadequate to ensure that software changes were fully documented to permit them to be traced from authorization to the final approved system modification.

Support for changes made to Paylinks did not include test plans, test results, documentation of tests being approved, or documentation of program changes made. The Paylinks change request form had a space for specifying whether the developer submitted Functional/Technical specification documentation. In many cases, this section was marked "yes," but no documentation was provided. Most support for changes was in the form of emails from individuals involved.

CobiT AI7.2, Test Plan, states:

Establish a test plan and obtain approval from relevant parties. The test plan is based on organization-wide standards and defines roles, responsibilities and success criteria. The plan considers test preparation (including site preparation), training requirements, installation or update of a defined test environment, planning/performing/documenting/retaining test cases, error handling and correction, and formal approval. Based on assessment of the risk of system failure and faults on implementation, the plan should include requirements for performance, stress, usability, pilot and security testing.

2. Testing Changes

Controls were inadequate to ensure that test plan standards defining responsibilities for each party (such as users, programmers, quality assurance personnel) were developed for all levels of testing and to ensure that test plans were documented and approved, and test results were documented and reviewed.

CAO had not developed and documented test plan policies, procedures, or standards to guide individuals in developing and using test plans. It had developed policies and procedures for SDLC and configuration management. These documents did not, however, provide detail about what should be included in test plans, who should perform what actions during testing, and how test results should be documented, reviewed, and approved.

In addition, test documentation was not being included with support for changes made in production. Changes reviewed primarily consisted of change request forms and email correspondences documenting the problem being addressed.

3. Reviewing Changes

Controls were inadequate to ensure that security administrators periodically reviewed production program changes to determine if access and change controls were followed.

CAO did not have controls in place to ensure that only authorized program changes were introduced into production. It had not identified a security administrator for Paylinks to be responsible for periodically reviewing changes. The Paylinks project manager was responsible for approving all changes requested and implemented.

4. Moving Changes into Production

Controls were inadequate to ensure that a group independent of the user and programmers controlled movement of programs and data among libraries. Controls were not adequate to ensure that before-and-after images of program code were maintained and compared to ensure approval of all changes.

Controls were not in place to prohibit movement of program code into the production environment without management knowledge or approval. Although responsibility for moving program changes was assigned, management did not have controls in place to ensure that all changes were authorized before moved into production.

We identified five individuals with the ability (SuperUser) to move changes into production. When changes were moved into production, management was alerted only if the individual moving the change notified management. Paylinks does not log when changes are introduced into production.

5. System Development, Testing, and Implementation

Controls were not adequate to ensure that Paylinks was adequately developed and tested before being placed into production. Management did not follow industry best practices and documented House SDLC

Issue No.	Description	Estimated Completion Date
107	Establish a help desk	January 1, 2006
209	Document payroll data entry processes and procedures for compliance and effectiveness.	February 15, 2006
210	Document payroll auditing process and procedures to ensure integrity of data entered.	January 9, 2006
204	Determine who can use the reversal-of-personnel-actions function in the system.	January 20, 2006
327	Formalize access control/account management processes and procedures.	January 12, 2006
406	Determine if FMS data conversion issues exist through the reconciliation process. History records from FMS were never fully reconciled to Lawson. Data loaded into Lawson did not agree with amounts paid to the IRS via the 941.	January 9, 2006
501	Define and document policies and procedures in support of Lawson staff training and identify training needs, define training plan, and train users to use Lawson for their core functions.	February 1, 2006
305	Determine if audit log for Lawson/Oracle exists and can be used.	December 31, 2005
306	Institutionalize system change control, establish and implement initial procedures).	October 31, 2005

Without a clear process for identifying and documenting system requirements (including security requirements) and incorporating them into the system under development, management cannot ensure that the system will meet user needs when in production. In addition, without adequate testing and identification of go/no-go criteria, management cannot make an informed decision on whether to move a system into production without subjecting the system and data to excessive or unacceptable levels of risk.

As a result of the inadequate application development and program change controls over Paylinks, numerous errors occurred in the monthly processing of payroll transactions that may not have occurred if Paylinks been developed and tested in accordance with House policies and procedures. Errors include the following:

- ? House contribution data totaling \$7,719,248 for Thrift Savings Plan and Basic Life insurance was not converted from FMS to Paylinks, but should have been to prepare accurate yearend reports.
- ? The Paylinks process for capturing military leave did not support the House's tracking and reporting needs.
- ? The longevity tracker system for House Officer employee longevity contained erroneous dates.
- ? Payroll data entry procedures were not developed during planning and implementation.
- ? Payroll auditing processes and procedures to ensure data integrity were not developed during planning and implementation.
- ? Incorrect Federal tax withholdings from employee pay checks occurred.
- ? Processes and procedures for issuing earnings statements for manual checks were not developed.

- ? An excessive number of employees have system permissions to reverse personnel actions in Paylinks.
- ? Plans for issuing and compiling employee W-2s were not developed to address data discrepancies between individual Lawson reports (PR 941 and other Paylinks reports).
- ? Thrift Savings Plan earnings for 317 House employees were lost.
- ? Incorrect life benefit data were reported to the Office of Personnel Management as the result of inadequate reconciliation of Paylinks reports (PR 141 and 2812 reports).
- ? During the September 2005 payroll cycle, the House made overpayments of \$550,968 to 278 employees. Payroll counselors detected the error during the payroll certification validation process, and the House decided to perform an Electronic Funds Transfer (EFT) pullback of overpayments. Shortly after the pullback was accomplished, it was determined that the House pulled back too much money for 174 of the 278 employees, resulting in an underpayment to some employees.

To resolve these errors, OFP staff members were directed away from their daily responsibilities to resolve payroll issues, thus increasing the risk of error in their other areas of responsibility. One such area was monthly reconciliations between House records and Treasury records for Fund Balance with Treasury (FBWT). Differences were not resolved in a timely manner, because OFP was addressing more immediate Paylinks issues.

Finally, another effect of the Paylinks issues impacted the House decision to change its yearend reporting date. In early 2005, House management decided to move its financial reporting yearend from December 31 to September 30. This decision was primarily to align the House financial reporting with the Federal Government funding of House operations.

OFP devoted numerous hours in preparing for the change and developing prior-year financial reports (as of September 30th) and had made considerable progress. When issues with Paylinks became apparent, House management decided to retain the current yearend to allow additional time to correct errors and lessen the impact on the House's ability to prepare timely and accurate financial statements.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
12. Require that functional/ technical specification documentation submitted by the developer be attached or included with change request forms and other documentation supporting changes to Paylinks.	New Recommendation	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. The CAO has revised change management procedures and updated the Paylinks Configuration Management plan accordingly. Additionally, the CAO is following the revised procedures for new changes to Paylinks. The CAO believes we have taken appropriate action to close this recommendation.</p>

Recommendation	Status of Recommendation	Management Response
<p>13. Develop procedures to ensure that test plans and results for changes are documented and included with other documentation supporting changes to Paylinks.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation. The CAO has established procedures to fully document changes to Paylinks and is following these procedures for new changes to Paylinks. The CAO believes we have taken the appropriate action to close this recommendation.</p>
<p>14. Develop and document detailed test plan standards that define responsibilities for all personnel (users, programmers, quality assurance), require all test plans be approved, and require test results be documented and approved.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with this recommendation. The CAO has established, documented, and communicated a revised Test Plan template, including procedures to assure delineation of responsibilities and requiring approval of the plan and test results by the test and quality assurance officer. The CAO believes we have taken appropriate action to close this recommendation.</p>
<p>15. Develop, document, and implement controls to ensure that only authorized and approved changes to Paylinks are introduced into production.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation and has updated the configuration management and change control procedures for Paylinks accordingly. Standard operating procedures for moving code from one environment to another have been established and documented. The CAO believes we have taken appropriate action to close this recommendation.</p>
<p>16. Periodically review production program changes to ensure that access and change controls are being followed.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO concurs with the recommendation. As part of fully implementing the CAO Configuration Management program, Paylinks has updated a Configuration Management Plan that establishes program change procedures and review. These procedures include routine review of program changes with the Technology Advisory Board, previously the Engineering Review Board, and participation in an annual, internal Configuration Management audit. An internal audit is scheduled</p>

Recommendation	Status of Recommendation	Management Response
		for the first quarter of FY2007. With completion of this internal audit and action taken on any resulting recommendations, the CAO believes we will have mitigated the identified risk. Access control changes have been addressed with the development of access control processes, access requests retained in an access control manual, and the recertification of all current users. The CAO will complete the required action to close this recommendation by July 9, 2007.
17. Develop, document, and implement controls over movement of program changes for Paylinks. Controls should be adequate to ensure that only authorized changes are moved into production, and management is notified.	New Recommendation	CONCUR. The CAO concurs with the recommendation and has updated the configuration management and change control procedures for Paylinks accordingly. Standard operating procedures for moving code from one environment to another have been established and documented. The CAO believes we have taken appropriate action to close this recommendation.
18. Develop and implement procedures to ensure that systems are developed and tested in accordance with House SDLC requirements and industry best practices, particularly in light of the forthcoming FFS replacement.	New Recommendation	CONCUR. The CAO concurs with the recommendation and is in the process of presenting the Committee on House Administration with a new policy to replace current House Systems Development Life Cycle policy. This new policy address the project management and systems development life cycle best practices referred to in this recommendation. Concurrently the CAO has established policies and procedures; and deployed, and committed resources to sustaining, a project management oversight methodology that ensures compliance with House and CAO policy. The CAO will complete the required actions to close this recommendation by December 29, 2006.

Recommendation	Status of Recommendation	Management Response
<p>19. Continue to address and resolve existing issues resulting from processing errors that occurred in Paylinks.</p>	<p>New Recommendation</p>	<p>CONCUR. The CAO continues to address and resolve all Paylinks-related processing errors identified in the financial statement audit. New policies and procedures have been put into place and corrective action has been taken in these areas:</p> <ul style="list-style-type: none"> ? Conversion Issues related to TSP and Basic Life Insurance ? Recording of Military Leave ? Erroneous dates related to longevity ? Procedures related to payroll data entry and payroll auditing ? Federal tax withholding ? Earnings statements for manual checks ? Reduced system access for employees ? Issuance of W-2 forms ? Payroll overpayments <p>The CAO believes we have taken the appropriate action to close this recommendation.</p>

Segregation-of-Duty Controls

CAO policy, procedures, and practices for implementing and enforcing segregation-of-duty controls over financial applications were inadequate. Policies and procedures have not been developed, documented, and implemented to ensure that CAO financial systems identify incompatible duties and enforce segregation-of-duty controls. Segregation-of-duty issues are described below:

1. Weak Segregation-of-Duty Controls in Paylinks

System administration and end-user personnel had excessive access in Paylinks. Management did not sufficiently identify, incorporate, and test segregation-of-duty controls before placing Paylinks into production. We identified the following specific segregation-of-duty control weaknesses within Paylinks:

- ? **Security Classes Identified and Tested in Development.** Before Paylinks was moved into production, an independent contractor identified and tested seven security classes to which users were to be assigned in Paylinks. These seven security classes did not address system support functions, including account administration and security administration, and did not address all financial activities that users perform in Paylinks, such as reversals.
- ? **Security Classes in Production.** When Paylinks was moved into production, users were not assigned to security classes originally documented and tested. Instead, users were assigned to one

of three security classes, SuperUser, Open, and V-only (view only), thus minimizing segregation-of-duty controls. These three security classes did not sufficiently segregate duties according to individual job responsibilities.

- ? **System Administrator Access.** System administrators (Application) had full access (SuperUser) in Paylinks. In addition, management had not identified or assigned a security administrator to review activities of personnel with SuperUser access.
- ? **Database Administrator Access.** Two database administrators had SuperUser access in the application.
- ? **UNIX Administrator Access.** Two UNIX administrators had SuperUser access in the application.
- ? **Programmer Access.** One account titled programmer was in the production environment. Programmers should not be given access to production unless absolutely necessary. If such access is required, management should have sufficient compensating controls in place to ensure that only authorized activities take place.

OFP had guidelines addressing segregation of duties titled *U.S. House of Representatives Office of Finance and Accounting Department Segregation of Financial Duties Guidelines*. This document did not, however, address segregating payroll and personnel duties or Paylinks.

2. Segregation-of-Duty Resources and Training

Senior management did not provide adequate resources and training to ensure that segregation-of-duty principles were understood and established, enforced, and institutionalized within the House. Policies and procedures to ensure that segregation-of-duty principles are understood, established, and enforced did not exist. Also, senior management had not identified specific individuals responsible for ensuring that adequate resources and training on segregation-of-duty principles were understood, established, enforced, and institutionalized within the organization.

Management involved in developing and implementing Lawson Financials/Paylinks did not take sufficient steps to ensure that segregation-of-duty principles were identified, documented, and implemented before the system was placed in production.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
20. Develop, document, and implement policies and procedures to ensure that CAO financial systems identify incompatible duties and enforce segregation-of-duty controls both at the end user and administrative levels.	New Recommendation	CONCUR. The CAO concurs with the recommendation. Several CAO managed financial systems have identified, documented, and enforce segregation-of-duty controls. The CAO will ensure these actions are

Recommendation	Status of Recommendation	Management Response
		<p>guided by policy requiring CAO maintained systems identify incompatible duties and establish segregation-of-duty controls at the end user and administrative levels. The CAO will place such policy into effect and complete required actions to close this recommendation by December 29, 2006.</p>
<p>21. Develop and implement procedures to ensure that segregation-of-duty principles are understood by key personnel, such as system and data owners and program managers.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. The majority of CAO managed financial systems have identified, documented and enforce segregation-of-duty controls. In accordance with CAO policy requested by Recommendation 20, the CAO will require all system owners of CAO supported systems to develop and implement procedures to ensure that segregation-of-duty principles are in effect by key personnel for each system. The Director of CABS will be responsible for the CAO systems under the CABS purview. The CAO will establish and implement recommended procedures by May 31, 2007.</p>
<p>22. Identify and document incompatible administrative and end-user duties in Paylinks.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation and has established documentation requested in an access control manual and recertified all users. The CAO believes we have taken appropriate action to close this recommendation.</p>
<p>23. Assign users in Paylinks to appropriate security classes to enforce proper segregation-of-duty controls. Follow the concept of least-privilege when assigning users to security classes. Provide users with only enough system access to perform their assigned roles or responsibilities.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation. The CAO established documentation requested in an access control manual, and recertified all users to the appropriate access roles. The CAO believes we have taken appropriate action to close this recommendation.</p>

Recommendation	Status of Recommendation	Management Response
<p>24. Remove Paylinks database and operating system administrator's access to the Paylinks application. If removal is not possible, access should be limited to only what is necessary for business purposes. In addition, compensating controls should be put in place to monitor administrator activities in the application.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the recommendation; however, the version of Lawson currently in production requires the current administrative privileges. To mitigate the identified risk, the CAO has established clear policies and procedures around access control. The CAO intends to update the production application to support the access changes required for this recommendation in fiscal year 2008. The CAO will complete required action to close this recommendation by September 28, 2008.</p>

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

<p>05-HOC-07, 2.01</p> <p>Develop, approve, and implement a system security plan for the Financial Management System. The system security plan should cover all security over the application and be approved by key affected parties.</p>
<p>03-HOC-05, 3.04</p> <p>Require all CAO business units to install security software at the work-station level or server to impose an automatic deactivation of the terminal or the user's session for user inactivity.</p>

Weakness 2: The Financial Reporting Internal Control Framework was Inadequate**Summary Status: Reportable Condition****Prior Condition - Revised Recommendation to replace CY 2004 Reportable Condition
“Procedures over Yearend Reporting and Property, Plant, and Equipment
are Weak”**

We identified numerous weaknesses in House financial management system controls and monitoring, including gaps in cross-cutting elements of internal control over financial reporting. Improvements are needed in the control environment, control activities, information and communication, and monitoring of control activities and financial transactions. The House has not placed a priority on updating policy and procedure guidance to reflect current requirements, communicating updated guidance to appropriate personnel, and ensuring its implementation.

The three primary objectives of an internal control system are to ensure:

- ? Efficient and effective operations.
- ? Accurate financial reporting.
- ? Compliance with laws and regulations.

Management support of strong internal control is critical to accurate financial reporting, because it sets the tone for the entire reporting entity. Numerous control weaknesses exist, however, within House offices that affect the accuracy and reliability of the financial statements, as well as increase control risk in the operating environment.

Best practices of the Federal Government contained in Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*, requires that agencies establish controls to reasonably ensure that:

(i) obligations and costs are in compliance with applicable law; (ii) funds, property, and other assets are safeguarded against waste, loss, unauthorized use or misappropriation; and (iii) revenues and expenditures applicable to agency operations are properly recorded and accounted for to permit the preparation of accounts and reliable financial and statistical reports and to maintain accountability over the assets.

Individually, these issues are not material to the financial statements. When taken as a whole, however, they represent widespread internal control weaknesses.

Yearend Reporting Quality Control Procedures

Yearend reporting and quality control procedures used by OFP are inadequate to ensure accurate preparation and presentation of the House's financial statements. Our audit testing disclosed the following errors:

- ? OFP incorrectly reported amounts on the Statement of Cash Flows (SCF) as the result of incorrect reporting methodology. This resulted in a \$3,198,265 understatement of the SCF in the Purchase of Property and Equipment from Investing Activities line item. The SCF was subsequently corrected.
- ? OFP erroneously reported expenses occurring in the prior year as current year transactions because of its faulty accrual calculation methodology. This resulted in the House reporting expenses related to long-term service contracts of \$206,046 on its CY 2005 financial statements which were actually incurred in CY 2004.
- ? The House has not developed policies and procedures for determining yearend accruals for expenses attributable to member and committee offices. If a member or committee office submits a voucher for payment of certain types of purchases after yearend for an expense incurred in the prior year, the expense and related payable will not be recorded in the general ledger and reported on the financial statements until the following year. This condition will result in liabilities and expenses being understated in the prior-year financial statements and overstated in the current-year financial statements.
- ? OFP oversights during financial reporting resulted in duplicate reporting of a general ledger account and an overstatement of \$1,196,796 on the SCF. The SCF was subsequently corrected.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>1. Require OFP to perform a thorough analysis of its procedures for preparing the SCF to ensure that all FFS and subsidiary ledger data are included and properly classified in the SCF.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>OFP has performed an analysis of our procedures for preparing the SCF and has modified the methodology to ensure that all FFS and subsidiary ledger data are included and properly classified in the SCF. During our review, emphasis was placed on correcting the two areas where errors were identified during the financial statement audit: changes affecting capital lease liability and property and equipment. New procedures are already in place for the next financial statement audit that will ensure that all transactions that affect the SCF, including adjusting journal entries to both FFS and financial statement software, will be presented correctly. The CAO believes we have taken the appropriate action to close this recommendation.</p>

Recommendation	Status of Recommendation	Management Response
<p>2. Require OFP to identify and implement a process to ensure a thorough review of the subsequent period to capture all financial reporting data. Document these activities in OFP policies and procedures manual.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>OFP has implemented a new process to ensure a thorough review of the subsequent period to capture all financial reporting data. The new process has already been used for the calendar year 2005 financial statement compilation. Specifically, the new process corrects a condition first identified during the calendar year 2004 financial audit whereby accounts payable were understated at year end related to service contract payments processed during the first quarter of the year subsequent to the financial statement reporting period. In addition, for future financial statement audits, OFP will use historical data to estimate accounts payable for payments processed after the normal cut-off period. This process has been documented in OFP policies and procedures. The CAO believes we have taken the appropriate action to close this recommendation.</p>

Property and Equipment Monitoring and Reporting Procedures

Capitalized and accountable property and equipment (P&E) monitoring and reporting continued to be a persistent control weakness for CAO offices. In prior-year audit reports, weaknesses in monitoring and reporting have been a consistent subject that continues into this year. CAO offices lacked adequate controls and procedures to ensure that property and equipment acquisitions, dispositions, and depreciations were recorded and reported completely and accurately. Our audit testing disclosed a number of errors:

- ? HIR did not update FAIMS with the proper operating status when it removed 148 accountable property items from operations. Eight of these items were capitalized accountable property items that were still being depreciated even though they had been removed from service.

Additionally, two of the non-capitalized accountable property items were improperly expensed by HIR, even though their individual acquisition costs were greater than the House's capitalization threshold. The overall effect of these control weaknesses resulted in understatements of capitalized property of \$122,869, accumulated depreciation of \$57,723, and depreciation expense of \$25,262.

- ? HIR and OFP in two separate instances improperly recorded the acquisition cost of capitalized security software by including maintenance expense fees in the capitalized cost. This resulted in a

total overstatement of capitalized property by \$10,466 and both accumulated depreciation and depreciation expense of \$2,560. Also, operating expense were understated by \$10,466.

- ? HIR improperly expensed 20 new property items with a total acquisition cost of \$1,109,880 that should have been capitalized. Individually, each item exceeded the capitalization threshold. The \$1,109,880 capital asset understatement resulted in understatements of accumulated depreciation and depreciation expense accounts of \$30,182 and a net overstatement of \$1,079,698 in expenses.
- ? OFP erroneously recorded in FAIMS the placed-in-service-date of a capitalized property item months after it was actually placed in service. Capitalization using an incorrect in-service date resulted in an understatement of both accumulated depreciation and depreciation expense by \$3,326.
- ? OFP improperly recorded the cost of newly acquired assets obtained through trade-in of existing assets. It included cash discounts received in the acquisition cost of assets procured in coordination with a trade-in of similar assets, which violates generally accepted accounting principles. This resulted in an overstatement of capitalized assets by \$98,928, an overstatement of both accumulated depreciation and depreciation expense by \$9,869, and an understatement of work-in-process by \$26,040.
- ? OFP did not update FAIMS with shipping-and-handling charges associated with capitalized property items, which resulted in an overstatement of the disposal losses account balance by \$29,863. OFP documented these charges on manual worksheets rather than updating FAIMS with the correct acquisition cost. Further, when the capitalized items were disposed of in FAIMS in the prior years, OFP did not dispose of the associated shipping-and-installation costs maintained on the manual worksheets.
- ? HIR delays in recording capital asset additions in FAIMS affected financial reporting. We tested capitalized property items identified by OFP as CY 2005 capital asset additions and identified \$12,075,397 of the additions with in-service dates prior to CY 2005. OFP prepared a late adjustment to the CY 2004 financial statements to record \$9,925,639 of this amount, which resulted in \$2,149,758 of capital assets as unreported. Comparisons of the HIR asset in-service date to the month FAIMS was updated showed that HIR takes an average of 5.41 months to update FAIMS once the asset is physically placed in-service.
- ? The House did not remove a capital software asset from its financial records until CY 2005, although the asset should have been disposed as of December 31, 2002. The delay in disposal resulted, in part, because disposals of software did not require a disposal request form (or other signed request), and capitalized software is not inventoried annually per Committee on House Administration rules.

This had no material effect on the financial statements, because the net book value of the capital asset is zero. Failure to promptly dispose of capital assets from the property and equipment ledger (FAIMS) and general ledger (FFS), however, causes the House to report assets that it did not own.

In addition, the House's failure to require disposal request forms, combined with the absence of a capitalized software annual inventory process, leaves the House vulnerable to misstated financial statements.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>3. Require all CAO personnel responsible for capitalized property procurement, monitoring, and reporting to attend training in generally accepted accounting principles for fixed assets.</p> <p>Prepare a memorandum to non-CAO offices responsible for purchasing capitalized property instructing them of the House's fixed-asset policies and provide training, if necessary.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The Accounting Department conducts periodic training for all CAO offices regarding the proper treatment of fixed assets and will continue to do so in the future. The appropriate personnel will be identified and training materials will be prepared and distributed to attendees on the proper treatment of budget object codes, purchases and disposals, and depreciation. Attendance will be taken for each session and compared to a list of employees responsible for capitalized property. Also, training literature will be distributed to non-CAO offices responsible for purchasing capitalized property and training will be provided to those offices as required. Training is a continual process and Accounting will work closely with all affected offices to ensure capitalized property is accounted for correctly. Accounting will conduct at least one more training class before the end of the calendar year, and will conduct training quarterly thereafter. The CAO believes we will take the appropriate action to close this recommendation by December 31, 2006.</p>
<p>4. Develop and implement a policy requiring timely updates to FAIMS for all capitalized property purchases and discontinue use of manual worksheets.</p> <p>Require OFP to revise its policies and procedures to state that assets removed from service should not be depreciated.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>HIR has revised its policies and procedures to require timely updates to FAIMS for all capitalized property purchases. OFP will work with HIR and HSS to phase out manual worksheets by transferring assets to FAIMS that are currently being tracked manually. This process will be completed by September 30, 2007. OFP has revised its policies and procedures to state that assets removed from service will not be depreciated, and will work with HIR</p>

Recommendation	Status of Recommendation	Management Response
		to identify assets that have been removed from service. The CAO believes we have taken the appropriate action to close this portion of the recommendation.
<p>5. Allow OFP staff responsible for property and equipment monitoring and reporting be granted FAIMS user access privileges to adjust capital asset costs, as necessary.</p>	<p>New Recommendation</p>	<p>CONCUR.</p> <p>The CAO concurs with the intent of this recommendation, but believes granting OFP personnel user access privileges to FAIMS could create potential internal control problems. Changes to FAIMS, whether intentional or not, could be made by OFP without the knowledge or consent of the property custodian. To address the recommendation, OFP will continue to analyze property and equipment transactions and provide direction to various CAO offices when adjustments to capital asset costs are required, and will follow up with the offices to ensure FAIMS has been updated timely. The CAO believes we have taken the appropriate action to close this recommendation.</p>
<p>6. Work with the Committee on House Administration to amend its rules and require annual inventories of capitalized internal use software. Subject capitalized software to the same acquisition, monitoring, and disposal controls as all other capitalized property.</p>	<p>New Recommendation</p>	<p>PARTIALLY CONCUR.</p> <p>HSS concurs that a process must be established to verify the inventory. However, software is an internal item, and is not physically accessible to any staff other than that of the Member/House office. Therefore, HSS cannot physically inventory this software. As an alternative, HSS recommends that the Office Coordinators send a yearly email to their House contacts to verify that each office is using the CMS software that is listed on their inventory. Verification by email exchange will ensure that offices do not have CMS software on their inventory that is no longer in use. The CAO believes we will take the appropriate action to close this recommendation, beginning with a year-end inventory in the current year, by December 31, 2006.</p>

Other Entity-Wide Control Weaknesses

Our testing revealed other matters representing entity-wide control issues that management needs to address:

- ? A House employee erroneously received a \$3,000 bonus intended for another employee as the result of a Payroll Office data entry error. This error occurred because Paylinks did not have systematic controls, and separate management reviews within the Payroll Office were not conducted. Also, the erroneous bonus resulted in the monthly salary for this employee exceeding the maximum allowable under the Speaker's Pay Order. This is a violation of House rules, but was not detected by the employing authority during review of monthly payroll exception reports.
- ? Processing errors within the Payroll Office resulted in the House withholding Virginia state tax rather than District of Columbia tax, as requested by the employee. Also, the Payroll Office miscalculated FEGLI deductions from an employee's pay check.
- ? Human Resources could not provide documents to support certain payroll and benefit deductions, and HIR was unable to provide a vendor invoice for a component of a capitalized system. As a result, we were unable to complete testing for several payroll items and one property item.
- ? Control weaknesses within Employee Services resulted in accounts receivable misstatements. As part of the September overpayment and subsequent pullback, Employee Services recorded duplicate receivables for two individuals who had not reimbursed the House for the overpayments, resulting in an overstatement of \$6,323. Also, Employee Services did not properly include three employees in its accounts receivable calculation, resulting in an understatement of \$6,828.
- ? HIR erroneously paid an invoice for capitalized property based on the obligation amount of \$312,592, rather than the vendor invoice amount of \$311,542. This resulted in overstated capitalized property of \$1,050, as well as depreciation expense and accumulated depreciation overstatements of \$379. In addition, the House overpaid the vendor by \$1,050.
- ? HIR improperly recorded the acquisition cost of a capitalized property item at the purchase order amount of \$123,858, rather than the vendor invoice amount of \$109,525. The House overstated the acquisition cost of the item by \$14,333, as well as overstatement of depreciation expense and accumulated depreciation by \$5,176.

We recommend that the Chief Administrative Officer:

Recommendation	Status of Recommendation	Management Response
<p>7. Investigate the design of controls over (1) payroll data entry and other Human Resource processes and management review functions; and (2) review the Over Speaker Pay Edit report process to determine where weaknesses exist so these processes may be modified to ensure that similar errors are detected and prevented in the future.</p>	<p>New Recommendation</p>	<p>CONCUR. OFP has taken the following steps to address design controls over payroll data entry and management review functions: The Office of Employee Services (OES) is developing an interactive Payroll Authorization Form that will be proposed for usage to the Committee on House</p>

Recommendation	Status of Recommendation	Management Response
		<p>? Administration. The Form will ultimately be transmitted between offices electronically resulting in a more efficient process. Coding will be more legible which should result in fewer errors and less corrections processed by payroll counselors.</p> <p>? Payroll counselors use the payroll certification and copies of the original paperwork to validate gross amounts for all pay before the final payroll is run.</p> <p>? Benefits Division personnel spot-check a sample of all Federal Employee Health Benefits (FEHB), Thrift Savings Plan (TSP) and Life Insurance Enrollment Forms for accuracy.</p> <p>? Payroll, Benefits, Document Management and the Help Desk use a custom Access Data Base to capture all incoming payroll processing documents (i.e., Appointments, Terminations, Salary Adjustments, FEHB, Life Insurance, and TSP).</p> <p>? Payroll Division performs a two-person Payroll Counselor review of all Cash Due, EFT-Pull Back of salary actions that would result in an employee overpayment.</p> <p>? Benefits Division performs a two-person Benefits Counselor review of all LWOP or adjustments that would result in a deduction not being withheld accurately.</p> <p>? OES will conduct random sample audits of the W4 forms entered for each pay period.</p> <p>? During the off cycle payroll, OES must manually compute the Federal Employee Government Life Insurance withholding. This process has been improved by checking the life insurance calculation for reasonableness as OES reviews the entire PR140 to audit gross amounts to the paperwork.</p> <p>? OES uses a tracking system for monies due back to the House for payroll overpayments which</p>

Recommendation	Status of Recommendation	Management Response
		includes a spreadsheet that tracks individual gross to net calculations and a status of whether payment has been received by the House. OES has reviewed and corrected the <i>Over Speakers Pay Edit Report</i> process to identify employees who have exceeded allowable House payroll limits. Adjustments are made accordingly before the final payroll is run. The CAO believes we have taken the appropriate action to close this recommendation.

The following audit recommendations were made in past OIG audit reports. Based on tests conducted during CY 2005, the underlying weakness of these recommendations still exists. To resolve them, we recommend that the CAO implement recommendations not yet started.

Recommendation	Status of Recommendation	Management Response
05-HOC-07, 3.1 Review and revise <i>Accounting Department Policy and Procedures</i> and <i>Accounting Department Annual Financial Statement Compilation Procedures</i> , including quality control procedures to ensure that all functions are fully and completely documented.	Not Started	CONCUR. The Accounting Department will review and revise its policies and procedures and financial statement compilation procedures as necessary to ensure that all functions are fully and completely documented. Accounting periodically updates all procedures related to both operations and financial statement preparation as various methodologies change. During our next revision, we will emphasize quality control procedures related to the financial statement compilation process to address weaknesses discovered during the financial statement audit. The CAO believes we will take the appropriate action to close this recommendation by November 30, 2006.

The following prior-year recommendations were closed when changes in House operations remedied the associated underlying weaknesses:

05-HOC-07, 3.2 Periodically assess the need for training and provide training to OFP, HIR, and HSS staff regarding proper accounting treatment of PP&E transactions.

Management Comments

This Page Intentionally Left Blank

Office of the
Chief Administrative Officer
U.S. House of Representatives
Washington, DC 20515-6860

MEMORANDUM

To: James Cornell
Inspector General

From: Jay Eagen
Chief Administrative Officer

Subject: CAO responses to *Independent Auditor's Report on Internal Control* related to the House CY2005 Annual Financial Statement Audit

Date: OCT 26 2006

Thank you for the opportunity to comment on the subject audit report. We have carefully reviewed the report's findings and recommendations and concur with each of them.

The following is a brief response to each of the audit recommendations made in the audit report:

Weakness 1: Weaknesses in the financial information system reduced the integrity of financial data and reporting.

Recommendation 1: Develop, document, and implement procedures to ensure that all new CAO employees and contractors complete security awareness training before being granted access to the network and financial applications.

CONCUR.

The CAO concurs with the recommendation for all employees and contractors utilizing the House network and CAO supported financial applications to receive security awareness training. The CAO provides annual security awareness training online and through the House Learning Center. Most users take advantage of the online option, which requires a network account. To ensure timely completion of the training by new network account holders, the CAO will modify the notification process and ensure new employees complete security awareness training within 30 days after receiving a network account. The CAO will implement this modification for CAO employees by December 31, 2006. Contingent on availability of funding through the CAO unfunded process, the CAO will incorporate contractors into this process by May 31, 2007.

Recommendation 2: Develop, document, and implement a formal certification and accreditation program to achieve:

- Certification and accreditation of the general support system and all major financial applications.
- Recertification every 3 years or when major changes occur.
- Development of a SSP for the House general support system (network) to include requirements identified in HISPUB 024.
- Identification of system owners and administrators including security administrators.

Developing and fully implementing a formal certification and accreditation process should help resolve prior-year recommendations.

CONCUR.

The CAO concurs with the recommendation to establish a formal certification and accreditation program and to certify the general support system (network) and financial systems. The CAO has established the Security Compliance Program, documented in House Information Security Policy 007, which requires initial certification and subsequent two-year recertification of systems. The CAO is in the process of completing formal certification of all financial systems, including cited deliverables. Given the complexity of the House network, the CAO will complete its certification in phases. The first phase will include a baseline System Security Plan and a plan for completing the remaining phases. The CAO will have taken the appropriate actions to close this recommendation by August 31, 2007.

Recommendation 3: Require all CAO employees and contractors to read and sign expected rules of behavior annually as part of security awareness training. Signed statements should be retained for future use if necessary.

CONCUR.

The CAO concurs with the recommendation to require CAO employees and contractors that have been provided access to the CAO network and/or a CAO supported financial system to read and sign expected rules of behavior. Such documentation of users' acceptance of rules of behavior is outlined in the System Security Plan for each specific financial system. The CAO is in the process of acquiring user documentation for each financial system and the general support system. Once completed, the CAO believes these actions will sufficiently mitigate the risk identified. The CAO will explore ways to require all employees and contractors to read and sign expected rules of behavior annually as resources become available. The CAO will have acquired all user documentation for the aforementioned systems by May 31, 2007.

Recommendation 4: 1.) Develop procedures to ensure that access request forms are used for granting access to Paylinks in accordance with procedures documented in the Paylinks SSP.
2.) Complete user access request forms for all individuals in Paylinks who do not have an access request form. Access request forms should document the access level each user has been authorized.
3.) Update the Paylinks user access request form to include a space for the requesting supervisor and security administrator to sign and clearly show what access in Paylinks the user has been authorized in the system.

CONCUR.

The CAO concurs with the recommendation. The CAO updated the user account request forms as requested, recertified each individual with a current user account, and follows the aforementioned procedure for new account assignment. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 5: Develop, document, and put in place policies and procedures to ensure that Paylinks accounts are periodically reviewed and disabled or deleted when no longer needed.

CONCUR.

The CAO concurs with the recommendation. The CAO has updated the Paylinks System Security Plan and Paylinks Access Control Manual to reflect the policies and procedures for review of user accounts. The CAO certified all current users of Paylinks. Further, the CAO will continue the User Account Management process to assist individual system owners in monitoring of user access to CAO maintained systems. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 6: Take steps to ensure logon warning banners are in place and operating effectively for all CAO network users.

CONCUR.

The CAO will ensure logon warning banners are in place for all CAO network users by November 30, 2006.

Recommendation 7: 1.) Develop policies and procedures to ensure that standard security configuration baselines are developed, tested, and implemented for all CAO financial applications before placing them into production.
2.) Review detailed scan results from PD and Paylinks database scans and develop, document, and implement standard security configuration baselines for databases supporting financial applications.
3.) When management must configure a database against industry best practice for functionality reasons, clearly document this in the security baseline.

CONCUR.

The CAO concurs with the recommendation to ensure standard security configuration baselines are developed, tested and implemented for all CAO financial applications. The House has established policy guidelines for systems connected to the House network. The CAO maintains systems within this policy by utilizing established standards, or baselines, and regularly testing these baselines against House approved Information Security Checklists. Further, the CAO maintains systems within strict configuration management practices documenting system configuration and change to the standard baseline required by each application. This is documented and tracked within the configuration management procedures for each system. The CAO believes these actions mitigate the risk identified; however, the CAO will take action to ensure these operational procedures are properly documented and maintained to further ensure mitigation of this risk. The CAO will document standard security configuration baselines for all financial systems by June 29, 2007.

Recommendation 8: Update Paylinks SSP to address logging and monitoring at the application and database levels. The SSP should identify what

information or activities are to be logged, how long logs are to be retained, who has access to logs, and who should review logs.

CONCUR.

The CAO concurs with the recommendation and has updated the Paylinks System Security Plan to address logging and monitoring of the system at the application and database levels. The System Security Plan is currently compliant with HISPUB 007.2.1, System Security Plan Template for Major Applications. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 9: Ensure that security audits are performed in accordance with House Information Security Policy 007.

CONCUR.

The CAO concurs with the recommendation and has implemented the Security Compliance Program as described in House Information Security Policy 007. The most mature segment of the Compliance Program ensures servers are audited prior to being placed on the network and whenever a major change occurs, and every two years thereafter. When fully mature, the newest segment of the Compliance Program will ensure database audits are conducted on applications prior to production. Currently, the affected CAO business units are working to audit and improve existing databases and to ensure appropriate security controls are included in the databases that are in development. The CAO will have taken appropriate actions to complete this recommendation by August 31, 2007.

Recommendation 10: Review results from detailed operating system reviews performed by the OIG and develop and document standard security configuration baselines for all operating systems supporting CAO financial applications. Standard security configurations should be documented and clearly show how the operating system is intended to be configured. When risky or sensitive settings or processes must be used, management should clearly document reasons in the standard security configuration baseline.

CONCUR.

The CAO concurs with the recommendation to ensure standard security configuration baselines are developed, tested and implemented for all CAO financial applications including the operating system. The House has established policy guidelines for systems connected to the House network. The CAO maintains systems within this policy by utilizing established standards, or baselines, and regularly testing these baselines against House approved Information Security Checklists. Further, the CAO maintains systems within strict configuration management practices documenting system configuration and change to the standard baseline required by each application. This is documented and tracked within the configuration management procedures for each system. The CAO believes these actions mitigate the risk identified; however, the CAO will take action to ensure these operational procedures are properly documented and maintained to further ensure mitigation of this risk.

The CAO have properly documented standard security configuration baselines for all operating systems supporting financial systems by June 29, 2007.

Recommendation 11: Develop, document, and test emergency procedures for the Ford data center. Ensure that procedures include specific steps to take in the data center during an emergency and identify who is responsible for taking such steps. Address activities such as emergency shut down of systems and responding to fires or water leaks.

CONCUR.

The CAO concurs with the recommendation. Currently the CAO is renovating the Ford Data Center and operating at partial capacity. In an effort to mitigate this risk, individual system owners have established and tested emergency fail over procedures. To prepare for full capacity operations, the CAO is establishing, documenting, and testing emergency procedures for the Ford Data Center as part of the reconstitution phase of the renovation. The CAO will have these procedures in place by November 30, 2007.

Recommendation 12: Require that functional/ technical specification documentation submitted by the developer be attached or included with change request forms and other documentation supporting changes to Paylinks.

CONCUR.

The CAO concurs with the recommendation. The CAO has revised change management procedures and updated the Paylinks Configuration Management plan accordingly. Additionally, the CAO is following the revised procedures for new changes to Paylinks. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 13: Develop procedures to ensure that test plans and results for changes are documented and included with other documentation supporting changes to Paylinks.

CONCUR.

The CAO concurs with the recommendation. The CAO has established procedures to fully document changes to Paylinks and is following these procedures for new changes to Paylinks. The CAO believes we have taken the appropriate action to close this recommendation.

Recommendation 14: Develop and document detailed test plan standards that define responsibilities for all personnel (users, programmers, quality assurance), require all test plans be approved, and require test results be documented and approved.

CONCUR.

The CAO concurs with this recommendation. The CAO has established, documented, and communicated a revised Test Plan template, including procedures to assure delineation of responsibilities and requiring approval of the plan and test results by the test and quality assurance officer. The CAO believes we have taken appropriate action to close this

recommendation.

Recommendation 15: Develop, document, and implement controls to ensure that only authorized and approved changes to Paylinks are introduced into production.

CONCUR.

The CAO concurs with the recommendation and has updated the configuration management and change control procedures for Paylinks accordingly. Standard operating procedures for moving code from one environment to another have been established and documented. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 16: Periodically review production program changes to ensure that access and change controls are being followed.

CONCUR.

The CAO concurs with the recommendation. As part of fully implementing the CAO Configuration Management program, Paylinks has updated a Configuration Management Plan that establishes program change procedures and review. These procedures include routine review of program changes with the Technology Advisory Board, previously the Engineering Review Board, and participation in an annual, internal Configuration Management audit. An internal audit is scheduled for the first quarter of FY2007. With completion of this internal audit and action taken on any resulting recommendations, the CAO believes we will have mitigated the identified risk. Access control changes have been addressed with the development of access control processes, access requests retained in an access control manual, and the recertification of all current users. The CAO will complete the required action to close this recommendation by July 9, 2007.

Recommendation 17: Develop, document, and implement controls over movement of program changes for Paylinks. Controls should be adequate to ensure that only authorized changes are moved into production, and management is notified.

CONCUR.

The CAO concurs with the recommendation and has updated the configuration management and change control procedures for Paylinks accordingly. Standard operating procedures for moving code from one environment to another have been established and documented. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 18: Develop and implement procedures to ensure that systems are developed and tested in accordance with House SDLC requirements and industry best practices, particularly in light of the forthcoming FFS replacement.

CONCUR.

The CAO concurs with the recommendation and is in the process of presenting the Committee

have identified, documented and enforce segregation-of-duty controls. In accordance with CAO policy requested by Recommendation 20, the CAO will require all system owners of CAO supported systems to develop and implement procedures to ensure that segregation-of-duty principles are in effect by key personnel for each system. The Director of CABS will be responsible for the CAO systems under the CABS purview. The CAO will establish and implement recommended procedures by May 31, 2007.

Recommendation 22: Identify and document incompatible administrative and end-user duties in Paylinks.

CONCUR.

The CAO concurs with the recommendation and has established documentation requested in an access control manual and recertified all users. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 23: Assign users in Paylinks to appropriate security classes to enforce proper segregation-of-duty controls. Follow the concept of least-privilege when assigning users to security classes. Provide users with only enough system access to perform their assigned roles or responsibilities.

CONCUR.

The CAO concurs with the recommendation. The CAO established documentation requested in an access control manual, and recertified all users to the appropriate access roles. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation 24: Remove Paylinks database and operating system administrator's access to the application.

CONCUR.

The CAO concurs with the recommendation; however, the version of Lawson currently in production requires the current administrative privileges. To mitigate the identified risk, the CAO has established clear policies and procedures around access control. The CAO intends to update the production application to support the access changes required for this recommendation in fiscal year 2008. The CAO will complete required action to close this recommendation by September 28, 2008.

Recommendation: (03-HOC-05, 3.02) Establish a compliance program that would monitor and report on CAO business units' compliance with HISPOL and CAO policies for implementing computer security controls at the financial application level.

CONCUR.

The CAO concurs with the recommendation and has completed the implementation and deployment of the Security Compliance Program. The final phase of the program was to

develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.

Recommendation: *(04-HOC-07, 2.02)* Develop, document, and put in place procedures to ensure compliance with HISPOL 003.0. These procedures should include risk assessments performed at all levels (application, database, and server) before new systems are installed and when enhancements are made to existing systems. In addition, this would include developing a schedule of risk assessments for existing and new financial systems and developing procedures to identify, implement, and track corrective actions designed to resolve weaknesses identified in the risk assessment.

CONCUR.

The CAO concurs with the recommendation and has completed the implementation and deployment of a Security Compliance Program. The final phase of the program was to develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.

Recommendation: *(04-HOC-07, 2.03)* Develop procedures to ensure that system-specific security plans are developed and updated as needed to reflect changes to software, hardware, and business operations.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications required to establish system security plans for financial systems. The Paylinks system security plan has been developed and approved in this format. The CAO is currently in the process of revising existing security plans for financial systems with the new format and content, and developing a baseline System Security Plan for the general support system (network). These activities will be completed by August 31, 2007.

Recommendation: *(05-HOC-07, 2.02)* Modify HISPUB 024 (pending) to require CAO SSPs to identify specific individuals as system and data owners.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of specific system and data owners. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.

Recommendation: *(05-HOC-07, 2.03)* Modify HISPUB 024 to include guidance on what

develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.

Recommendation: *(04-HOC-07, 2.02)* Develop, document, and put in place procedures to ensure compliance with HISPOL 003.0. These procedures should include risk assessments performed at all levels (application, database, and server) before new systems are installed and when enhancements are made to existing systems. In addition, this would include developing a schedule of risk assessments for existing and new financial systems and developing procedures to identify, implement, and track corrective actions designed to resolve weaknesses identified in the risk assessment.

CONCUR.

The CAO concurs with the recommendation and has completed the implementation and deployment of a Security Compliance Program. The final phase of the program was to develop the risk assessment methodology and that phase was completed in June of 2006. The CAO believes we have taken necessary action to close this recommendation.

Recommendation: *(04-HOC-07, 2.03)* Develop procedures to ensure that system-specific security plans are developed and updated as needed to reflect changes to software, hardware, and business operations.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications required to establish system security plans for financial systems. The Paylinks system security plan has been developed and approved in this format. The CAO is currently in the process of revising existing security plans for financial systems with the new format and content, and developing a baseline System Security Plan for the general support system (network). These activities will be completed by August 31, 2007.

Recommendation: *(05-HOC-07, 2.02)* Modify HISPUB 024 (pending) to require CAO SSPs to identify specific individuals as system and data owners.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of specific system and data owners. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.

Recommendation: *(05-HOC-07, 2.03)* Modify HISPUB 024 to include guidance on what

expected behaviors should be documented within CAO SSPs. CAO should fully implement all requirements identified in HISPUB 024 by updating CAO SSPs to comply with HISPUB 024.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of expected behaviors. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.

Recommendation: *(05-HOC-07, 2.04)* Take steps to ensure that all CAO network access requests are documented and retained for future reference.

CONCUR.

The CAO concurs with the recommendation. The CAO intends to establish and implement a procedure for granting network access including documenting and retaining access requests. The CAO intends to take required action by May 31, 2007.

Recommendation: *(05-HOC-07, 2.05)* Modify existing procedures to ensure that CAO system administrators are notified immediately when employees leave or are terminated from employment with the House. Assign responsibility for quarterly review of all CAO network accounts and require all reviews be documented for future reference. Reviewers should look for active accounts that have not been used in a specified period of time. These accounts should be followed up to determine if they are still necessary and disabled or deleted if not.

CONCUR.

The CAO concurs with the recommendation. The procedures to notify systems administrators have been established and implemented. Because of the natural tie between network accounts and email accounts, the CAO will conduct review and recertification of all CAO network users in conjunction with deployment of Exchange 2003. The CAO intends to establish and implement a procedure for granting network access including documenting and retaining access requests. The CAO intends to take required action by May 31, 2007.

Recommendation: *(05-HOC-07, 2.06)* Identify and document specific activities that security administrators should be logging and reviewing on a weekly basis such as failed logon attempts, changes to security profiles, and unsuccessful attempts to access unauthorized systems or data by users and outsiders.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the

Committee, the House Information Security Publication modifications. In addition, the CAO is in the process of revising System Security Plans for all financial systems with the identification of expected behaviors. The system security plans will be updated and required actions necessary to close this recommendation will be taken by August 31, 2007.

Recommendation: *(05-HOC-07, 2.07)* Finalize and implement HISPUB 022.0, Computer Security Incident Management. Effective implementation would include taking steps to ensure that all CAO system administrators are aware of the HISPUB and fully understand their roles and responsibilities for identifying and reporting potential security incidents.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. The CAO has coordinated the revisions with systems administrators and will provide formal notification when the Committee has approved the revised documents. The CAO believes we have taken appropriate action to close this recommendation.

Recommendation: *(05-HOC-07, 2.08)* Develop and implement policies and procedures to ensure that CAO system administrators are notified, and access is removed on the same day an employee leaves or is terminated from the House.

CONCUR.

The CAO concurs with the recommendation to notify systems administrators when employees depart and promptly remove access. The CAO has implemented the associated procedures. Further, the CAO re-emphasized the importance of adhering to this policy with systems administrators and Information Technology management. The CAO believes these actions mitigate the identified risk and believes we have taken the appropriate action required to close this recommendation.

Recommendation: *(05-HOC-07, 2.09)* Document policies and procedures for granting emergency and temporary access. Monitor emergency and temporary access, and automatically terminate access after a predetermined period when possible.

CONCUR.

The CAO concurs with the recommendation and intends to document the requested policies and procedures for granting temporary and emergency access by May 31, 2007.

Recommendation: *(05-HOC-07, 2.10)* Modify existing HISPUBs and develop additional policies and procedures where necessary to ensure that all blank or default passwords are identified and changed before any CAO financial

system is placed into production. Include specific steps in House audit checklists for determining if blank or default passwords exist.

CONCUR.

The CAO concurs with the recommendation and has revised, approved, and forwarded to the Committee, the House Information Security Publication modifications. The CAO has also audited all financial systems under the revised policy. The CAO believes we have taken required action to close this recommendation.

Recommendation: *(02-HOC-06, 4.05)* Coordinate contingency planning and recovery policies and procedures to ensure a comprehensive approach that includes the network, mainframe computer, FFS, PD, and all critical financial systems.

CONCUR.

The CAO concurs with the recommendation and is in the process of developing recovery procedures and processes for the alternative site. The CAO will have taken the necessary action to close this recommendation by December 31, 2007.

Weakness 2: The Financial Reporting Internal Control Framework was Inadequate

Recommendation 1: Require the Office of Finance and Procurement (OFP) to perform a thorough analysis of their procedures for preparing the Statement of Cash Flows (SCF) to ensure that all FFS and subsidiary ledger data are included and properly classified in the SCF.

CONCUR.

OFP has performed an analysis of our procedures for preparing the SCF and has modified the methodology to ensure that all FFS and subsidiary ledger data are included and properly classified in the SCF. During our review, emphasis was placed on correcting the two areas where errors were identified during the financial statement audit: changes affecting capital lease liability and property and equipment. New procedures are already in place for the next financial statement audit that will ensure that all transactions that affect the SCF, including adjusting journal entries to both FFS and financial statement software, will be presented correctly. The CAO believes we have taken the appropriate action to close this recommendation.

Recommendation 2: Require OFP to identify and implement a process to ensure a thorough review of the subsequent period to capture all financial reporting data. Document these activities in OFP policies and procedures manuals.

CONCUR.

OFP has implemented a new process to ensure a thorough review of the subsequent period to capture all financial reporting data. The new process has already been used for the calendar year

2005 financial statement compilation. Specifically, the new process corrects a condition first identified during the calendar year 2004 financial audit whereby accounts payable were understated at year end related to service contract payments processed during the first quarter of the year subsequent to the financial statement reporting period. In addition, for future financial statement audits, OFP will use historical data to estimate accounts payable for payments processed after the normal cut-off period. This process has been documented in OFP policies and procedures. The CAO believes we have taken the appropriate action to close this recommendation.

Recommendation 3: Require all CAO personnel responsible for capitalized property procurement, monitoring, and reporting to attend training in generally accepted accounting principles for fixed assets. Prepare a memorandum to non-CAO offices responsible for purchasing capitalized property instructing them of the House's fixed-asset policies and provide training, if necessary.

CONCUR.

The Accounting Department conducts periodic training for all CAO offices regarding the proper treatment of fixed assets and will continue to do so in the future. The appropriate personnel will be identified and training materials will be prepared and distributed to attendees on the proper treatment of budget object codes, purchases and disposals, and depreciation. Attendance will be taken for each session and compared to a list of employees responsible for capitalized property. Also, training literature will be distributed to non-CAO offices responsible for purchasing capitalized property and training will be provided to those offices as required. Training is a continual process and Accounting will work closely with all affected offices to ensure capitalized property is accounted for correctly. Accounting will conduct at least one more training class before the end of the calendar year, and will conduct training quarterly thereafter. The CAO believes we will take the appropriate action to close this recommendation by December 31, 2006.

Recommendation 4: Develop and implement a policy requiring timely updates to FAIMS for all capitalized property purchases and discontinue use of manual worksheets. Require OFP to revise its policies and procedures to state that assets removed from service should not be depreciated.

CONCUR.

HIR has revised its policies and procedures to require timely updates to FAIMS for all capitalized property purchases. OFP will work with HIR and HSS to phase out manual worksheets by transferring assets to FAIMS that are currently being tracked manually. This process will be completed by September 30, 2007. OFP has revised its policies and procedures to state that assets removed from service will not be depreciated, and will work with HIR to identify assets that have been removed from service. The CAO believes we have taken the appropriate action to close this portion of the recommendation.

Recommendation 5: Allow OFP staff responsible for property and equipment monitoring and reporting be granted FAIMS user access privileges to adjust capital asset costs, as necessary.

CONCUR.

The CAO concurs with the intent of this recommendation, but believes granting OFP personnel user access privileges to FAIMS could create potential internal control problems. Changes to FAIMS, whether intentional or not, could be made by OFP without the knowledge or consent of the property custodian. To address the recommendation, OFP will continue to analyze property and equipment transactions and provide direction to various CAO offices when adjustments to capital asset costs are required, and will follow up with the offices to ensure FAIMS has been updated timely. The CAO believes we have taken the appropriate action to close this recommendation.

Recommendation 6: Work with the Committee on House Administration to amend its rules and require annual inventories of capitalized internal use software. Subject capitalized software to the same acquisition, monitoring, and disposal controls as all other capitalized property.

PARTIALLY CONCUR.

HSS concurs that a process must be established to verify the inventory. However, software is an internal item, and is not physically accessible to any staff other than that of the Member/House office. Therefore, HSS cannot physically inventory this software. As an alternative, HSS recommends that the Office Coordinators send a yearly email to their House contacts to verify that each office is using the CMS software that is listed on their inventory. Verification by email exchange will ensure that offices do not have CMS software on their inventory that is no longer in use. The CAO believes we will take the appropriate action to close this recommendation, beginning with a year-end inventory in the current year, by December 31, 2006.

Recommendation 7: Investigate the design of controls over (1) payroll data entry and other Human Resources processes and management review functions; and (2) review the Over Speaker Pay Edit report process to determine where weaknesses exist so these processes may be modified to ensure that similar errors are detected and prevented in the future.

CONCUR.

OFP has taken the following steps to address design controls over payroll data entry and management review functions:

- The Office of Employee Services (OES) is developing an interactive Payroll Authorization Form that will be proposed for usage to the Committee on House Administration. The Form will ultimately be transmitted between offices electronically resulting in a more efficient process. Coding will be more legible which should result in fewer errors and less corrections processed by payroll counselors.
- Payroll counselors use the payroll certification and copies of the original paperwork to validate gross amounts for all pay before the final payroll is run.
- Benefits Division personnel spot-check a sample of all Federal Employee Health Benefits (FEHB), Thrift Savings Plan (TSP) and Life Insurance Enrollment Forms for accuracy.
- Payroll, Benefits, Document Management and the Help Desk use a custom Access Data Base to capture all incoming payroll processing documents (i.e., Appointments, Terminations, Salary Adjustments, FEHB, Life Insurance, and TSP).

- Payroll Division performs a two-person Payroll Counselor review of all Cash Due, EFT-Pull Back of salary actions that would result in an employee overpayment.
- Benefits Division performs a two-person Benefits Counselor review of all LWOP or adjustments that would result in a deduction not being withheld accurately.
- OES will conduct random sample audits of the W4 forms entered for each pay period.
- During the off cycle payroll, OES must manually compute the Federal Employee Government Life Insurance withholding. This process has been improved by checking the life insurance calculation for reasonableness as OES reviews the entire PR140 to audit gross amounts to the paperwork.
- OES uses a tracking system for monies due back to the House for payroll overpayments which includes a spreadsheet that tracks individual gross to net calculations and a status of whether payment has been received by the House.

OES has reviewed and corrected the *Over Speakers Pay Edit Report* process to identify employees who have exceeded allowable House payroll limits. Adjustments are made accordingly before the final payroll is run. The CAO believes we have taken the appropriate action to close this recommendation.

Recommendation: (05-HOC-07, 3.1) Review and revise *Accounting Department Policy and Procedures* and *Accounting Department Annual Financial Statement Compilation Procedures*, including quality control procedures to ensure that all functions are fully and completely documented.

CONCUR.

The Accounting Department will review and revise its policies and procedures and financial statement compilation procedures as necessary to ensure that all functions are fully and completely documented. Accounting periodically updates all procedures related to both operations and financial statement preparation as various methodologies change. During our next revision, we will emphasize quality control procedures related to the financial statement compilation process to address weaknesses discovered during the financial statement audit. The CAO believes we will take the appropriate action to close this recommendation by November 30, 2006.

STATUS OF PRIOR-YEAR RECOMMENDATIONS

Recommendation: (05-HOC-07, 1.2) Develop a proposal, for Committee on House Administration approval, which corrects the payroll inefficiency in preparing and processing supplemental payroll.

CONCUR.

The CAO concurs with this recommendation which corrects the payroll inefficiency in preparing and processing supplemental payroll. The CAO will work together with the OIG and OIG contract support to help analyze the various pay cycle options and their impact on reports and other payroll-related processes. The OIG support is intended to provide valuable advisory support to the CAO. Based on the findings, the CAO will develop a proposal to correct the payroll inefficiency in preparing and processing supplemental payroll. The CAO intends to develop the proposal by April 30, 2007.

This Page Intentionally Left Blank