KEARNEY& COMPANY

Certified Public Accountants and Consultants

4501 Ford Avenue, Suite 1400, Alexandria, VA 22302
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

Independent Auditor's Report

To the Architect of the Capitol

We have audited the accompanying balance sheets of the Architect of the Capitol as of September 30, 2004 and 2003. The balance sheets are the responsibility of the Architect of the Capitol's management. Our responsibility is to express an opinion on the balance sheets based on our audit.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America, standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*, as amended. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the balance sheets are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the balance sheets. An audit also includes an assessment of the accounting principles used and significant estimates made by management, as well as an evaluation of the overall balance sheet presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the September 30, 2004 and 2003 balance sheets referred to above present fairly, in all material respects, the financial position of the Architect of the Capitol as of September 30, 2004 and 2003, respectively, in conformity with accounting principles generally accepted in the United States of America.

In accordance with *Government Auditing Standards*, we have also issued our reports dated May 26, 2005, on our consideration of the Architect of the Capitol's internal control over financial reporting and our tests of its compliance with certain provisions of laws, regulations, contracts, and grants. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and should be read in conjunction with this report in considering the results of our audit.

Kearney & Company

May 26, 2005
Alexandria, VA

KEARNEY& COMPANY

Certified Public Accountants and Consultants

4501 Ford Avenue, Suite 1400, Alexandria, VA 22302
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

Independent Auditor's Report on Compliance with Laws and Regulations

To the Architect of the Capitol

We have audited the balance sheet of the Architect of the Capitol (AOC) as of September 30, 2004, and have issued our report thereon dated May 26, 2005.

We conducted our audits in accordance with auditing standards generally accepted in the United States, standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*.

The management of AOC is responsible for complying with laws and regulations applicable to AOC. As part of obtaining reasonable assurance about whether AOC's balance sheet is free of material misstatement, we performed tests of its compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts and certain other laws and regulations specified in OMB Bulletin No. 01-02. We limited our tests of compliance to these provisions and we did not test compliance with all laws and regulations applicable to AOC. However, providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit and, accordingly, we do not express such an opinion.

The results of our tests of compliance with the laws and regulations described in the preceding paragraph disclosed two instances of noncompliance, described below, with the following laws and regulations that are required to be reported upon under *Government Auditing Standards* and OMB Bulletin No. 01-02.

- The Comptroller General of the Government Accountability Office (GAO) issued a ruling on September 30, 2005. In the ruling, the Comptroller General concluded that AOC could not compensate Senior Executive Service Employees above Level III of the Executive Schedule. GAO concluded that AOC did not maintain a certified performance appraisal system and could not compensate at rates above Level III as required by Executive Branch agencies by U.S.C. Sect.5382. In 2004, the Level III maximum pay rate was $145,600, and AOC established two employee pay rates at $152,000 and $150,000, respectively.

KEARNEY& COMPANY

- AOC was not compliant with the Congressional Accountability Act (CAA) of 1995. In the CAA, Congress made its facilities and employees subject to the same safety laws that apply outside of the Legislative Branch. In 1997, other provisions of the CAA applied fire safety standards to Congressional buildings, including the buildings of AOC. The Office of Compliance conducted a year long fire safety investigation that culminated in a report issued in January 2001 that identified numerous safety hazards in several of AOC's buildings.

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

Kearney & Company

May 26, 2005
Alexandria, VA

KEARNEY& COMPANY

Certified Public Accountants and Consultants

4501 Ford Avenue, Suite 1400, Alexandria, VA 22302
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

Independent Auditor's Report on Internal Control

To the Architect of the Capitol

We have audited the balance sheet of the Architect of the Capitol (AOC) as of September 30, 2004, and have issued our report thereon dated May 26, 2005.

We conducted our audit in accordance with auditing standards generally accepted in the United States, standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements*.

In planning and performing our audit, we considered AOC's internal control over financial reporting by obtaining an understanding of AOC's internal control, determined whether internal controls had been placed in operation, assessed control risk, and performed tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the balance sheet. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 01-02. We did not test all internal controls relevant to operating objectives, as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal control. Consequently, we do not provide an opinion on internal control.

Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control over financial reporting that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of the internal control that, in our judgment, could adversely affect AOC's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements. 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 amounts that would be material in relation to the financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. However, we noted certain matters discussed in the following paragraphs involving the internal control and its operations that we consider to be reportable conditions and material weaknesses.

We also noted other matters involving the internal control over financial reporting which have been reported to AOC management in a separate letter dated May 26, 2005.

MATERIAL WEAKNESSES

Finding 1. Internal Control Assessments

Finding – AOC lacked a formal and systematic process to assess and evaluate the design and operation of internal controls. In the absence of such an assessment, AOC cannot determine if their current internal control design mitigates existing risks and effectively safeguards assets.

Recommendation – AOC should formally evaluate the effectiveness of the design and operation of their internal control structure, including the identification of risks to material accounts and the existence of internal controls to mitigate those risks. Although AOC is not subject to OMB Circular A-123, we recommend that AOC consult the recently released "Implementation Guide for OMB Circular A-123 Appendix A Internal Control over Financial Reporting (the Guide)." The Guide was issued by the Chief Financial Officer's Council in May 2005 and is currently in draft form. The Guide includes very useful guidance to enable management to evaluate internal controls and monitor and test these controls throughout the year.

Finding 2. Annual Leave

Finding – AOC annual leave processing lacked controls to ensure the following:

- Differences between the time recording system and the payroll processing system were identified, investigated, and resolved in a timely manner
- Manual adjustments to leave balances were approved and monitored, and the adjustments were reversed when automatic system entries were posted
- Leave earning rates were consistent with years of service.

Annual leave in the time and attendance system did not match the balances in the NFC payroll processing system. AOC maintains parallel leave databases in the STAR time and attendance system and in the NFC payroll processing system. Due to processing delays, timekeepers regularly modify leave balances in the time and attendance system after payroll is processed. AOC policy requires that timekeepers inform Human Resources of any modifications in a timely manner. Human Resources should validate these modifications and update the payroll records. These actions did not occur in a timely manner. Out of 78 sample items, 16 had NFC leave balances that did not match those in the STAR system. Since accounting uses the NFC leave balances for financial reporting, but the STAR system contains the most recent information, the differences resulted in an understatement of payroll expense and payroll accrual liability of approximately $130,000.

Additionally, annual leave carryover hours from calendar year 2003 through 2004 exceeded AOC's maximum carryover of 240 hours. When an employee transfers to AOC from another agency, Human Resources manually enters the leave balances into the payroll system. Subsequently, when AOC officially receives the Form 1150 from the other agency, the transferred leave is automatically entered into the leave system for a second time. Human Resources did not reverse the original manual entry, which resulted in the double counting. We noted that 27 employees had an annual leave carryover of over 240 hours, which resulted in an overstatement of the annual leave liability.

Period leave accrual was not consistent with the years of service. We identified one instance where the employee's annual leave accrual was zero hours per pay period. Based on the years of service, four hours of annual leave should have been accrued per period. This resulted in an accrued annual leave understatement of 104 hours.

Recommendation – AOC should perform the following:

- Communicate with NFC to develop a method to update the NFC system simultaneously with the STAR system
- Develop a process which tracks leave hours that have been manually entered and ensures that manual entries are properly authorized by management and reversed when the official hours on the Form 1150 are entered
- Develop a process that validates the annual update of pay period leave balances.

Finding 3. Timekeeping Controls

Finding – AOC did not have effective controls over time and attendance processing. We identified an instance in which an employee, who was also the department timekeeper, was compensated for more hours than on the approved timesheet. The hours worked per the timesheet were 91.75 and the hours per NFC were 98.75. AOC performed subsequent follow-up procedures and identified 35 discrepancies for the original timekeeper and an additional timekeeper in calendar years 2003 and 2004. The recorded number of hours worked in the payroll system needs to reflect the accurate number of hours worked, as confirmed by the employee and approved by the supervisor.

Supervisors and employees did not regularly sign the STAR timesheets as required by personnel policies. Fourteen employees and nine supervisors out of 78 samples did not sign the STAR timesheets. Such a condition may allow the employee to be underpaid or overpaid if the employee has not been able to verify the time that has been entered into the STAR system or the supervisor did not approve the time worked.

Additionally, supervisors did not regularly approve annual leave and overtime. Out of 78 samples taken, 24 included overtime or annual leave that was not approved by the supervisor. The payroll expense and annual leave accrual may be either overstated or understated.

Recommendations – AOC should perform the following:

- Implement a control that validates compensated hours to approved timesheet hours
- Ensure that policies concerning the approval of overtime and annual leave and the approval of timesheets are well understood and enforced by supervisors. AOC should devise a more effective method of monitoring and enforcement.

Finding 4. Construction Work-in-Progress

Finding – AOC Project Management and Procurement does not maintain a formal system that ensures execution of a contract or modification before the initiation of work. All AOC expenditures must first be obligated, as required by law. We found that invoices totaling over $32,775,000 were dated before or within 14 days of when the contract or contract modification for those expenditures was signed. Based on the lead time required for the performance of the underlying work and the billing cycle, contracts should be executed at least 14 days before a payment requisition. Allowing or encouraging contractors to expend money prior to the execution of contract modifications is contrary to Federal guidance and accepted Federal practice. In addition, as a result of this practice, AOC may lose bargaining power in the negotiation of contract pricing and could incur increased costs. Finally, this could lead to situations in which invoices are presented for payment prior to execution of contract modifications, and could result in AOC expending funds that were not obligated or under an executed contract.

AOC records construction costs for long lived assets in the Construction Work-in-Progress (CWIP) account. CWIP should include only expenditures which qualify for capitalization (useful life of more than two years) and will ultimately be charged to operations as a depreciation expense once placed in service. AOC did not have formal procedures in place that provided guidance for the proper classification of projects. Our testing identified two projects with total expenditures of $1,767,337, which did not meet capitalization requirements and should not have been included in CWIP. AOC subsequently charged $1,749,891, or 99% of this amount to operations.

Finally, AOC's payment requisition approval process does not contain a formal step that validates requisition contract values against executed contract amounts and notifies contractors of discrepancies. We discovered that, out of 105 tested, contract amounts on 17 payment requisitions did not match the contract amount to date, as evidenced by the executed original contract and supplemental agreements. Payment requisitions should reflect current contract values to ensure that AOC does not overpay vendors.

Recommendation – AOC should perform the following:

- Adopt procedures to prevent initiation of contract work and/or acceptance/use of materials until funds are obligated through a contract or contract modification

- Review all CWIP project charges and verify that costs qualify for capitalization and are properly classified
- Create a formal process that validates payment requisition contract values to the current executed contract amounts. If the amounts do not match, AOC should resolve the discrepancy with the contractor as soon as possible.

REPORTABLE CONDITIONS

Finding 1. Capital and Operating Leases

Finding – AOC does not have an effective policy in place to identify the execution or modification of lease agreements and perform the requisite analyses to determine if they are capital or operating leases for financial reporting in a timely manner. During testing, we discovered that AOC had not compiled all lease obligations and accompanying footnote disclosures as of September 30, 2004. Subsequent to year-end, AOC asked all jurisdictions for identification of all known leases. This process resulted in the identification of 19 leases, five of which qualified for capital lease treatment. This process of identifying and analyzing leases is informal and occurs after year-end.

Furthermore, the calculation used to determine the present value of the minimum lease payments does not conform to the methodology prescribed in Federal Accounting Standards Advisory Board (FASAB) standards. The methodology applied overstated the present value of the capitalized lease.

Recommendation – AOC should implement procedures which facilitate timely and accurate identification of leases. These procedures should incorporate information flows from the jurisdictions and the Procurement Office. Accounting should obtain all relevant financial information (i.e., term, payments, and fair market value of the underlying assets) and perform analyses required to determine if the obligations should be treated as capital or operating leases. Accounting should also update the capital and operating lease footnote disclosures as new leases are identified. In addition, AOC should correct the calculations used to determine the present value of the minimum lease payments.

Finding 2. Information Technology Controls

Finding – We evaluated AOC's Information System general controls following guidance provided by the National Institute of Standards and Technology (NIST) and the Government Accountability Office's (GAO's) Federal Information System Controls Audit Manual (FISCAM). We provided a detailed report, as well as a prioritization of findings, under separate cover. For a detailed description and recommendations to these findings, refer to the separately issued report.

AOC does not have an effective information system security program. This has resulted in weaknesses in AOC's information system control environment. Weaknesses in general controls impaired AOC's ability to ensure, for example, the following:

- Computer risks are adequately assessed and security policies and procedures are effective and consistent with overall organizational policies and procedures
- Users have only the access needed to perform their duties
- Software changes are properly documented before being placed into operation
- Critical applications are properly restored in the case of a disaster or interruption.

AOC is working to enhance Information Technology (IT) controls in order to provide effective control over the general support systems and applications. In this effort, AOC has developed and implemented a phased approach based on best practices, and is in the process of developing policies and performing risk assessments for the general support systems on which mission-critical applications rely. AOC has also contracted assistance for the development of a Continuity of Operations Plan (COOP) and a Disaster Recovery Plan (DRP).

We summarize some of the salient findings from that report below. Findings are reported under the following general categories:

- Entity-wide Security Program (SP)
- Access Control (AC)
- Change Control (CC)
- Service Continuity (SC).

Because we could not rely on the essential controls within the general categories above, we did not perform all tests as detailed in the FISCAM. Additional findings may have arisen from the omitted procedures.

Entity-wide Security Program (SP)

This category provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. We noted weaknesses in the following areas relating to AOC's entity-wide security program:

- No formal risk assessments for financial and core operational components
- The established entity-wide security program plan should be improved upon
- Information Systems Security Plans (ISSP) have not been completed
- Security responsibilities have not been clearly defined
- Lack of documentation of detailed procedures in a Computer Incident Response Plan
- The security plan does not provide detailed hiring procedures
- No documentation of the expertise needed to carry out information security responsibilities in the security plan
- No Certification and Accreditation Statements for all general support systems and major applications.

Access Control (AC)

Controls within this category limit or detect access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. We noted weaknesses in the following areas relating to the AOC's access control:

- No Certification and Accreditation Statements for all general support systems and major applications
- No definition of user profiles or documentation in system security plans
- The process for auditing user access should be automated
- No definition of policies and procedures for the administration of special access privileges and the control of emergency and temporary authorizations
- Physical and logical access control maps should be documented
- Tools should be implemented and procedures formalized for the handling of security violations.

Change Control (CC)

The controls in this category prevent unauthorized programs or modifications to an existing program from being implemented. We noted weaknesses in the following areas relating to the AOC's change control:

- Procedures for the implementation of the AOC system development life cycle (SDLC) should be defined and documented
- User account settings should be verified and the use of public domain and personal software should be restricted.

Service Continuity (SC)

The controls in this category prevent loss of the capability to process, retrieve, and protect information maintained electronically. We noted weaknesses in the following area relating to the AOC's service continuity:

- A COOP and a DRP should be completed.

Recommendations – We recommend that AOC perform the following:

- Complete full risk assessments on all Mission-Critical General Support Systems and Major Applications
- Develop an entity-wide security plan to include definition of scope and responsibilities
- Complete full risk assessments on Mission-Critical General Support Systems and Major Applications

KEARNEY& COMPANY

- Develop and implement a security management structure with clearly defined security responsibilities and solicit independent advice and comment on the ISSP prior to the plan's implementation
- Complete the Computer Incident Response Plan and Procedures and implement best practices
- Office of Information Resource Management (OIRM) positions should be defined by level of sensitivity
- Implement OIRM policy and procedures to ensure proper documentation of minimum experience requirements for positions
- AOC CISO should continue the development and implementation of the System Security Plans
- AOC CISO should continue development of procedures for implementation of IT Security Risk Management Policy
- Complete System Security Plans to include development of standard User Profiles
- Select and implement an integrated Identity Management tool
- Perform a full risk assessment, which should include the identification of all physical and logical access points
- Document the implementation of tools and procedures for logging security violations
- Implement and document their SDLC methodology and incorporate procedures to ensure compliance with the policies
- Conduct an inventory of desktop settings to ensure that administrative and power user access is limited
- Develop a COOP and a DRP.

This report is intended solely for the information and use of the Office of Inspector General of the Architect of the Capitol, Architect of the Capitol management, the Government Accountability Office, and the U.S. Congress, and is not intended to be, and should not be used by anyone other than these specified parties.

May 26, 2005
Alexandria, VA