



*Certified Public Accountants  
and Consultants*

---

4501 Ford Avenue, Suite 1400, Alexandria, VA 22302  
PI4: 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 financial statements of the Architect of the Capitol (AOC) as of September 30, 2005, and have issued our report thereon dated August 16, 2006. 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, as amended*.

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 financial statements. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control over financial reporting that, in our judgment, could adversely affect the AOC's ability to record, process, summarize, and report financial data consistent with the assertion of management in the financial statements. 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 August 16, 2006.

## **MATERIAL WEAKNESSES**

### **1. Internal Control Assessments (Repeat Condition)**

AOC lacks 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 its current internal control design mitigates existing risks and effectively safeguards assets.

Recommendation – We recommend that AOC formally evaluates the effectiveness of the design and operation of its 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, *Management's Responsibility for Internal Control*, 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.

### **2. Annual Leave (Repeat Condition)**

AOC had instances in which maximum leave balances were exceeded, accrued leave did not correspond with years of service, and leave balances in the time and attendance (T&A) system did not match National Finance Center (NFC) payroll system balances:

- From the year 2004 to the year 2005, 27 employees carried over more than the 240 hours maximum leave balance
- In the NFC payroll system, 25 out of 76 employees' annual leave balances in the T&A system did not match balances in the NFC payroll system. The differences ranged from 1 hour to 122 hours
- One STAR Web T&A did not reflect the employee's leave accrual according to the employee's years of service.

Recommendation – We recommend that AOC develop a process in which annual leave amounts in the STAR Web system are reviewed for accuracy and compared to amounts in the NFC payroll system.

### **3. Time Keeping, Processing, and Approval Procedures (Repeat Condition)**

We identified instances in which AOC time recordation and payroll was not properly authorized, paid accordingly, or appropriately transmitted. The instances are as follows:

- Out of a sample of seventy-six, two timekeepers, two employees, and three supervisors did not sign the time summary. Two of the three timesheets not signed by supervisors included overtime hours. As a result, we could not establish statistical reliance on payroll internal controls, and we performed additional testing including further testing of the certification of overtime hours. During the additional testing, we noted that ten employees, five timekeepers, and sixteen supervisors out of one hundred twenty-eight samples did not sign the time summary
- Timekeepers were entering their own time into STAR Web system
- In 11 of 76 sample timesheets, overtime and annual leave was not pre-approved by supervisors
- Payroll documentation does not support 103 hours of overtime totaling \$3,647 paid to an employee.

Recommendation – We recommend that AOC ensure that policies concerning the approval and entering of time are strictly enforced. Also, we recommend that AOC determine the accuracy and propriety of the \$3,647 of overtime wages and take the necessary follow-up actions based on the resolution.

### **4. Responsibility for Procurement and Disbursement Internal Controls, and Policies and Procedures**

AOC has decentralized many components of the purchase and disbursement process including initiating requisitions, purchase authorizations, receiving and disbursement approvals. We identified several areas which were not monitored and managed by a central process owner. This lack of centralized oversight resulted in internal control weaknesses in the following areas:

- Integrated Assessment of Risks and Internal Controls – No organization or entity within AOC acknowledges responsibility for or performs documented oversight of the collective procurement process ensuring that the decentralized units function in a coordinated fashion to identify and address risks inherent in the cycle and produce information necessary for financial and operational reporting. Within a decentralized process, this lack of central monitoring and oversight results in a weakened control environment, i.e., vacuum of leadership, and variability in the controls' performance at the individual units
- Vendor Database – We identified 24 individuals with access and the ability to modify the vendor database, with no process to ensure the propriety and accuracy of changes
- Procurement Card Monitoring – AOC has not clearly defined responsibility for the selection of purchase card holders to “no pre-approved status,” and the formal

monitoring responsibility encompassing the selection, data input, and regular review of purchase card holders to determine if a particular cardholder having the authority is warranted

- Contract Information – AOC does not maintain an easily accessible repository of current contract information. Invoice approvers and processors cannot easily verify the billing amounts are correct and within current contractual limits exposing the AOC to the risk of overpayment.

Recommendation – We recommend that AOC assign formal authority for oversight and monitoring of the process including risk assessments and control design. We recommend limiting access to the vendor database to a select number of individuals, and that proposed charges be reviewed and approved before data entry. Data entry should also be reviewed for accuracy by a third party. We recommend that a regular review be conducted that compares system authorized “no pre-approval status” users to a master list and determines if the cardholder is following all purchasing guidelines. It should also be determined if the individual cardholder is the appropriate individual to have the purchasing authority within the jurisdiction. Invoice approvers and processors should have ready access to the most recent contract information.

## **REPORTABLE CONDITIONS**

### **1. Information System Controls (Repeat Condition)**

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) Federal Information System Controls Audit Manual (FISCAM). We provided a detailed report as well as a prioritization of findings under separate cover. For detailed descriptions and recommendations for 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 have impaired AOC’s ability to ensure, for example, that:

- Computer risks are adequately assessed and security policies and procedures are effective and consistent with overall organizational policies and procedures
- Users only have the access necessary 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. The AOC has also contracted

assistance for the development of a Continuity of Operations Plan (COOP) and a Disaster Recovery Plan (DRP).

We summarize the 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***

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 SP:

- No formal risk assessments for financial and core operational components
- The established entity-wide SP 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 ISSP
- No Certification and Accreditation Statements for all general support systems and major applications.

### ***Access Control***

Controls within this category limit or detect access to computer resources (i.e., 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 AC:

- 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 AC maps should be documented
- Tools should be implemented and procedures formalized for the handling of security violations.

### ***Change Control***

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 AOC's CC:

- 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***

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 AOC's SC:

- A COOP and a DRP should be completed.

Recommendation – We recommend that AOC perform the following:

- Complete full risk assessments of all mission-critical GSS and major applications
- Develop an entity-wide SP to include definition of scope and responsibilities
- 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's Chief Information Security Officer should continue the development and implementation of the System Security Plans
- AOC CISO should continue development of procedures for implementation of the 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 AOC's SDLC methodology and incorporate procedures to ensure compliance with the policies
- Conduct an inventory of desktop settings to ensure that administrative and broad supervisory 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 GAO, and the U.S. Congress, and is not intended to be, and should not be used by anyone other than these specified parties.

A handwritten signature in blue ink that reads "Kearney & Company". The signature is written in a cursive, flowing style.

August 16, 2006  
Alexandria, Virginia