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 financial statements of the Architect of the Capitol (AOC) as of September 30, 2006, and have issued our report thereon dated January 12, 2007. We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 06-03, *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 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. 06-03. 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 January 12, 2007.

MATERIAL WEAKNESSES

1. Internal Control Assessments (Repeat Condition)

AOC has not completed a formal and systematic assessment and evaluation of the design and operation of internal controls. As of September 30, 2006, AOC has completed an assessment of the procure-to-pay process and has partially completed the human resources and time and attendance processes. AOC has not yet addressed the project management process. In the absence of a complete assessment, AOC cannot determine if its current internal control design mitigates existing risks and effectively safeguards assets.

Recommendation –AOC should complete and document internal control assessments that evaluate 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 "Implementation Guide for OMB Circular A-123 Appendix A Internal Control over Financial Reporting" (the Guide). The Guide was issued by the Chief Financial Officers Council in May 2005. The Guide includes guidance enabling management to evaluate internal controls and monitor and test these controls throughout the year.

2. Annual Leave (Repeat Condition)

We identified instances at AOC in which maximum leave carryover balances were exceeded, and leave balances in the WebTA and STAR Web time and attendance systems did not match National Finance Center (NFC) payroll system balances. While AOC has demonstrated improvement in this area, the controls structure does not yet reduce financial misstatement risk to an acceptable level.

- From 2005 to 2006, 15 employees carried over more than the 240-hour maximum leave balance. AOC could not support the propriety of the excess carryover amounts.
- In the NFC payroll system, employees' annual leave balances in the WebTA and STAR Web time and attendance systems did not match balances in the NFC payroll system.

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

3. Time Recordation, Processing, and Approval Procedures (Repeat Condition)

We identified instances where AOC time recordation and payroll was not properly authorized. The instances include:

- Out of a sample of ten, there were three occurrences where timekeeper certification and supervisor approval were performed by the same individual. In addition, input of an employee's time and attendance by the timekeeper was not independently reviewed for accuracy
- Out of a sample of 76, 11 employees were either missing an overtime approval form or did not have the required authorizing signature
- Out of a sample of 76, five leave request forms were not approved prior to leave being taken.

Recommendation – AOC should develop procedures to ensure policies concerning the approval and entering of time are enforced.

4. Risk Assessment Updates

AOC's internal control environment does not have formal, documented processes to monitor the internal and external environment, identify changing risk profiles, or respond accordingly. Specifically, AOC did not implement controls to reconcile the payroll data transmitted to and received from NFC (as recommended by NFC) as an appendix to its qualified SAS 70 opinion. While several employees performed additional tests, this did not constitute a repeatable and sustainable systemic effort.

Recommendation – AOC should implement procedures to monitor and identify changing risks. Also, AOC should reconcile NFC payroll data transmission to data receipt including, at a minimum, jurisdictional employees and hours.

5. Internal Control Design and Management of the Purchase to Disbursement Process

No organization/entity within AOC is accountable for the collective purchase to disbursement process. AOC has decentralized many components of the purchase and disbursement process including initiating requisitions, purchase authorizations, and receiving and disbursement approvals. Within a decentralized process, this lack of central monitoring and oversight results in a weakened control environment.

We also identified 16 individuals from three divisions with the ability to access and modify the vendor database, with no process to ensure the propriety and accuracy of

changes made. Supervisors also do not approve vendor requests before new vendors are created in the system.

Recommendation – AOC should assign formal authority for the oversight and monitoring of the collective purchase to disbursement process, including risk assessments and control design. These assessments should focus on interchange points between process participants to ensure that financial statement risks are adequately mitigated. We also recommend limiting access to the vendor database to a select number of individuals, and that proposed changes be reviewed and approved before data entry. Data entry should also be reviewed for accuracy by a third party.

REPORTABLE CONDITIONS

1. Information System Controls (Repeat Condition)

We evaluated AOC's information system general controls in accordance with 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 have provided a detailed report and a prioritization of findings under separate cover. For detailed descriptions and recommendations for these findings, refer to the separately issued report.

AOC has made improvements to its overall information system security program since the completion of the FY 2005 audit. AOC's progress includes:

- Development of security plans that cover all major facilities and operations, which are resource owner approved. Security plans for the general support systems (GSS) and major applications are reviewed periodically and adjusted to reflect current conditions and risks
- A security management structure has been established and documented in the security plans for the GSS and major applications. The security plan clearly identifies resource owners and assigns security responsibility to the Chief Information Security Officer (CISO)
- Establishment of resource classifications and related criteria; therefore, consideration has been given to data sensitivity and integrity
- Development and testing of the Continuity of Operations (COOP) and Disaster Recovery Plans.

Having noted improvements, AOC still has areas of weakness that should be addressed. Some of the more significant findings from that report are summarized below. Findings are reported under the following general categories:

- Entity-wide Security Program
- Access Control
- Service Continuity.

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 security program:

- Risk assessments for financial and core operational components
- Information Systems Security Plans (ISSP) are not fully implemented
- Incident response procedures
- Detailed hiring procedures
- Security awareness and technical security training
- Effectiveness of corrective action process.

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 access control:

- Documentation of user profile definitions
- De-provisioning and reassessing user accounts and assigned privileges
- Administration of special access privileges and the control of emergency and temporary authorizations
- Formalized procedures for the handling of security violations.

Service Continuity

The controls in this category prevent loss of the capability to process, retrieve, and protect information maintained electronically. AOC should improve and test the COOP.

Recommendation – AOC should perform the following:

- Conduct a comprehensive risk assessment using NIST SP 800-30 methodology to identify risks and implement appropriate mitigating controls to address vulnerabilities, including those identified in SAS 70 audit reports
- Implement security plans
- Revise customer help desk incident response procedures to include responsibilities for security incident response
- Define Information Technology Division (ITD) positions including level of sensitivity
- Require all AOC employees to receive annual security awareness training and require information technology (IT) security staff to receive specialized training

for assigned job duties. Evidence of such training should be documented and maintained

- Develop a formal process to address observations from security reviews, which should include independent evaluation of the corrective action
- Document user profiles and include them in the system security plans
- Develop and implement user account management procedures to ensure timely removal or modification of user accounts and assigned privileges
- Implement monitoring procedures in accordance with NIST SP 800-92 to ensure network management is compliant with ITD policies and procedures
- Implement network management tools and procedures to enhance control
- Continue to develop a comprehensive COOP, perform tests of the COOP, and make necessary changes based on results.

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, GAO, and the U.S. Congress, and is not intended to be, and should not be used by anyone other than these specified parties.

January 12, 2007
Alexandria, Virginia