**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**

Report to the Board of Directors

For the Fiscal Year Ended June 30, 2006

DRAFT

**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**
**Report to the Board of Directors**
**For the Fiscal Year Ended June 30, 2006**

*Table of Contents*


| | *Page(s)* |
|---|---|
| Transmittal Letter | 1 |
| Required Communications | 2-4 |
| Current Year Comments and Recommendations | 5-9 |


DRAFT

MACIAS GINI & O'CONNELL LLP
CERTIFIED PUBLIC ACCOUNTANTS & MANAGEMENT CONSULTANTS

3000 S Street, Suite 300
Sacramento, CA 95816
916.928.4600

2175 N. California Boulevard, Suite 645
Walnut Creek, CA 94596
925.274.0190

515 S. Figueroa Street, Suite 325
Los Angeles, CA 90071
213.286.6400

402 West Broadway, Suite 400
San Diego, CA 92101
619.573.1112

To the Board of Directors
of the State of California Department of Technology Services
Sacramento, California

We have completed our audit work related to the financial statements of the State of California Department of Technology Services (the Fund) as of and for the year ended June 30, 2006. The accompanying report contains a summary of important matters related to our audit. We recommend that this report be read in conjunction with the financial statements.

Professional standards require that independent auditors communicate with the Board of Directors (Board) about matters that are likely to be important to the Board's oversight role. In the following report, we have provided commentary related to these communications.

During our audit we observed several opportunities to improve internal control and operations effectiveness. Our comments and suggestions regarding these matters are summarized in the current year comments and recommendations section.

We will review the status of these comments during our next audit engagement. We have already discussed these recommendations with the Fund's management, and we will be pleased to discuss them in further detail at your convenience,

The accompanying report is intended solely for the information and use of the Board of Directors and management of the Fund and is not intended to be and should not be used by anyone other than these specified parties.

Certified Public Accountants

Sacramento, California
January 23, 2007

**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**
**Report to the Board of Directors**
**Required Communications**
**For the Fiscal Year Ended June 30, 2006**

Professional auditing standards require that we provide you with the following information related to our audit.

## I. Our Responsibility Under U.S. Generally Accepted Auditing Standards and *Government Auditing Standards*

As stated in our engagement letter dated October 2, 2006, our responsibility as described by professional standards, is to plan and perform our audit to obtain reasonable, but not absolute assurance about whether the financial statements are free of material misstatement and are fairly presented in accordance with U.S. generally accepted accounting standards. Because an audit is designed to provide reasonable, but not absolute assurance, and because we did not perform a detailed examination of all transactions, there is a risk that material misstatements may exist and not be detected by us.

As part of our audit, we considered internal control of the Fund. Such considerations were solely for the purposes of determining our audit procedures and not to provide any assurance concerning such internal control.

As part of obtaining reasonable assurance about whether the Fund's financial statements are free of material misstatement, we performed tests of the Fund's compliance with certain provisions of laws, regulations, contracts and grants. However, the objective of our tests was not to provide an opinion on compliance with such provisions.

## II. Significant Accounting Policies and Unusual Transactions

Management is responsible for the selection and use of appropriate accounting policies. In accordance with the terms of our engagement letter, we will advise management about the appropriateness of accounting policies and their application. The significant accounting policies used by the Fund are described in Note 1 to the financial statements. No new accounting policies were adopted and the application of existing policies was not changed during the year. We noted no transactions entered into by the Fund during the period that were both significant and unusual, and of which, under professional standards, we are required to inform you, or transactions for which there is a lack of authoritative guidance or consensus.

## III. Accounting Estimates

Accounting estimates are an integral part of the financial statements prepared by management and are based on management's knowledge and experience about the past and current events and assumptions about future events. Certain accounting estimates are particularly sensitive because of their significance to the financial statements and because of the possibility that future events affecting them may differ significantly from those expected. The most sensitive estimates are depreciation and amortization of capital assets and intangible assets

**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**
**Report to the Board of Directors**
**Required Communications (continued)**
**For the Fiscal Year Ended June 30, 2006**

## III. Accounting Estimates (continued)

Management's estimate of the depreciation and amortization are based on historical cost and the useful lives of such assets. We evaluated the key factors and assumptions used to develop accumulative depreciation and amortization in determining that they are reasonable in relation to the financial statements taken as a whole.

## IV. Audit Adjustments

For the purposes of this report, professional standards define an audit adjustment as a proposed correction of the basic financial statements that, in our judgment, may not have been detected except through our auditing procedures. An audit adjustment may or may not indicate matters that could have a significant effect on the Fund's financial reporting process (that is, cause future financial statements to be materially misstated). In our judgment, none of the adjustments we posed, whether recorded or unrecorded by the Fund, either individually or in aggregate, indicate matters that could have a significant effect on the Fund's financial reporting process.

## V. Disagreements with Management

For purposes of this report, professional standards define a disagreement with management as a matter, whether or not resolved to our satisfaction, concerning a financial accounting, reporting, or auditing matter that could be significant to the financial statements or the auditor's report. We are pleased to report that no such disagreements arose during the course of our audit.

## VI. Consultations with Other Independent Accountants

In some cases, management may decide to consult with other accountants about auditing and accounting matters, similar to obtaining a "second opinion" on certain situations. If a consultation involves application of an accounting principle to the governmental unit's financial statements or a determination of the type of auditor's opinion that may be expressed on those statements, our professional standards require the consulting accountant to check with us to determine that the consultant has all the relevant facts. To our knowledge, there were no such consultations with other accountants.

## VII. Issues Discussed Prior to Our Retention of Independent Auditors

We generally discuss a variety of matters, including the application of accounting principles and auditing standards, with management prior to retention as the Fund's auditors. However, these discussions occurred in the normal course of our professional relationship and our responses were not a condition to our retention.

## VII. Difficulties in Performing the Audit

We encountered no significant difficulties in dealing with management in performing our audit.

DRAFT

**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**
**Report to the Board of Directors**
**Current Year Comments and Recommendations**
**For the Fiscal Year Ended June 30, 2006**

## I. REGULAR INVENTORY OF CAPTIAL ASSETS

During our review of capital assets, we noted that the Fund maintains a separate subsidiary ledger, which has different assets listed than what is listed on the capital assets listing from the California State Business Unit. In addition, several assets are recorded on the Business Unit's capital asset subsidiary ledger do not appear on the Fund's subsidiary ledger. According to policy, before disposing of property, the Business Services Unit should be contacted to ensure proper approval and disposal of equipment. The Business Services Unit should prepare the Property Survey Reports (STD. 152), when the disposal of the property occurs, or Transfer of Location of Equipment (STD. 158), when the property is being transferred to another state department.

In the past two years, there has been no reconciliation between the Fund's inventory of capital assets and the Business Unit's records. According to the Fund's policy, an inventory count should be conducted annually. Because no physical inventory of the capital assets has been performed, it is uncertain whether or not certain assets still exist or are impaired. We recommend that the Fund conduct regular physical inventories that would verify the existence and state of capital assets and update its capital asset subsidiary ledger as necessary. This subsidiary ledger should in turn be reconciled the Fund's general ledger and to California State Business Unit in order to ensure accurate reporting of capital assets on the financial statements.

In addition, we recommend the capital assets inventory, be tagged with a number that is recorded in both the Fund's and the Business Unit's subsidiary ledger. This process would improve management's ability to track the existence and possible impairment of capital assets.

**Management's Response:**

Management is in agreement. Effective with fiscal year 2006/07, the Fund has consolidated all asset records to one system. Items purchased by the department are recorded into the Remedy system by the Business Service staff. The Business Service staff also tag each asset with an inventory number when items are received and before they are put into production. The Fund has a policy in place for Business Service staff to prepare the Property Survey Reports when equipment is disposed or the Transfer of Location of Equipment form when property is transferred. The department plans on conducting a statewide asset inventory by the end of the calendar year. At the time of the inventory the department will reconcile the asset records with the financial records.

**STATE OF CALIFORNIA**
**DEPARTMENT OF TECHNOLOGY SERVICES**
**INTERNAL SERVICE FUND**
**Report to the Board of Directors**
**Current Year Comments and Recommendations (continued)**
**For the Fiscal Year Ended June 30, 2006**

## II. AGING OF "DUE FROM OTHER FUNDS"

During our examination of the receivable "due from other funds" account, we noted that $28,881,000 of the total $73,299,000 was outstanding for over 90 days as of June 30, 2006. In addition, another $12,463,000 was outstanding for over 60 days as of June 30, 2006. The total aged receivables over the allowable 60-days as established by the fund represent $41,344,000 or 56% of the total amount of the receivable. Although, the aging of the receivables does not indicate an issue of collectability (since the amounts are due from other State of California funds), it does significantly affect the Fund management's ability to properly manage cash flow, including timely payment of operating & nonoperating expenses. The Fund relies entirely on its revenue collections to maintain a 60-day working capital reserve.

We recommend that Fund management continue to communicate payment terms with the various customers that historically have not paid in accordance with such terms.

**Management's Response:**

Management is in agreement. Collection of outstanding accounts receivables is critical to the operation of our department. Our standard process for collection parallels the State guidelines. We send out invoices and follow up with three collection letters at 30 day intervals. We also maintain contact with our customers to promote timely payment. Regardless of our efforts, over 50% of our customers are significantly late in making payments which is a major concern of the department.

## III. REGULAR CHANGE IN PASSWORDS

Passwords used to access the Fund's network and the PeopleSoft application does not expire and there is no password configuration standard that is being enforced. This places the agency at an increased risk of unauthorized access to the network and financial data as well as all other electronic systems within the Fund's network. We recommend that the Fund formally adopt the Password Standards proposed by the Security Management Division as soon as possible and enforce an agency-wide password expiration period for network access and for financial application access.

**Management's Response:**

Management is in agreement. A password expiration period is currently not being enforced for either network or application access. The Fund's network (Windows network) password expiration was deactivated during the Active Directory consolidation project. As of November 8, 2006, the Password Standards (Department of Technology Services Bulletin 3136), is being revised and will require that passwords for access to the network and servers expire after a period of 90 days. There is, however, no specific password standard governing access to the PeopleSoft application. The Fund's Security Management Division will work to develop and implement a Password Standard for the PeopleSoft application in the first quarter of calendar year 2007 and will work to ensure the password standard is enforced for both network and application access.

## IV. DISASTER RECOVERY PLAN

The Fund does not have a comprehensive business continuity and disaster recovery plan. A defined plan is needed to address how the Fund would retrieve the department's financial information and regain operations of the financial management system. A plan is also needed to define how the financial administrative units would operate in the event the financial management applications were unavailable for an extended period of time. Without a defined plan that has been thoroughly reviewed with all critical personnel and tested to ensure it is an operationally viable plan, the Fund is at risk of loosing the availability of financial data and the ability to conduct financial transactions in the event financial management system were unavailable for an extended period. The Fund Administrative Division, in conjunction with the Engineering and Operations Divisions should work to develop and implement a comprehensive business continuity and disaster recovery plan for the financial systems data and all financial applications. Once developed and implemented, the plan should be periodically tested to ensure its viability. All findings from the tests should be incorporated into updates to the plan.

**Management's Response:**

Management is in agreement. Although we do not have a plan for recovery of the Fund's financial data in the event of a disaster, this is being addressed in the Continuity of Operations/Continuity of Government (COOP/COG) and an estimated completion date is scheduled for July 31, 2007. By this date management will have a comprehensive plan that covers the backup and recovery of all the Fund's functions. The Governor's Office, OES and Agency are also aware of this date.

## V. TERMINATION POLICY AND COMPUTER ACCESSS

While procedures are in place to ensure that network access is rescinded for personnel who terminate employment with the Fund (regular employees, temporaries, contractors, interns), there are no formal review procedures (internal audit procedures) to ensure only active personnel have access to the Fund's network and servers. Additionally, there are no formal procedures to ensure that access to the PeopleSoft application is terminated for these same terminated personnel. Having terminated employees with access to the financial applications places the financial data at risk and increases the likelihood of inappropriate or malicious activity taking place. The Fund Security Management Division should develop formal procedures and perform an audit as soon as possible over all user identification logons used for accessing the Fund's computer network and PeopleSoft application. This should be done to ensure that no terminated employees, temporaries, contractors, or interns remain active.

**Management's Response:**

Management is in agreement. The Fund utilizes a custom application called Staff Movement that includes the exit clearance process. This application includes an automated notification to all areas of the department requesting access termination for departing employees. However, the application does not include automated deletion or disabling of application access. It is up to each of the areas to deactivate user codes. Security Management agrees that an audit has to take place and Security Management is in the process of establishing the guidelines for this audit. PeopleSoft application managers have not historically been included in the notifications from the Staff Movement application. The Security Management Division will work to ensure that the PeopleSoft application managers are notified of departing personnel in a timely manner, so that their access may be rescinded. The audit guidelines and the procedures for notification of the PeopleSoft application managers will be completed in the first quarter of calendar year 2007.

## VI. POLICY FOR PERIODIC REVIEWS

While authorization profiles have been established within the PeopleSoft application there is no policy requiring the periodic review of users and their authorizations to ensure they are up-to-date and enforce a proper segregation of duties. The Fund Security Management Division should develop and implement a policy requiring the periodic review of user authorization roles within the financial applications to ensure they are up-to-date and enforce a proper segregation of duties.

**Management's Response:**

Management is in agreement. The Security Management Division is in the process of establishing a policy that will address this finding. The policy is scheduled for completion by March 2007.

## VII. PASSWORD PROTECTION – CONFIGURATION POLICY

The Fund's current password policy does not require that passwords be used for both network or application access, nor does it define a minimum password configuration standard for application access. The lack of appropriate password management places the agency at an increased risk of unauthorized access to the system and the financial data. While this lack of a complete password configuration policy is being addressed with the development of formal Passwords Standards, it has yet to be issued to all the Fund's functional users. The Fund should make a concerted effort to adopt and issue the Passwords Standards policy as soon as possible. Upon issuing the policy, audits should be performed by the Security Management Division to ensure compliance.

**Management's Response:**

Management is in agreement. As addressed in Section IV. REGULAR CHANGE IN PASSWORDS, the Password Standards (Department of Technology Services Bulletin 3136) has been revised as of November 8, 2006 and defines a password configuration standard for network and server access. A password standard, however, has not been implemented for application (PeopleSoft) access. The Fund's Security Management Division will work to implement an application password standard and will establish procedures to ensure audits are performed to ensure compliance. These efforts will be completed in the first quarter of calendar year 2007.

## VIII. ACTIVITY MATRIX

IT activities are not periodically evaluated against defined metrics and reported to senior management. It is through a defined set of activity metrics, such as network and application up-time, transactional processing time, and helpdesk response time, that the performance of the IT organization can be measured and tracked. Without defining the expectations of the IT organization, it is difficult to ascertain performance from year-to-year. The Fund's Operations and Engineering Divisions, in conjunction with the functional user departments should identify and establish a defined set of IT activity metrics upon which the divisions are rated. These metrics should be periodically reported to senior management.

**Management's Response:**

Management is in agreement. The agency understands the importance of the activity metrics in measuring and tracking the performance of the service deliverables and has plans to begin working on metrics and procedures by June 2007.