Commonwealth of Massachusetts

Management Letter
Year Ended June 30, 2002

COMMONWEALTH OF MASSACHUSETTS

TABLE OF CONTENTS

COMMONWEALTH OF MASSACHUSETTS

TABLE OF CONTENTS (CONTINUED)

Deloitte & Touche LLP
200 Berkeley Street
Boston, Massachusetts 02116

Tel: (617) 437-2000
Fax: (617) 437-21111
www.deloitte.com

Delittte
& Touche

December 30, 2002

Martin Benison, Comptroller
The Commonwealth of Massachusetts

In planning and performing the Single Audit of the Commonwealth of Massachusetts (the "Commonwealth") for the year ended June 30, 2002, on which we have issued our report dated December 30, 2002, we considered its internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on the Commonwealth's internal control. However, we noted certain matters involving the Commonwealth's internal control structure and compliance of management of the Commonwealth with laws and regulations that we consider to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the Commonwealth's internal control that, in our judgment, could adversely affect the Commonwealth's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements. Such matters have been reported to the management of the Commonwealth in the "Report on Compliance with Requirements Applicable to Each Major Program and Internal Control over Compliance in Accordance with OMB Circular A-133" dated December 30, 2002.

Our consideration of the Commonwealth's internal control would not necessarily disclose all matters in the Commonwealth's internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are considered to material weaknesses. A material weakness is a reportable condition 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 caused by the error or fraud in amounts that would be material in relation to a major federal program being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. None of the reportable conditions noted above are believed to be material weaknesses.

We also submit our comments concerning certain observations and recommendations relating to other accounting, administrative, and operating matters. These recommendations resulted from our observations made in connection with our audit of the Commonwealth for the year ended June 30, 2002. Our comments, arranged by Department, are presented on the following pages.

This report is intended solely for the information and use of management and federal awarding agencies and is not intended to be and should not be used by anyone other than these specified parties.

Yours truly,

Deloitte & Touche LLP

STATEWIDE OBSERVATIONS

Statewide Business Continuity Plan

A statewide business continuity plan has not been developed. A business continuity plan is broader than a disaster recovery plan, in that it provides an effective and organized way to determine critical business operations, including any that may be manual in nature, which may not be restored as a part of the disaster recovery. Funding for such a comprehensive plan, including the various state agencies, their critical business functions, employee responsibilities and infrastructure needs, has not been provided.

The effectiveness of the recovery of the data center during a disaster is diminished without provisions to support the recovery of each key business function. The disaster recovery plan is one element of an overall business continuity plan that covers all critical business resources. In the absence of a business continuity plan, there is a risk that critical business functions, especially manual in nature, may not be restored in a timely manner. In the absence of business impact analysis to determine the critical resumption point after a disruption, there is a risk that vital processes may not be restored. Such an analysis drives all other business continuity-planning activities, such as determining continuity strategies and policy and procedure development.

The Commonwealth has an obligation to protect its business, customer and citizen interests in the event of a major interruption of operations. This includes the ability of each state agency to provide the services expected of them and to carry out functions critical to the mission of the Commonwealth should an event occur, which interrupts the normal course of operations.

We recommend that the Commonwealth perform a comprehensive Business Impact Analysis (BIA) to determine which business functions are critical, what physical and logical infrastructure supports those functions, and to what degree its loss would impact the various agencies and the public in general. The analysis should identify the business, operational, financial and behavioral impact of potential disruptions. Once, the BIA is performed, a strategic plan should be developed, which defines resource requirements, develops recovery alternatives and recommends a recovery strategy. This strategic plan should then be used to drive the development of a comprehensive Business Continuity Plan. A thorough business continuity plan includes the following:

- Complete business impact analysis
- Resource and service requirements
- Backup and off-site storage programs
- Threat analysis and prevention programs
- Emergency response procedures
- Emergency teams
- Employee safety problems
- Business interruption insurance coverage
- Information systems, telecommunications, facility continuity plans

This plan should address the financial, operational and behavioral impact of a potential interruption. Upon completion, the plan should be shared with all employees and reviewed and tested periodically.

Reporting on the Commonwealth's Retirement Systems

The Commonwealth is unique among state governments in that it does not have separately prepared and audited public employee retirement systems annual report. The Commonwealth currently has the investments audited but does not prepare a comprehensive annual financial report for the public employee retirement systems. Therefore, many aspects of the program do not have the same level of audit coverage as would be found in other states.

The Commonwealth should consider preparing a separate comprehensive annual report for each of the retirement systems.

Also, on another issue concerning the Commonwealth's retirement systems, the Pension Reserve Investment Management Board ("PRIM") prepares and has audited the financial statements for the Pension Reserves Investment Trust Fund ("PRIT") on the cash basis of accounting. A review of these financial statements shows that investment income is the only income recognized. Withdrawals and contributions are not recognized as income/expense on these financials but they are recognized as income/expense by the Office of the Comptroller ("OSC") for the Statutory Basis Financial Report ("SBFR"). The cash basis PRIT financial statements are prepared and audited separately from the SBFR.. The OSC performs a conversion from the cash basis financials to the statutory basis financials shown in the SBFR. The largest reconciling item between PRIT and the SBFR relates to the withdrawals and contributions. For SBFR purposes, PRIT income and expenses are separated between State Retirement and Teacher's Retirement.

Prior to 1999, PRIM tracked, recorded and provided to the OSC the withdrawals from the State and Teacher's Retirement plans based on actual payments to retirees. However, because of personnel shortages, this tracking has ceased. The information on withdrawals from PRIM provided to the OSC for these two plans is now based on a 50/50 estimate. For example, if the total withdrawals are $1,000,000, $500,000 is credited to the State Retirement Plan and $500,000 is credited to the Teachers. For reporting purposes in the SBFR, OSC must perform a cumbersome and time consuming separation of the withdrawals based on actual payments for each retirement plan. In fiscal year '02, when the separation was completed, the OSC recorded an $81,025,000 adjustment between State and Teachers Retirement so that the withdrawal number equaled the actual amount withdrawn for each retirement plan.

We recommend that OSC work with PRIM to restore the tracking and recording of the withdrawals from the State and Teacher's Retirements plans based on actual payments to retirees rather than a 50/50 estimate.

Higher Education Shared Services Center

The Commonwealth should evaluate whether a higher education shared services center would improve the efficiency and accountability of the accounting and student financial aid operations of the community and small state colleges. A secondary goal would be to use the shared services center to reduce the operating costs of non-academic functions. The recent problems encountered at Roxbury Community College and Salem State College combined with the turnover experienced by other institutions as a result of the ERIP program, indicate the need to challenge the current approach to providing the "back room" operations of the state's higher education system.

The use of a shared services center is one approach to improving the accounting and student financial aid operations of many of the smaller institutions of higher education. A shared services center, whether run by a governmental entity or outsourced to a private entity, could provide the following benefits:

1. The ability to keep pace with ever-changing technology
2. Flexibility and scalability
3. The foundation for Internet based e-Business/e-Government

4. The ability to enhance responsiveness and customer satisfaction
5. Best business processes and practices
6. The ability to attract and retain good people
7. Optimizing the allocation of existing resources
8. Cost savings and cost control
9. Better information for management decision making
10. Continuous improvement with new ideas and service offerings

Various governmental entities have begun to use shared services centers or similar concepts (See June 2001 issue of *Government Finance Review*). In addition, the Apollo Group (University of Phoenix) has used outsourced providers to service both its accounting and student financial assistance functions.

In considering whether to move to a shared services concept the Commonwealth should perform the following steps:

- Complete a business process diagnostic evaluation at a number of institutions;
- Prepare a requirements definition of core financial functions;
- Obtain buy-in from upper management and user institutions;
- Develop documentation deliverables;
- Perform a best practices review of current operations and new technology; and
- Research the cost of communications links to the shared services center.

Early Retirement Programs and Service Continuity Planning

In response to the significant budget deficits experienced during fiscal year 2002, the Commonwealth offered an early retirement incentive program ("ERIP") to its employees in an effort to reduce spending and another such program is being currently discussed. Under the 2002 ERIP, only the most critical positions vacated were filled. This situation, while not new to the Commonwealth, highlights an issue that the Commonwealth must address–ensuring continuity of service in all of its most critical functions. These personnel reductions may have been a prime contributor to the increase in the number of noncompliance and internal control findings resulting from the Single Audit from 49 in 2001 to 81 in 2002.

As part of the Office of the Comptroller's Internal Control Campaign (See related comment on Compliance with Chapter 647), it has urged and educated departments to conduct department-wide risk assessments. In essence, department heads and managers should be asking themselves the question "What keeps me awake at night?" One of the answers to this question in these times of budget deficits and retirement incentives should be ensuring the continued delivery/performance of their most critical functions. Completing the risk assessment and making sure that there are policies and procedures in place to mitigate those risks is critical. Also, any additional ERIP programs should allow sufficient time to ensure the transfer of the requisite knowledge from the individual leaving to his/her replacement.

Employee Recognition Programs

As the Commonwealth enters the uncertain economic period of 2002/2003 with reduced tax collections and looming budget deficits, it is important to look at programs that produce cost savings while at the same time rewarding and retaining the resources needed to run the business of government. The impact of the loss of talented, experienced employees has been evidenced throughout the Commonwealth in the wake of the ERIP program that was offered during fiscal year 2002 (see previous comment). At this time, it is more important than ever to ensure that the retention of talented employees is a high priority.

The Pride in Performance in Massachusetts has cut back on the emphasis of employee recognition during this fiscal period–from dinners to brief receptions.

Rewarding and retaining governmental employees has always been a challenge for governmental entities. It is always more of a challenge to reward employees in tight economic times. In looking at models from other states. Several programs are worth noting.

One idea is a "Shared Savings Program" modeled after similar private sector models. This program encourages employees to submit ideas for managing, building or buying something more efficiently. Any actual savings go into a special account and, after a year, half of the savings recognized in the department goes to the department employees.

A second idea is a quality service award, which allows individual employees to earn financial recognition for accomplishments. The program awards up to $10,000 to one person or to a number of people. Massachusetts does have the Carballo award which awards up to $1,000 to one person or group.

While other types of programs exist, the goal for Massachusetts should be to reward talented employees while reducing overall costs and improving operational efficiency.

Education Program

During fiscal year 2002, the Commonwealth implemented the provisions of Governmental Accounting Standards Board ("GASB") Statement No. 34, "Basic Financial Statements – and Management's Discussion and Analysis – for State and Local Governments" ("GASB 34"). This statement establishes new financial reporting standards for state and local governments and component units. The new standards are designed to make governmental financial reports easier to understand and more useful to the citizenry, legislature, oversight bodies, investors and creditors. These statements include requirements for a management's discussion and analysis and dramatically change the basic format of the financial statements, by requiring governments to provide basic financial statements both at a fund level, similar to what has been reported in the past, and at a government-wide level. The latter changes to the governmental reporting model focus attention on the overall financial condition of the government. The display of the overall operations of the government into a limited number of columns with debt and long-term assets combined with the other assets and liabilities will begin to place an emphasis on the questions of whether the government as a whole is better or worse off than the previous year. While the concept is commercial in nature the emphasis will be on the change in net assets.

This emphasis on financial condition is similar to the emphasis on the issue of interperiod equity. This focus should be on the development of plans to pay for long-term obligations, both debt related and non-debt related, while also recognizing that financial plans need to exist for the repair or replacement of fixed assets and infrastructure. The focus is not so much on the growth of net assets as it is on the maintaining of a net asset balance that demonstrates a sound and stable financial condition with sufficient resources to offset economic downturns.

As management has been planning and working to implement GASB 34 over the past several years, the focus on education relating to the new reporting model has been directed at those individual's responsible for preparing the financial statements. The implementation has been completed and management now should consider the needs of the users of the financial statements. Given the focus on the overall financial condition of the Commonwealth and the issues of intergovernmental equity that are inherent to the new financial reporting model, management should also consider developing a training program that is focused on educating the administration, the legislature and other potential users of the financial statements to the changes and more specifically, what those changes mean. Models should be developed that stress the need for plans to support the future financing of obligations and assets. Management should ensure that legislators understand the impact that GASB 34 will have on the financial statements and the implications of legislative action on financial reporting. This will ensure that decisions made at the legislative level will be consistent with those deemed prudent by management.

Individual Funds

As discussed in previous years' management letters, the number of funds required by the Legislature and used by the Commonwealth hampers the efficiency of the accounting and financial reporting process. In fiscal year 2002, the Office of the Comptroller ("OSC") operating under the requirements of State Finance Law and the requirements of the Legislature, as established through the budget and Massachusetts General Laws, used approximately 113 individual funds to account for the operations of the Commonwealth.

The use of 113 individual funds makes it difficult for either internal or external users of the Commonwealth's financial information to obtain a clear, concise understanding of the overall operations and financial position of the Commonwealth. Instead of enhancing accountability, the large number of funds makes it difficult for management to perform an effective analysis of operations and to detect errors.

While many of the individual funds designated by the Legislature have been created to monitor and control resources for a specific purpose or associated with a specific peeve of legislation, this function can effectively be met by using "sub-funds" within the General Fund.

The existing fund structure and number of funds has resulted in the following issues:

1. The Legislature regularly budgets expenditures in funds without providing corresponding revenue to support the activity. This effectively overstates the General Fund balance, creates deficits in other funds and, more importantly, raises the question of whether, in fact, a balanced budget at all levels has been passed as required by Massachusetts General Laws.

2. Split appropriations require extensive effort on the part of management to properly account for the fiscal year activity and report final operating results. Split appropriations are a budgetary practice that is unique to Massachusetts.

3. With the implementation of GASB 34, each of the individual 113 funds must be analyzed to determine if it should be reported as a major fund. In addition, the activities of the funds will need to be reviewed to determine the "individual" adjustments necessary to bring the accounts to full accrual.

4. Generally accepted accounting principles require all fund balance deficits to be reported in the financial statements along with a plan for correcting those deficits. Currently, 33 funds have fund balance deficits.

5. GASB Statement No. 38, "Certain Financial Statement Note Disclosures," also implemented in fiscal year 2002, requires the Commonwealth to provide the detail of all transfers between the funds and such transfers need to be discussed in the Commonwealth's footnotes.

The following table lists the budgeted funds with a statutory fund balance deficit (amounts in thousands) at June 30, 2002:

Budgeted Fund #	Fund Name	Deficit*
101	Highway	$ 437,529
102	Local Aid Fund	1,119,125
106	Anti-trust Law Enforcement Fund	2,901
110	Victim and Witness Assistance Fund	13,323
111	Intercity Bus Capital Assistance Fund	5,562
119	Child Support Penalty Fee	498
134	Environmental Challenge Fund	797
149	Toxic Use Reduction Fund	8,416
152	Environmental Permitting & Compliance Assurance Fund	50,872
154	Underground Storage	19,360
156	Environmental Law Enforcement Fund	4,482
157	Public Access Fund	414
158	Harbors and Inland Waters Maintenance Fund	6,244
159	Marine Fisheries Fund	6,498
160	Watershed Management	2,104
161	Low-Level Radio Active Waste Management Fund	433
172	Leo J. Martin Recreation Fund	240
173	Clean Air Act Compliance Fund	1,700
186	Second Century Fund	2,819
188	Children and Senior Health	60,784
192	Trans. Aid to needy families	7,618
193	Social Services Program Fund	2,314
194	Local Consumer Inspection Fund	574
	Total	$1,754,607

*Deficits in these budgeted funds increased by $1,335,237 during the fiscal year ended June 30, 2002.

While some funds with minimal activity were repealed during the fiscal year and more are legislated for repeal during fiscal year 2003, a large number of funds remain and should be evaluated as to their continued need. The following table (amounts in thousands) shows fund activity as of June 30, 2002 for those funds with minimal or no activity during the year. This list excludes funds that were created or repealed during fiscal 2002 and funds whose repeal has been legislated for fiscal 2003.

Fund Number	Fund Name	Revenues and Other Financing Sources	Expenditures and Other Financing Uses
018	Ratepayer Parity Trust Fund	$ 531	$ -
019	Child Support Penalty Fee Fund	784	1,195
022	Brownfields Revitalization Fund	397	2,416
025	Liability Management & Reduction Fund	2,642	2,570
026	Firearms Records Keeping Fund	518	206
027	Mass Clean Election Fund	1,383	356
029	Debt Defeasance Trust	-	-
031	Oil Overcharge	228	1,788
033	Civil Monetary Penalty Fund	902	3
036	Catastrophe Illness in Children's Relief Fund	2,519	120
041	Division of Professional License Trust Fund	1,019	318
042	Victims of Drunk Driving Trust Fund	17	-
106	Antitrust Law Enforcement Fund	364	500
107	Government Land Bank Fund	2,456	2,456
108	Natural Heritage and Endangered Species Fund	485	290
111	Intercity Bus Captial Assistance Fund	644	136
118	Federally-Assisted Housing Fund	136	136
132	Motorcycle Safety Fund	93	147
136	Environmental Trust Fund	1,604	1,909
138	Children's Trust Fund	7	24
140	Labor Shortage Fund	33	1,499
144	Drug Analysis Fund	90	87
153	Massachusetts AIDS Fund	163	252
157	Public Access Fund	936	1,054
158	Harbors & Inland Waters Maintenance Fund	2,938	1,583
161	Low-Level Radioactive Waste Mgt. Fund	184	112
165	Ponkapoag Recreational Fund	885	877
168	Board of Registration in Medicine Fund	1,805	1,805
169	Asbestos Cost Recovery Fund	1,551	1,026
172	Leo J. Martin Recreation Fund	443	504
179	Reggie Lewis Track and Athletic Center Fund	303	270
180	Assisted Living Administration Fund	784	356
185	Solid Waste Disposal Fund	-	-
187	Safe Drinking Water Fund	2,205	2,232
189	Diversity Awareness Education Trust Fund	-	-
190	Child Care Quality Fund	286	107
194	Local Consumer Inspection Fund	-	-
198	Voting Equipment Loan Fund	-	1,397
330	Revolving Loan Fund	964	12
	Total	$ 30,299	$ 27,743

Such funds represent less than 1% of the activity of the governmental funds of the Commonwealth.

To improve accountability, the OSC, working with the Secretary for Administration and Finance and the Legislature, should seek legislation to:

- Combine or eliminate many of the existing funds noted above. Any remaining funds should be specifically identified in the legislation and any "new activities" subsequent to the legislation should be limited to the establishment of sub-funds unless, after consultation with OSC, a conclusion is reached that individual fund reporting is appropriate.

- If combining or eliminating funds is not accomplished, legislation should be proposed to require funds, other than Capital Project Funds, that have had a deficit in fund balance for three consecutive years be reduced to a zero balance as part of the subsequent year's budget.

- "Sunset" provisions should be enacted to require that every fund and sub-fund, other than the General Fund, be reviewed every five years to determine whether or not it should be continued. In the absence of a positive action by the Legislature to continue the fund, the Legislature should require that its balance be transferred to the General Fund and the fund or sub-fund abolished.

Prior Appropriations Continued

Massachusetts makes extensive use of the carryforward of unexpended appropriations ("prior appropriation continued" or "PAC") therefore reducing the effectiveness of the current budget process. Appropriations continued from fiscal year 2002 to 2003 totaled approximately $171 million, a $119 million decrease from the prior fiscal year. The unexpended balance in the General Fund for all appropriations at June 30, 2002 is approximately $86 million, a $97 million decrease from the prior year. Though these balances decreased in the current year, those decreases are the result of deteriorating tax collections and budget deficits not the result of any changes in policy with regard to the use of PACs. In fact, these decreases reverse an upward trend that has continued since 1993.

Under Massachusetts General Law, the Commonwealth has the option of either reverting unexpended funds or carrying the balances forward to the next fiscal year. Though not the case over this past year because of the current fiscal crisis, the recent trend indicates that more funds are being carried forward from year-to-year than is necessary, thereby diminishing the value of the budgetary controls that should be an element of the annual appropriation process.

The Legislature should carefully review and evaluate its use of PACs and its procedures for appropriating and carrying forward funds so that the available funds are more fully utilized to operate the various programs sponsored by the Commonwealth.

Workers' Compensation and Group Health Insurance

The Commonwealth should establish a funding schedule to accumulate assets to satisfy the current under-funded liability related to the internal service funds. As of June 30, 2002, the unfunded liability for the workers compensation and group health insurance funds was $267.6M and $53.9M, respectively. With the implementation of GASB 34 in fiscal year 2002, these balances now represent accumulated liabilities and, as such, are reported as liabilities in the governmental fund statements directly reducing the "net assets" of the Commonwealth. Ultimately, these and other obligations could result in a negative net asset position.

Available options to furnish the necessary funding include a surcharge to the current statutory charge back to state agencies, an annual appropriation based upon an actuarially calculated funding schedule, a redirection of investment earnings, and other actions. The Office of the Comptroller and the Legislature should coordinate their efforts to evaluate all options and select the most appropriate steps to satisfy the existing liabilities and fund future liabilities as incurred.

Activity Based Costing

Management, citizens and their representatives in the Legislature have a heightened interest in what programs cost, the cost of delivery under various alternative models and the cost of the individual items or elements required to deliver a service. Activity based costing is an approach used by many governmental entities to determine the true cost to deliver a service.

The Commonwealth benefits from having agencies like the Office of the Comptroller employing activity based costing models as part of the overall management reporting systems. These models allow the Commonwealth to more accurately determine the benefits of electronic benefits transfers, payroll direct deposits or the privatization of an activity. We recommend that the Commonwealth begin additional pilot projects to determine the cost of activities and services that are currently under review for changes in their processes. These pilots should then be used to develop a process for calculating the cost of a broad range of Commonwealth activities.

Investor Relations Programs and Related Disclosures

The Commonwealth should review its investor relations program.

In spite of other events that have occurred over this past year in the securities markets, the United States Securities and Exchange Commission ("SEC") continues to focus on municipal securities and investor information because of the emerging dominance of individual investors in the municipal market. More than 70% of the outstanding obligations are held by or for individuals either directly or through bond funds and nearly 40% of the total is held by individuals themselves or in their personal trust accounts. Because many investors purchased their bond holdings in the secondary market, the disclosures to that segment of the marketplace are receiving a growing level of attention. The SEC has begun to focus on information on governmental websites and whether the information has the potential to mislead investors. Properly used, the website is an important element of an investor relations program and an aid in complying with the SEC rules applicable to governmental securities.

The Government Finance Officers Association ("GFOA") has issued a recommended practice on "Maintaining an Investor Relations Program". The centerpiece of the GFOA's recommended investor relations program is a commitment to provide annual financial, operating, and other significant information in a timely manner consistent with federal and state laws and SEC rules. Issuers were encouraged to consider addressing the following concerns:

1. Identify individuals responsible for speaking on behalf of the issuer.

2. Develop procedures for identifying and selecting information, both positive and negative, to be made available to investors.

3. Develop procedures for disseminating information so that it gets to all parts of the market simultaneously and not just selected investors.

4. Develop procedures to ensure potential investors receive a copy of the preliminary official statement at least one week in advance of a bond sale.

5. Identify ways to stay abreast of issues that are likely to be of concern to investors.

6. Develop and maintain a good relationship with the rating agencies.

7. Establish procedures to ensure that financial statements or other information needed for disclosure purposes are completed on a consistent schedule from year-to-year and prior to the date established in any contractual commitments.

8. Delineate clearly the roles and disclosure responsibilities in conduit borrowings.

9. Engage in marketing activities to alert investors of a pending bond sale.

10. Identify investors who hold the issuer's bonds to improve communications.

11. Be aware that legal issues may exist with respect to securities information provided by electronic means.

Recent industry publications have described examples of investor relations programs and specifically the fact that most investors do not accept the minimal disclosures required by SEC Rule 15c2-12 as sufficient. The following steps, over and above what has been recommended by the GFOA, have been recommended as ways that such programs may be enhanced:

1. Conduct research into the legal requirements.

2. Examine the information needs of the bond rating agencies, bond insurers and underwriters regarding their requirements to comply with SEC and Municipal Securities Rulemaking Board rules.

3. Develop a cover sheet for all filings with the Nationally Recognized Municipal Securities Information Repositories (NRMSIRs) that contained all CUSIP numbers. Such a cover sheet is to accompany all filings and is necessary for the NRMSIRs to be able to tie disclosure documents to specific bond issues

4. Add an "investor relations site" to the governments Web page.

5. Develop a quarterly investor newsletter that is posted on the Web site.

In the current environment and in consideration of recent scrutiny that has been given to the Commonwealth by the SEC, the development of such a program can only enhance its relationships with both the investor community and the SEC. In addition, by providing information directly to the investor community in this manner and by increasing confidence in the marketplace the Commonwealth may ultimately increase investor interest in the debt with a corresponding lower interest rate as a result of demand and obtain more favorable bond ratings.

Chapter 647, the Internal Control Act - The Campaign Continues

Massachusetts General Law, Chapter 647, *State Agencies Internal Control Act of 1989* ("Chapter 647") outlines internal control standards, defines the minimum level of internal control systems and establishes the criteria against which internal controls will be evaluated. Chapter 647 also states "Internal control systems for the various state agencies and departments of the Commonwealth shall be developed in accordance with internal control guidelines established by the Office of the Comptroller." The Office of the Comptroller ("OSC") has issued written guidance in the form of the *Internal Control Guide for Managers* and the *Internal Control Guide for Departments.* Departmental implementation of Chapter 647 and these Guides have become known throughout the Commonwealth as the "departments' internal control plans".

Since the passage of Chapter 647, the OSC in addition to publishing the above-mentioned guides, has assisted departments, when requested, in developing internal control plans; conducted training sessions on internal controls and risk assessments; and, in conjunction with the Office of the State Auditor ("OSA"), reviewed departmental internal control plans upon request or as part of the statewide Single Audit. The fiscal year 2002 statewide Single Audit was used as a vehicle to continue the OSC's internal control campaign and build upon the groundwork that was set during the fiscal year 1999 Single Audit. The 1999 Single Audit was used a vehicle to educate departments on the new definition of internal control and emphasize the need for internal control plans to adopt this new definition. The 2000 Single Audit continued the education process primarily by: (a) making site visits to the departments which receive the major emphasis of the Single Audit, (b) interviewing the department's Internal Control Officer to discuss the department's approach to implementing internal controls, (c) reviewing the internal control plan to obtain an understanding of the plan's organization, scope and composition with a special emphasis on determining if the department had conducted a department-wide risk assessment. In 2001, follow-up site visits of the departments whose plans were reviewed in 2000 were made.

In the 2002 Single Audit, a team comprised of personnel from the OSC, OSA and the independent audit firm began reviewing the department-wide risk assessment component of a department's internal control plan. In addition, OSC held statewide training on building a risk assessment and performed individual customized training, as requested. All 157 departments were requested to provide their risk assessment for review and, as of the end of audit fieldwork, the review continues. Feedback letters, jointly signed by the OSC and OSA, were provided to the departments whose risk assessment review was complete. The team found that most departments have made a good faith effort to document their top five to ten department-wide risks. However, improvements are still needed. For example, some departments continue to think only in fiscal terms to the exclusion of programmatic risks, some departments' risks appear not to align with all of the important goals of the department and some provided risks that were at a level lower than department-wide.

The OSC's internal control campaign has had significant results and is continuing so that the intent and spirit of Chapter 647 and the Guides can be more fully realized. To this end:

1. The Comptroller should issue a memo to each department's Chief Financial Officer and Internal Control Officer urging them to use their internal control plan as a major component in the department's transition documents for the new administration;

2. The review of all departments' risk assessments should be completed;

3. The departments whose risk assessments have been judged to most fully comply with the Guides should be asked to show that it has internal control policies and procedures in place to mitigate those risks;

4. The OSC should consider developing a template or model internal control plan or risk assessment component for those departments with common operations, such as the 15 community colleges and the 10 sheriffs' offices; and

5. The OSC and the OSA should continue to evaluate the need to amend Chapter 647 to re-emphasize and re-energize the internal control focus.

OFFICE OF THE COMPTROLLER

GAAP Packages

All departments are required by the Commonwealth to submit a "GAAP Package" to the Financial Accounting and Reporting Bureau ("FRAB") of the Office of the State Comptroller ("OSC"). The purpose is to properly accumulate the information needed to report the Commonwealth's financial condition and results of its activities in accordance with generally accepted accounting principles ("GAAP"). In anticipation of the preparation of the GAAP packages, OSC distributes instructions to all departments detailing the information needed, including accruals for receivables, leases and other balances.

The OSC set August 10, 2002 as the submission deadline for the GAAP Packages. Twenty-four priority III departments failed to submit a GAAP Package for fiscal year 2002. Many of these departments also failed to file GAAP packages in prior years as well. This forces FRAB to make certain estimates and assumptions (concerning payroll, number of employees, etc.) in order to prepare statements. Although these priority III departments are immaterial individually and in the aggregate, the amounts should be reported to provide an accurate financial picture.

The OSC should continue to communicate with Chief Fiscal Officers the need to prepare this package in a timely manner.

OFFICE OF THE STATE TREASURER AND RECEIVER GENERAL

Long-Term Debt Information

In the Office of the State Treasurer ("Treasury") the management of the Commonwealth's long-term debt program is the responsibility of a single employee who is assisted by a professional staff member. Under this individual's direction, transactions entered into by the Treasury on behalf of the Commonwealth have become increasingly complex, including innovative refunding transactions and variable rate bonds that involve imbedded derivatives.

Given the complexity of the transactions being entered into by the Commonwealth and the importance of the debt management program to the fiscal health of the Commonwealth, the continuing implementation of an effective debt management cross-training program at the Treasury is essential. The loss of this individual and the intellectual capital that would result could be detrimental to the Commonwealth's ability to effectively manage it's debt.

It should also be noted that this same individual is also responsible for preparing all of the documentation relating to the proper accounting for these transactions (i.e. distribution and use of funds). Competing responsibilities placed upon this individual have resulted in significant delays in the preparation of documentation to both the Office of the Comptroller and auditors of the Commonwealth's financial statements as well as in recording transactions on the official books and records of the Commonwealth.

The Treasury should continue to implement a cross-training program for its debt management program. The objective of the program should be to provide for an effective sharing of knowledge and information to ensure that the loss of one individual will not significantly impact the Commonwealth's ability to effectively manage its long-term debt. Management should also be supplementing this cross-training program by formally documenting the policies and procedures relating to managing and accounting for long-term debt.

To mitigate the delays experienced in the processing of a proper accounting of debt transactions, management should assign someone other than the individual preparing the transaction to prepare the accounting for the individual bond transactions. To that end, management should develop a transaction-closing checklist to identify all the steps that need to be completed before a sale is considered final. The checklist should include information necessary for the preparation of financial reporting systems and be monitored by management so that delays in completion can be explained. If the checklist is designed correctly, the rollforward of debt information can be continually updated throughout the year.

Cash Management

In prior years, we have noted a need for management to consider a cross-training program in the area of Cash Management similar to what has been discussed above for Debt Management. During the current fiscal year, there has been a significant increase in staff in this area, processes have been documented and some responsibilities have been delegated. Final review and responsibility, however, remains centralized to one person. The loss of this individual's experience and expertise could potentially have an adverse effect on the Treasury's cash management operations.

Management should continue the work that they have begun but the focus should be refined. Adequate staff resources are now in place. Management should consider the creation of a high level supervisory position. The supervisory position should be staffed with a qualified individual having a background in accounting and adequate management experience. This high level supervisor should be qualified and effectively cross-trained to relieve a good portion of the burden placed on the Deputy Treasurer and be trained to understand the acting role of the Deputy Treasurer and be able to act as a temporary replacement in the event of the Deputy Treasurer's absence.

Disaster Recovery and Business Continuity Planning

The Treasury does not have a documented Disaster Recovery Plan ("DRP" or "Plan") or an updated Business Continuity Plan ("BCP") that encompasses all of its operations. While the Treasury did develop a Business Continuity Plan for Y2K which was updated in May 2000, it has not been tested or updated since then. Also, the Treasury has developed and updated a Plan and BCP for its cash management operations.

The day-to-day business activities at the Treasury include regular exchange of data with the Information Technology Division ("ITD") of the Commonwealth. However, all Treasury systems are housed outside of ITD's data center. It is therefore essential for the Treasury to develop its own disaster recovery plan and align it with that of ITD's, so as to ensure a seamless recovery of systems and related business processes.

A DRP documents the actions to be taken should the data processing facility be damaged or destroyed. Without an up-to-date, tested Plan, valuable time can be lost while options are identified and evaluated, alternative processing methods developed and the required approvals obtained. However, the information technology Plan is one element of an overall BCP that covers all critical business resources. The effectiveness of the recovery of the data center during a disaster is diminished without provisions to support the recovery of each key business function, e.g., debt and payroll as well as cash management. To this end, an all-encompassing business impact analysis to examine the Treasury's business processes and identify critical areas of exposure, for which mitigating actions are needed, has not been performed.

We recommend that the Treasury perform a comprehensive analysis to determine which business functions are critical, what physical and logical infrastructure supports those functions, and to what degree the loss of this infrastructure would impact its respective business units and the Treasury in general. Once the analysis is performed, a strategic plan should be developed, which defines resource requirements, develops recovery alternatives and recommends a recovery strategy. This plan should then be used to drive the development of a comprehensive Disaster Recovery Plan and finally, a Business Continuity Plan. A detailed BCP is a tactical approach based on pre-identified critical technical functionality. The BCP is a strategic approach, which outlines the policies and procedures for conducting disaster emergency response, recovery, and restoration operations. A thorough BCP includes the following:

- Complete business impact analysis
- Resource and service requirements
- Backup and off-site storage programs
- Threat analysis and prevention programs
- Emergency response procedures
- Emergency teams
- Employee safety
- Business interruption insurance coverage
- Crisis notification scripts
- Information systems, telecommunications, facility continuity plans

Upon completion, the BCP should be shared with all employees and reviewed and tested periodically.

Backup Storage and Backup Analysis

The Information Technology group at the Treasury has a defined backup schedule, however, it has not been revisited (in the past few years) to ensure that critical systems are backed up appropriately. In addition, backups are not sent offsite on a daily basis. They are maintained in a room adjacent to the data center. Since backups are shipped offsite only once a week, in the event of a disaster, the Treasury can lose up to a week's worth of data.

System backup is a critical component of an effective business and technology recovery plan. It is important to revisit this plan periodically, to ensure that all existing systems and any new systems or upgrades are backed up according to business requirements. Regular off-site storage of data ensures that vital records are available in the event of an emergency.

A good retention and rotation strategy allows an organization to maintain the flexibility of their systems and gives them the reasonable assurance that they will be able to recover their systems in the event of a disaster. We recommend the Treasury perform a detailed analysis of its existing backup strategy. This analysis should include identifying critical systems and related maximum recovery time objectives. Based on the results, the Treasury should develop a backup schedule. The Treasury should also consider increasing the frequency of shipping backup tapes offsite, potentially to a daily rotation schedule. This will ensure that in the event of damage or destruction of the facilities, the Treasury can retrieve data maintained offsite and perform a recovery of its systems.

Notification of Terminations and Transfers

The Information Security ("IS") group at the Treasury does not have a formalized process to receive notification from individual departments regarding user terminations or transfers. As a result, there could be a potential delay between the effective change and notification to the IS group.

Active administration of information systems security is important to ensure that security policies and procedures are consistently applied across the organization especially over time and during instances of high employee turnover, such as currently occurring in the Commonwealth due to the Early Retirement Program which is discussed on page 4. The lack of standard procedures to administer user access related to additions, terminations and other changes increases the risk of unauthorized access and may contribute to higher levels of administration and overhead costs, inefficiencies and potential security exposures.

The Treasury's Human Resources group should provide regular reports to its IS group, in order to ensure that any changes in the users' access privileges are communicated and performed in a timely manner.

Access paths are the logical routes of access to systems and data. In a multi-systems environment, such as the Treasury, there are multiple access paths to data. It is therefore essential to evaluate systems' access privileges granted to employees, by performing periodic user access reviews. The reports from such reviews should be sent to the individual department heads to verify that existing access privileges are commensurate with job functions.

Physical Security Mechanisms

The Treasury does not have adequate physical security mechanisms in place to ensure that critical data and sensitive information are protected from unauthorized access. It was observed that:

- Although individuals working in the Ashburton data center monitor user access, there are currently no physical access restrictions in place to record access;

- Although access to the check printing area in the Chelsea data center is restricted, the key to the check stock room is not maintained in a secure area. There are no means to record who accessed the room or if the key was duplicated; and

- The door of the office, where blank check stock for legislative or reissue checks is stored, is open and accessible during office hours. Although the cabinet storing the stock is locked, the key is physically accessible. In addition, it was confirmed that the check printer, although it can be locked, currently does not have a key.

The primary goal for providing physical security of critical information resources is to minimize the threats due to damage or losses to computer assets maintained in a centralized area. Like all negotiable instruments, blank check stock is subject to a high degree of fraud or theft. Inadequate controls surrounding the security and accountability of this stock may result in misappropriation of assets. Hence it is essential to ensure that adequate physical security is maintained to restrict access to such information to authorized individuals only.

We understand the Treasury recognizes this exposure and is currently soliciting bids for installing key cards in the Ashburton and the Chelsea data center. We recommend management continue to make this a priority. Also, we recommend that management move all blank stock for legislative and reissue checks to a secure area. The check printer used to print such checks should be locked at all times and keys should be provided to authorized individuals only.

Legislative Payroll System

The Treasury is responsible for maintenance and administration of the Legislative Payroll system. Although the system has pre-established office expense amount for new Legislators, there are no system restrictions to prevent the amount from being altered. Office expense amounts are granted at a flat rate to all Legislators.

In the absence of system controls to ensure that this amount is not being altered, office expense funds may be misappropriated to the Legislators. Treasury should consider expanding the functionality of the system, such that this amount cannot be changed, without invoking a program change. In order to enforce effective segregation of duties, the Legislative Payroll group should not be granted the authority to make the program change.

Password Confidentiality on the Fleet System

The Fleet online system (used for stops, splits and reissued checks) is kept logged on throughout the day. The system remembers the login credentials of the first person to log on, therefore not requiring any subsequent users to logon separately. In addition, one of the users does not have a unique UserID and password assigned, hence always shares an ID and password with another user.

In order to help ensure a strong information security environment, password confidentiality is essential. Also, it is essential that users be assigned their own UserID and passwords. In the absence of unique UserID and passwords, there are no means to establish an audit trail.

We recommend the Treasury assign unique UserID and passwords and encourage users to login uniquely on the Fleet online system. This control will promote accountability and help to identify an audit trail for monitoring unauthorized activity. Also, users should completely disconnect the Fleet connection and sign off before leaving the terminal. This will ensure that the system forces the next user to log in with their unique ID.

System Controls to Promote Effective Segregation of Duties

Certain departments within the Treasury, have manual procedures in place to facilitate a segregation of duties, however, there were no system controls in place to enforce the procedures. During our work the following observations were made:

- There are no system controls in place to restrict an individual from stopping and reissuing a check
- In the Abandoned Property system, there are no system controls in place to prevent a Supervisor (with approval authority) from entering, reviewing and approving their own work; and
- The State Retirement Board system does not prevent an individual performing deposits from changing a retiree's bill.

System controls supplementing manual procedures will help minimize the threat of misappropriation of assets and enforce stronger segregation of duties. System controls should be such that they can record UserID to help maintain an audit trail and promote accountability.

The Treasury should consider implementing greater system restrictions in the Check Stop and Split system, so that an individual is not allowed to stop and reissue the same transaction. In the case of the Abandoned Property system, the Treasury should enhance the existing controls to a more refined level, such that the Level 3 Analyst (Supervisor level) does not have the authority to approve his/her own transaction. In case of the State Retirement Board system, the Treasury should expand the system functionality to include the Buyback function security, thereby restricting those in deposits from changing a bill.

Access to Management of Retiree Accounts

The State Board of Retirement is a division within the Treasury. It is primarily responsible for administration of pension and retirement benefits granted to state employees. Although two individuals have been designated to manage retiree account information, the State Retirement Board ("SRB") system does not restrict access to only those two individuals. Other SRB users have COSMO access #33, which allows all account maintenance activities. Maintenance audit trail reports exist to record user ID, but reports are not reviewed regularly to ensure that only designated users are making the changes.

Audit trail reports provide detailed information regarding who accessed an application and when. Without regular review of such reports, it is difficult to ensure continued appropriation of access to critical information and establish accountability.

COSMO access #33 grants an individual the access to change a retiree's beneficiary and other related account maintenance information. We recommend SRB management revisit user access privileges granted to individuals to verify that access is commensurate with job function. Also, it is essential that management review audit trail reports on a regular basis to ensure that unauthorized users are not accessing the application thereby compromising the integrity and confidentiality of the data.

INFORMATION TECHNOLOGY DIVISION

Service Level Agreements with Agencies and End-Users

The Information Technology Division ("ITD") is responsible for the day-to-day administration, maintenance and upkeep of the servers of approximately 170 agencies that use the ITD data center. The Infrastructure Group does not have documented service level agreements ("SLA") with the agencies that ITD services. Although there is an SLA for Mass Mail, which includes all the agencies using this product, an SLA for the upkeep and maintenance of other servers does not exist. ITD's Common Help provides help-desk services to users from various agencies. Although detailed procedures exist for various problems types, a standardized Service Level Agreement with end-users has not been established.

Service level agreements are essential to outline users' responsibilities and to clearly define expectations. Informal agreements may result in complaints and user dissatisfaction and more importantly, where service levels have not been defined, there may not be a reliable basis for assessment of the quality of services rendered and no effective control in terms of responsibility, accountability, measurement, and feedback.

We recommend that ITD develop an SLA with the agencies it supports as well as the end-users it provides systems and application support to. The scope and the depth of these agreements will depend on the nature of the services provided. However, at a minimum, the SLAs should include information on the following:

- Purpose of the SLA;
- Parties included in the agreement;
- Details on definitions of key terminology used;
- Services/Software/Hardware Supported;
- Responsibilities and Priority Levels; and
- Escalation Charts.

Once developed, compliance with the SLA should be monitored. Any changes to the SLAs should be updated in the agreement.

DEPARTMENT OF REVENUE

Offsite Backup Storage Schedule

The Information Services Organization ("ISO") at the Department of Revenue ("DOR") has a defined backup schedule, according to which tapes are sent offsite Monday through Friday. Weekend backup tapes are maintained onsite and shipped out the following Monday. Given the number of transactions processed at the DOR in a given day, depending on when a disaster occurred, there is a potential risk that three days' data could be lost.

System backup is a critical component of an effective business and technology recovery plan. Regular off-site storage of data ensures that vital records are available in the event of an emergency. Storing backup tapes off-site helps ensure that if a disaster were to occur at the data processing site, backup data could be recovered from the offsite tape storage site.

DOR's critical business processes directly depend on the use of information and information systems technology to provide trusted and uninterrupted service to its customers, business partners, employees, and the citizens of the Commonwealth of Massachusetts. Thus, it is highly essential to maintain the availability and reliability of these information assets. A good retention and rotation strategy enables an organization to not only maintain the flexibility of their systems, but also gives them the reasonable assurance that they will be able to recover their systems in the event of a disaster. We recommend DOR revisit its existing backup rotation policy and consider increasing the frequency of shipping backup tapes offsite to a daily rotation schedule. This will ensure that in the event of damage or destruction of the facilities, DOR can retrieve data maintained offsite and perform a recovery of its systems.

Change Control Methodology

The DOR performs development in various application environments, residing on a variety of operating systems and network management platforms. The following observations were noted regarding the application and network change control process:

A standardized change control methodology across all applications and network environments does not exist. Within a standardized methodology a centralized database of project assignments, requirements, specifications, test plans and production plans would be maintained;

In most of the environments, programmers also have access to production. PVCS (version control software) reports to compare PVCS and production versions are only run weekly and they only include the Masstax and Oracle environments. In addition, there are no alarms to trigger notification of changes made to production; and

Issues noted during network change implementation or maintenance-related troubleshooting are not consistently logged. Some groups use Remedy application; others use spreadsheets for logging their problem tickets.

The DOR relies heavily on its systems to meet its operational, financial and information requirements. In the absence of certain internal controls, the design and acquisition of new systems and modifications to existing systems may not be adequately controlled. Lack of enforcing standardized systems' lifecycle development policies, which include focus on project management, development methodologies, testing effort, migration strategies and documentation can compromise the effectiveness of the DOR's systems.

To safeguard the integrity of production data, update access to the production environment should be very restrictive. Should a programmer choose to do so, he/she has the capability and the knowledge to create and approve an unauthorized change for movement into production. As a result, data integrity may be jeopardized.

The objective of a problem reporting system is to track problems and to ensure that they are resolved in a timely manner. In the absence of a centralized tool to report how problems were fixed or troubleshooting issues, management may not be able to learn about problem types, response times and resources required to support systems.

We recommend that the DOR develop a formal project lifecycle approach and a standardized methodology for systems development, implementation and maintenance for all application and network environments. The objective of a more consistent approach is to minimize the impact of change on core business groups as well as the Information Services Organization ("ISO") and to create more consistency and stability in daily production processing. At a minimum, the approach should address management's intentions related to changes performed, authorization and prioritization, project plans and metrics, testing and Quality Assurance, migration procedures and ongoing support. All system development teams performing application and network changes should follow a consistent approach with specific standard procedures. A significant component of the methodology should emphasize documentation especially since the DOR has certain highly customized products and applications.

DOR management should also reassess and evaluate its current change migration strategies. A clear separation between development/test and production should be in place. As a tactical approach, management should expand the use of PVCS version control software to include all application development environments. On a more strategic level, management should consider developing a workflow, so that all changes to the production environment are made through authorized channels only, and by a small number of individuals who do not have conflicting responsibilities (i.e. database development, program development, or security).

Finally, DOR management should consider the development of a centralized database to track implementation or troubleshooting issues. This will ultimately allow the ISO group to perform more effective problem analysis, monitor trends, serve as a knowledgebase of solutions and provide cost/time savings in the future.

Logical and Physical Security Procedures

ISO's Accounts Management Group is responsible for the granting and removal of logical access privileges to DOR employees and Inspectional Services Division ("ISD") is responsible for granting and removal of physical access privileges. Both Accounts Management and ISD are notified by the DOR's Human Resources Department ("HR"), regarding new hires, employee separations or transfers. The following observations were noted during the review:

- HR notification regarding terminations/transfers is sent out every two weeks, not when the change occurs;
- A termination checklist exists; however, it does not get filed with the individual's records;
- Inconsistent policies that new hires and seasonal employees are required to sign. Not all newly issued DOR polices are required to be signed off on and they are not maintained with the individual's records; and
- ISD does not perform proactive monitoring to identify those individuals that have not used their card over a certain period of time.

Lack of standard procedures to administer user access related to employee additions, changes and terminations increases the risk of unauthorized logical and physical access. Active administration of information systems security is important to ensure that security policies and procedures are consistently applied across the organization, especially during instances of employee turnover. Such policies and procedures are a vehicle to educate users about the value of information assets while the lack of standard procedures may contribute to higher levels of administration and overhead costs, inefficiencies and potential security exposures. Access paths are the logical routes of access to systems and data. In a multi-systems environment, such as that at the DOR, there are multiple access paths to data, for example, through operating system utilities, database facilities, and application software. It is essential to evaluate systems' access and physical access privileges granted to employees on a regular basis. In the event of employee separation, a termination checklist should be used as a tool to track all DOR property (security badges, laptops, etc.) to be acquired from the user. Absence of such a checklist makes it difficult to ensure that all separation-related requirements have been fulfilled.

We recommend that the DOR evaluate the effectiveness of its current procedures and enforce stricter policies to facilitate standardized security administration. HR should immediately notify the Account Management Group and ISD when an employee terminates or transfers so that the individual's access privileges can be changed accordingly. Proactively on a monthly basis, a comparison should be performed between the HR and User Accounts databases, to ensure that no changes have been missed. ISD management should perform a proactive check on physical access cards, to identify those individuals that have not used it for over 60-90 days.

In addition, HR management should mandate the completion of a Termination Checklist, upon the last day of employment. A copy of this checklist should be maintained with the terminated individual's records, so that concerned parties at DOR can follow up and recover all DOR equipment. We also recommend that the DOR ensure that its security policies and procedures are read and acknowledged by all employees (permanent or seasonal). This would help ensure that all employees are aware of the value of the DOR's and ultimately the Commonwealth of Massachusetts' information assets and their role in protecting them.

Computer Incident Response Policy

The DOR does not have a clearly defined set of procedures to handle security violations. ISD performs regular security monitoring and is responsible for follow-up in the event of an incident. Although certain informal procedures have evolved over time, a standardized set of incident response procedures or comprehensive checklists used to determine the steps that should be taken in the event of a security violation have not been developed and distributed to concerned parties.

Incident response procedures ensure that all security breaches are handled properly before serious damage can be done to systems. Without a clearly defined set of procedures to handle security violation incidents, there is a risk that security breaches may not be handled properly and serious damage may be caused to critical systems.

We recommend that DOR formulate and deploy a standardized set of incident response procedures that address all aspects of security violations from initial detection to resolution of the incident. A standardized set of incident procedures will ensure that, regardless of when the breach occurs or who is available to address the incident, it will be handled quickly and correctly before any damage can occur. At a minimum, incident response procedures should consist of four steps:

- Identification and categorization;
- Escalation and notification;
- Containment, eradication and recovery; and
- Post-incident follow-up.

Development of these procedures should be coupled with periodic training to ensure that all security personnel are prepared to handle an actual security violation in the event that it occurs, and that they know who to contact and how to resolve it.

At the Underground Storage Tank Division, Segregation of Duties Should be Improved

The Underground Storage Tank Division ("UST") of DOR runs the Underground Storage Tank Program, which assesses fees on delivery to, and use of, gasoline and diesel underground storage tanks. The following observations were noted regarding the controls at UST:

- The UST user, responsible for updating customer records in MMARS, has the ability to add a new customer, change an address, generate a new bill and increase/decrease a billing amount. There is no oversight or quality assurance process to ensure that receivable decreases or increases are valid;

- The billing and cash processing functions are not segregated in UST;

- All deletions have to be performed by the database administrator who also has access to the production environment where all changes are directly made. As such, the administrator has the ability to change/delete customer Ids, modify addresses, etc. Although a report exists which outlines all records changed or deleted, management does not review it. Besides, in a recent database corruption, all 'deletion audit trail' was deleted.

In the absence of effective segregation duties, there is a risk that assets could be misappropriated. In addition, in the absence of a clear separation between test and production, data integrity may be jeopardized.

We recommend that UST management develop a workflow to facilitate better segregation of duties. The functions associated with updating customer records and changing bills (generating new bills, performing receivable increases or decreases) should be appropriately segregated. In addition, management should reassess the division of the billing and cash processing functions. Two individuals are currently responsible for both billing and cash processing; management should consider dividing the responsibility, so that an individual is not responsible for processing cash related to the bills he/she generated. Management should also consider supplementing manual segregation through the use of system restrictions.

To safeguard the integrity of production data, update access to the production environment should be very restrictive. All changes to the UST database should be performed in a test environment, and individuals with non-conflicting responsibilities (e.g. database/application developer, security manager, etc.) should migrate the change to production. In addition, management should periodically review audit trail reports, to ensure that only appropriate changes are being made.

DEPARTMENT OF EDUCATION

One Documented System to Measure Supplement Not Supplant

The Department of Education ("Department") has developed procedures to review and monitor the supplement not supplant requirement for the three major federal programs included in the fiscal year 2002 Single Audit, however, it would be more effective and efficient if the Department implemented one documented Department-wide system to review and monitor the supplement not supplant requirement for all federally-funded programs. Three major federal programs included in the fiscal year 2002 Single Audit that had a supplement not supplant requirement were: Title I, Vocational Education and Class Size Reduction. In addition, there may be other federally-funded programs administered by the Department that have a supplement not supplant requirement. The supplement not supplant requirement requires the Department to ascertain if a Local Education Agency ("LEA") has used federal funds to provide services that were provided with non-federal funds in the prior year. In order to comply with this requirement, the Department must review each LEA's application for funding as well as year-end expenditures. While the administrators and directors for the three programs cited above have developed procedures to review and monitor the requirement at the LEAs to comply with federal regulations, each has done so independently.

We recommend that the Department determine all of its federally-funded programs that have a supplement not supplant requirement and work with the fiscal, school business services and program staff to implement one documented Department-wide system to ensure that this requirement is satisfied for all applicable programs.

OFFICE OF THE ATTORNEY GENERAL

Settled Yet Unpaid Legal Cases

The Office of the Attorney General ("AGO") is responsible for tracking and reporting on lawsuits pending or threatened against the Commonwealth. The Financial Reporting and Analysis Bureau ("FRAB") in the Office of the Comptroller ("OSC") has been working with AGO, along with the Commonwealth's auditors, to enhance the reporting information provided by AGO to FRAB for inclusion in the Commonwealth's financial statements.

A number of lawsuits, arising from the ordinary course of operations, are pending or threatened against the Commonwealth. For those cases in which a probable loss will be incurred and the amount of the potential judgment can be reasonably estimated, the AGO estimates the liability. The current portion of this liability is reported in the appropriate governmental funds and the long-term portion is recorded as a non-current liability in the Statement of Net Assets within the government-wide financial statements. This information is communicated to FRAB annually during the preparation of the Statutory Basis Financial Report and the Comprehensive Annual Financial Report. In addition, the AGO confirms the cases that were outstanding in the prior year but which have since been settled. The AGO, however, does not confirm the cases in which the Commonwealth has been successful..

AGO provides documentation to the Department Assistance Bureau ("DAB") of OSC of all cases settled with judgments against the Commonwealth. The DAB is then responsible for paying the settlement amount to the appropriate party.

AGO, DAB and FRAB should work together to develop roll-forward procedures and controls of all cases, including dismissed cases, on a quarterly or semi-annual basis.

DEPARTMENT OF PUBLIC HEALTH

Pre-Qualification Documents Are Not Maintained in an Efficient Manner

The Purchase of Service ("POS") bureau at the Department of Public Heath ("Department") is not maintaining subrecipient pre-qualifications documents in an orderly and efficient filing system. The POS bureau is responsible for the contracting and monitoring of contractors utilized by the Department. In this capacity, POS performs an annual Pre-Qualification process to ensure that the contractor meets the Commonwealth of Massachusetts contracting requirements. As a component of this process POS obtains various documents that should be maintained in the contractors folder. These documents can include:

- UFR reports
- Audited financial statements, including A-133 audit reports for entities receiving $300,000 or more in federal funding
- Communications between the Department's Procurement Office and the subrecipients.
- Corrective Action Plans

A review of the pre-qualification materials during the sub-recipient monitoring testing, indicated that some of the materials are not in the contractor's Pre-Qualification folder. Additionally, POS staff had a difficult time in locating some of the pre-qualification documents. Consequently, POS staff could not retrieve the information in an effective and efficient manner, due to the lack of consistency in the filing system.

POS should review the current pre-qualification filing system and make the changes necessary to develop a uniform file for each contractor to facilitate the collection and retrieval of documents. The new system should then be communicated to all POS staff through training and monitoring procedures to ensure proper implementation.

DEPARTMENT OF SOCIAL SERVICES

Standardization of the CORI Waiver

The Department of Social Services ("Department") is required to perform criminal background checks on all new hires, including individuals and families seeking to serve as family resources. In performing the background check, the Criminal Offense Record Information ("CORI") liaison, requests a CORI check on all household members age 14 years and older. If the CORI results in a finding, the individual is either disqualified or subjected to discretionary disqualification and reviewed on a case-by-case basis. If the individual has a category II or III record that is subject to a discretionary disqualification, the individual must obtain a written waiver in accordance with the Department's policies to be eligible to be a foster or pre-adoptive parent.

In performing a review of Title IV-E eligibility, waiver agreements from five area offices were obtained and reviewed. Each area office had a different waiver agreement. As a result, it was difficult to determine if each waiver agreement complied with Department policies and whether the waiver document had been properly approved.

We recommend that the Department standardize the waiver document for use by each of the area offices. Standardization of the document would provide for ease in determining compliance with Department policies, identifying key elements and proper authorization as well providing consistent training procedures.

THE MASSACHUSETTS TEACHERS' RETIREMENT BOARD

Need for Increased Controls Over Submission of Teachers' Retirement Data as Reported to the Teachers' Retirement Board

In order to accurately track teachers' retirements, the Teachers' Retirement Board ("TRB") collects data from every school district in the Commonwealth. Chapter 32 of the Massachusetts General Laws requires that the data must be submitted to the TRB within 10 days after the end of the month. This data includes demographic information (name, address, date of birth, etc.), information regarding the individual teachers' retirements (contribution rate, contribution amounts, date of hire, years of service, etc.), teachers' contribution information (percentage of salary withheld, total dollars withheld for the pay period, etc.) and the actual amount collected from employee contributions.

In the past, this information was difficult to obtain, because there was no common system for receiving this data. However, in 1997, the TRB developed a uniform reporting format, which is compatible with major commercial payroll-reporting software packages (such as ADP, Munis, etc.). The TRB also developed and provided a reporting software package, currently used by over eighty districts and charter schools. Every year, the TRB holds several regional employer training seminars for school payroll and business officials. The TRB staff also provide on-site training for newly hired school payroll officials and districts having reporting difficulties. Despite the efforts of TRB, certain school districts within the Commonwealth do not submit the data on a timely basis and TRB is required to pursue the data that is not provided by the school districts. When teachers within these districts are ready to retire the TRB is unable to process the retirement paperwork because the records are incomplete. This results in retired teachers not being able to receive their retirement benefits in a timely manner. In addition, when the districts do not submit retirement contributions on time, the teacher's overall benefits will suffer since the TRB is unable to earn investment income on contributions that they have not yet received. Moreover, several schools have not yet adopted compatible payroll software packages causing errors when TRB compiles information. TRB has controls in place to notify a change from previous periods so the errors are detected. However, as a result of the errors further delays are occuring while TRB corrects all errors.

Under Chapter 32, Section 18, Paragraph 1A, "If the Board.…determines that there has been an unreasonable delay in filing of any.…required information, the board, …shall so notify in writing such treasurer or other disbursing officer. If within thirty days thereafter, the board…has not received such required information, the board ….may petition the superior court to compel compliance with this section and enforce the penalty there under."

In order to remedy the current situation, the Board should continue to notify the members responsible for reporting the districts' information and remitting the appropriate contributions. If all else fails, the TRB should use the option of petitioning the superior court to enforce compliance.

The Board has submitted legislation that would require local school districts to submit monthly data and contributions on a more timely basis or be subject to an interest penalty.

COMPONENT UNITS

Submission of Financial Statements

Currently, the financial statements of the Commonwealth include 28 component units and 25 institutions of higher education. Each of these component units is subjected to an audit and is required to report its financial statements in accordance with GAAP. The OSC provided GAAP reporting requirements and guidelines and suggested a uniform set of accounting policies and financial statement disclosures to each component unit to ease the financial reporting process. The uniform information facilitates the inclusion of the component units into the Commonwealth's financial statements and helps ensure that similar acccounts across component units are grouped together properly.

OSC requires all institutions and component units to submit audited financial statements to them by October 15. This deadline is in place to ensure that all audited financial statements are ready for inclusion in the CAFR. Several of these entities, including the University of Massachusetts and Roxbury Community College, did not submit their final audited financial statements to OSC prior to deadline for completion of the CAFR audit.

The OSC should continue to hold group and individual meetings with the various entities to encourage an "ownership interest" in the Commonwealth's financial statements and to make them better understand their importance in the Commonwealth financial statements. Discussions should continue to focus on the disclosures needed in the entities' financial statements in order to meet their responsibility to comply with standards established by the Government Accounting Standards Board. The entities should include in their contracts with their independent audit firms the deadlines for their submission to OSC. But Serious consideration should be given to formalize in statute the need to submit audited financial statements in accordance with deadlines established by OSC.

* * * * * *