

VERMONT STATE AUDITOR'S REPORT ON STATE GOVERNMENT'S PROGRESS TOWARD YEAR 2000 PREPAREDNESS (Y2K COMPLIANCE)

FOR THE PERIOD ENDING NOVEMBER 1, 1998

EXECUTIVE SUMMARY

The State Auditor's Office (SAO) has conducted this review as a follow-up to its May 5, 1998 report concerning the State of Vermont's Y2K status. Our purpose was to assess the State's progress from April to November 1998.

Since our last report, an additional requirement of Y2K compliance has been placed on the State by the Governmental Accounting Standards Board (GASB): financial statements now should disclose material items concerning Y2K where omission would cause the financial statements to be misleading. An additional purpose of our review, therefore, was to assess the State's compliance with this new GASB requirement.

This review assessed the reliability of the Administration's estimates of state government's Y2K compliance and attempted to offer an objective measure of the State's progress toward full Y2K compliance over the period of seven months.

In May, we found that the State's Y2K project management and reporting structure were inadequate, which resulted in significant gaps in the response by individual offices. Contingency planning for Y2K was inadequate and misunderstood. Cost estimates for the work remaining to achieve Y2K compliance or a contingent alternative had not been developed.

For the current review period, our findings and recommendations are as follows:

FINDING A.1. Vermont's CIO has done significant work in establishing centralized Y2K project management.

Under the direction of the Chief Information Officer (CIO), good communication and networking has been established

throughout state government since April and the State has made significant strides in addressing the Y2K problem.

RECOMENDATION A.1. None.

FINDING B.1. A significant portion of state government has not reported on Y2K preparedness status. Therefore, the CIO lacks information and control over the State's total Y2K efforts.

RECOMMENDATION B.1. All of state government should report monthly on Y2K status to the CIO.

FINDING B.2. The CIO does not have a comprehensive control list or diagram of the State's information technology systems.

If reporting entities omit components from their Y2K reporting, the CIO does not have a template against which to confirm that assessments have been completed for all state systems. Without an IT architecture diagram, the State runs the risk that, even if all mission-critical State systems are checked, these systems could be endangered by smaller IT components that have not been checked, or through linkages with the State's external electronic partners.

RECOMMENDATION B.2. The CIO should develop a comprehensive State IT architecture diagram to ensure that all IT systems and linkages have been checked for Y2K compliance.

FINDING B.3. There is no independent evaluation or verification of the information in the monthly Y2K status reports submitted to the CIO, nor has the CIO engaged in any independent assessment of time and resource budgets developed by individual offices for Y2K compliance projects to determine if these budgets are appropriate.

Under the current reporting method, offices report on their expected hourly budget for all Y2K compliance activities and then report how many hours they have expended each month against that total budget. We note several apparent anomalies revealed by recent self-reporting that we feel reinforce the need for independent inquiry.

RECOMMENDATION B.3. The CIO should engage in independent verification of the information contained in the monthly Y2K status reports submitted by state offices. A review should be accomplished without delay, since time and resources may be in critically short supply.

FINDING B.4. Contingency planning for possible Y2K failures should be increased considerably.

RECOMMENDATION B.4. The CIO should direct all offices to complete contingency plans for mission-critical systems as soon as possible. The CIO should offer parameters for planning and, to the extent possible, review individual plans, particularly for certain key offices.

FINDING B.5. A complete and accurate estimate of the costs for agencies to reach Y2K compliance and for emergency budgeting for Y2K failures has not been prepared, consistent with the purposes set out by the Government Accounting Standards Board (GASB). As a result, Vermonters have no assurance that adequate resources have been made available to deal with Y2K. They also cannot know whether adequate provision has been made to cover those needs from which resources have been diverted to achieve Y2K compliance, or may be diverted in the future to deal with Y2K failures.

The new GASB standards require the State to disclose significant commitments of resources to Y2K compliance. A recent report indicates that Vermont is one of only five states failing to identify such costs.

RECOMMENDATION B.5. Consistent with the purposes of GASB Technical Bulletin 98-1, the State should accurately report the significant costs of Y2K compliance, beginning with FY1998. For FY1999 and FY2000, these estimates should be prepared for Legislative consideration in the context of the FY1999 supplemental budget and the FY2000 budget.

PURPOSE

The State Auditor's Office (SAO) has conducted this review as a follow-up to its May 5, 1998 report (for the period ending April 1, 1998) concerning the State of Vermont's preparedness for and response to the Year 2000 computer date issue (Y2K). Our purpose was to assess the State's progress over the seven months from April through October 1998.

Since our last report, an additional requirement of Y2K compliance has been placed on the State by the Governmental Accounting Standards Board (GASB) Technical Bulletin (TB) No. 98-1 (Disclosures About Year 2000 Issues) [see Appendix 1]. TB No. 98-1 says that the notes to the State's (and other public entities') financial statements should disclose material items concerning the Y2K compliance of the State's internal computer systems and other electronic equipment where omission would cause the financial statements to be misleading. This disclosure must be included in the State's audited comprehensive annual financial report (CAFR) for the years ended June 30, 1998 and June 30, 1999. It must include a general description of the State's Year 2000 readiness and an estimate of significant resources devoted to making computer systems and other electronic equipment Year 2000 compliant. An additional purpose of our review, therefore, was to assess the State's compliance with this new GASB requirement.

SCOPE

This review assessed the reliability of the Chief Information Officer's (CIO) estimate of all state agencies', departments', and offices' Y2K project status and project plans for attaining Y2K compliance. Additionally, this review attempted to offer an objective measure of the State's progress toward full Y2K compliance over the past seven months.

AUTHORITY

This review was conducted pursuant to the State Auditor's authority contained in 32 V.S.A. §§ 163 and 167.

METHODOLOGY

This review was conducted from August through December 1998 and covered the period from April 1, 1998 to November 1, 1998.

Our methodology included:

- Review of Executive Order 11-98, dealing with Y2K remediation efforts, September 18, 1998 [see Appendix 2].
- Interviews with the Secretary of Administration, CIO and assistant CIO.
- Review of the CIO's *[Y2K] Best Practices and Standards Handbook*.
- Attendance at the CIO's monthly Y2K workshops.
- Review of the Y2K Project Plans and Status Reports submitted to the CIO for the months of July, August, and September 1998.
- Review of the Agency of Administration's Y2K Status Reports and Action Plans, September 28, 1998 [see example, Appendix 3].
- Review of selected Web sites focusing on Y2K standards and experiences.
- Review of various General Accounting Office (GAO) guides and reports [see Appendix 4] (the CIO has adopted GAO's format for addressing Y2K in state government).

Consistent with our first review, this follow-up review has primarily focused on the efforts of the office of the CIO, including its assessment and monitoring of the State's overall Y2K compliance. The office of the CIO remains directly charged with ensuring Y2K compliance throughout state government. Its management of the State's Y2K efforts remains critical to the State's success or failure in meeting compliance goals.

The CIO reports directly to the Secretary of Administration. The CIO's Y2K responsibilities include:

- Directing Y2K efforts throughout state government to ensure consistent and timely compliance efforts;
- Providing support to each department (and each manager), through:
 - Implementation of Y2K processes and standards,
 - Provision of specialized contracts and legal support,
 - Creation and maintenance of a Web site which includes Y2K reporting tools and vendor compliance information,
 - Provision of contingency planning guidance,
 - Assistance with special projects;

- Centralized tracking of Y2K progress;
- Reporting progress to the Secretary of Administration, Legislature and other external audiences;
- Acting as spokesperson regarding Y2K efforts for the State of Vermont.

BACKGROUND

MAY 5, 1998 REPORT (FOR THE PERIOD ENDING APRIL 1, 1998):

The State Auditor's Office (SAO) completed a review of Vermont state government's preparedness for the Year 2000 computer date issue (Y2K) as of April 1, 1998 (report released on May 5, 1998). This initial review found that:

- **Project management of Y2K was inadequate.** The entire Y2K process was decentralized with individual agencies/departments/offices left largely on their own to cope with Y2K issues. Further, it appeared that the Chief Information Officer (CIO) had adopted a "hands-off" policy, suggesting that offices were going to proceed with little centralized assistance. The SAO felt this had led to a delay in effectively assessing Vermont's Y2K status and that it failed to encourage agencies/departments/offices to work jointly to minimize state business disruptions that could be caused by Y2K failures.
- **The State's reporting structure regarding its Y2K compliance status was inadequate.** We found that there was no system or requirement for regular and periodic reporting by all state offices to the CIO sufficient to establish the State's overall status; nor was there any reporting mechanism sufficient to establish an opinion of individual state offices' progress in reaching Y2K compliance.
- **Because of inadequate centralized leadership, there were significant gaps in the response by individual offices.** Offices without strong Information Technology (IT) staff and resources were clearly lagging behind in their awareness of Y2K issues and therefore were also behind in their responses. Further, without clear standards to guide state agencies in achieving an acceptable level of compliance, there was no clear benchmark against which individual offices could measure the efficacy of their compliance efforts.
- **Contingency planning for Y2K was inadequate and misunderstood.** We found that very few state offices had formal contingency plans and that no senior state government manager had either required verification or reviewed the contingency plans for adequacy or adherence with best practices.
- **There was no monitoring of State systems and equipment that could be adversely affected by non-compliant computer chips embedded in infrastructure.**

- **Cost estimates for the work remaining to achieve Y2K compliance or a contingent alternative had not been developed.** As a result, it was not clear whether current budgets would be sufficient to meet the Y2K challenge or whether emergency budgets would be required.
- **At least two key state agencies, Department of Motor Vehicles and Department of Buildings & General Services, appeared to be in serious danger of not reaching Y2K compliance.** We also noted concern about the progress of other departments and agencies.

FINDINGS AND RECOMMENDATIONS

A. STATE ACTION SINCE OUR MAY 5 REPORT FOR THE PERIOD ENDING APRIL 1, 1998

The State Auditor's Office found that Vermont state government has made significant strides in addressing the Y2K problem since our first review. The CIO has developed good communication and networking throughout state government, produced a handbook of best practices to assist remediation efforts, and required regular reporting throughout the Administration.

FINDING A.1. Vermont's CIO has done significant work in establishing centralized Y2K project management.

These actions, bolstered by the Executive Order mandating Y2K compliance by all State offices, include the following:

1. The assistant CIO, as Vermont state government's Year 2000 Coordinator, has been actively managing Y2K efforts.
2. Monthly Y2K workshops were established and met in July, August, September and October.
3. A best practices and standards handbook for Y2K has been produced and distributed to all relevant offices.
4. An on-line list service has been established for state managers to share questions and exchange ideas on a daily basis.
5. Monthly Y2K planning and status reports have been required to be submitted to the CIO.
6. A Y2K Status Report and Action Plan for all participating agencies, departments and offices was distributed by the Agency of Administration on September 28, 1998, informing participants of their overall progress toward Y2K compliance.
7. Focus groups for users of specific operating systems and applications have been formed.

RECOMENDATION A.1. None.

B. SEVERAL AREAS THAT STILL REQUIRE SIGNIFICANT ATTENTION

Completeness and Reliability of Reporting

Although we note significant progress in the State's Y2K efforts in our first finding, we remain concerned that the State lacks controls to assure the complete and reliable reporting necessary to determine whether offices have the financial, personnel or time resources necessary to meet Y2K deadlines. Our next three findings deal with the possibility that the State's efforts will miss critical Y2K areas since current monitoring efforts are not comprehensive and do not include independent verification.

Need for Contingency Planning and Disclosure of Costs

Our remaining findings deal with shortcomings we perceive in management of the Y2K issue at the individual office level. Overall, we remain concerned that the State's approach is largely "IT-driven." Although the actual remediation of Y2K problems is certainly an information technology (IT) issue, Y2K compliance is ultimately a business issue, since it affects the basic operations of every state office. Y2K failures could impact the basic missions of state government, such as the distribution of welfare benefits or the receipt of taxes. Y2K compliance demands the full attention of all agency heads and policy makers.

It is important to realize that some Y2K failures are likely in spite of the best Y2K efforts by the State (and other public and private entities). On October 7, 1998, the research director of the Gartner Group, a well-respected IT research organization, issued an assessment of the nation's readiness in testimony before the U.S. Senate Special Committee on the Year 2000 Technology Problem. In that testimony, Gartner predicts that 30 to 50 percent of all enterprises will experience at least one mission-critical system failure through March 30, 2000. Fifteen percent of state governments, according to Gartner, will experience such a failure and 10 percent of these failures will last three days or longer. In an October 11, 1998 *New York Times* article, the Gartner Group released its latest report tracking Y2K readiness. It found that:

- Operations failures will occur in about half of all government agencies and mid-sized businesses and in about 10-20 percent of larger businesses;
- The least Y2K-compliant entities are education, health care, government, farming, and local services.

As the General Accounting Office (GAO) says: "Despite the efforts of each business, state and local government, and federal agency to race against time and to renovate, validate and implement their mission-critical information systems, every organization remains vulnerable to the disruption of its business processes. Because most [government] organizations are highly dependent on information technology to carry out the business, Year 2000-induced failures of one or more mission-critical systems may

have a severe impact on their ability to deliver critical services." **In the face of this significant risk, we are emphasizing the need for contingency planning and a more complete accounting of all Y2K project costs by state managers.**

We believe that the State needs to budget more time and resources to fully test all of the State's interconnected and interdependent business functions and needs to act now to anticipate failures and prepare contingency plans, well before January 1, 2000. Further, state managers must fully disclose all Y2K compliance costs as well as anticipate unexpected costs due to Y2K failures.

FINDING B.1. A significant portion of state government has not reported on Y2K preparedness status. Therefore, the CIO lacks information and control over the State's total Y2K efforts.

At the end of the review period, the following boards, councils and commissions had not reported their Y2K status to the CIO:

1. Enhanced 9-1-1 Board
2. Criminal Justice Training Council
3. Fire Service Training Council
4. Governor's Commission on Women
5. Human Rights Commission
6. State Labor Relations Board
7. Board of Medical Practice
8. Racing Commission
9. Vermont Center for Geographic Information
10. Vermont Veterans' Home

In addition, the Judicial and Legislative branches of state government have not reported their Y2K status to the CIO. Although all state entities have been invited to join the CIO's Y2K monthly meetings, none is required to participate. Since attendance varies, many state offices are in danger of not being adequately informed about Y2K compliance requirements.

RECOMMENDATION B.1. All of state government should report monthly on Y2K status to the CIO.

FINDING B.2. The CIO does not have a comprehensive control list or diagram of the State's information technology systems.

Although Vermont state government is small, its IT structure is complex. The State's relatively decentralized offices tend to build their IT systems independently, but many of these systems are interconnected. Even stand-alone desktop computers can be used to create information that is uploaded to a server. Since the transfer of Y2K-related

problems is possible in some transfers of data from one unit to another, all IT resources must be identified and assessed.

Additionally, and perhaps more significantly, the **interfaces between state entities and business partners, such as federal and local governments, may remain unidentified** if agencies concentrate only on assuring the preparedness of their internal systems. A disruption of the flow of information from local agencies through state government to the federal level may interrupt the flow of resources or funding back down from the federal level to state or local recipients. Vermont is not alone in delaying the assessment of interchanges. The GAO reported on July 1, 1998 that only two of 39 reporting states had finished assessing their data exchanges. (Vermont state government's first inventory of its data exchanges was not undertaken until late 1997 in response to this GAO survey.) The GAO concluded that "unless Federal agencies take action to reach data format agreements with their data exchange partners and deal with data exchanges that will not be Year 2000 compliant, some agencies' mission-critical systems may not be able to function properly." The significance of this GAO finding for Vermont is not only that some federal agencies' mission-critical systems may not function properly, but also that Vermont may have to rely on its own contingency plans if these vital federal services are not available.

Clearly, any comprehensive Y2K compliance monitoring effort must ensure that every electronic partner link within and without state government is checked. A basic management tool for such a check would be a diagram (or flow chart) of the State's IT architecture. Currently, the CIO does not have such a tool. If reporting entities omit systems from their Y2K reporting, the CIO does not have a template against which to confirm that assessments have been completed for all state systems.

The Federal Financial Institutions Examination Council (FFIEC), a federal agency that audits Y2K efforts for the Federal Deposit Insurance Corporation, stresses that without a tool such as a control diagram or a flow chart, any part of a business system may remain hidden and unaddressed. Failure of a hidden component, it notes, could cripple an entire system. **Without an IT architecture diagram, the State runs the risk that, even if all mission-critical State systems are checked, these systems could be endangered by smaller IT components that have not been checked, or through linkages with the State's external electronic partners.**

RECOMMENDATION B.2. The CIO should develop a comprehensive State IT architecture diagram to ensure that all IT systems and linkages have been checked for Y2K compliance.

FINDING B.3. There is no independent evaluation or verification of the information in the monthly Y2K status reports submitted to the CIO, nor has the CIO engaged in any independent assessment of time and resource budgets developed by

individual offices for Y2K compliance projects to determine if these budgets are appropriate.

The CIO has not engaged in any kind of independent assessment of the adequacy of each office's Y2K compliance project. Instead, the CIO relies on individual offices to report their Y2K status and progress toward compliance. The obvious weakness of the State's current self-reporting model is that offices have no incentive to advertise their Y2K compliance deficiencies. For example, current status reporting measures only how far along an office is in relation to its own internal hourly budget. That approach does not necessarily measure true progress toward Y2K compliance.

This current reporting method tends to emphasize form over substance. Offices report on their expected hourly budget for all Y2K compliance activities and then report how many hours they have expended each month against that total budget. Thus, **offices that may have underbudgeted for time (and personnel) are rewarded under the current reporting scheme**, since they are more likely to appear to be on schedule (because they need to spend fewer hours in order to meet their budget). **Conversely, offices that may be conservative in their estimation (e.g., allowing extra time for testing and implementation) will be more likely to appear to be behind schedule.** There is an obvious built-in incentive under the present reporting scheme for offices to underestimate the scope of their Y2K compliance problems, and since the CIO has not assessed these plans, such underestimation could easily go undetected. There is also obvious incentive for offices to overstate their effort, which also could easily go undetected.

Some kind of independent inquiry by the CIO, even if on a spot-check basis, would lead to greater assurance that offices are accurately reporting their Y2K status, including potential risk for failure. We note several apparent anomalies revealed by recent self-reporting that we feel reinforce the need for independent inquiry:

- Our May review classified the Department of Buildings and General Services as "high risk" due to insufficient progress in the inventory of statewide infrastructure, including all buildings owned or leased by the State. However, the Secretary of Administration's September Status Report (based on self-reporting to the CIO) indicates that this department is now one of the best prepared in state government, 208 hours ahead of its Y2K time schedule. It would appear that, if correct, Buildings and General Services reported that it had surveyed more than 1,000 state buildings in less than six months time. Although we have no information that casts doubt upon the accuracy of this reporting, such an extraordinary effort seems worthy of some kind of independent verification.
- For all of the State's Y2K projects, offices reported that they had expended more than 34,000 hours as of September 10, 1998. The time period covered by this report was at least 10 months, suggesting an average monthly effort of 3,400 hours or less. However, offices reported that from September 10 to October 9, they expended more than 14,000 hours, suggesting that efforts had increased more

than four-fold in one month. An increase of this magnitude deserves further scrutiny.

Independent verification of Y2K status is widely accepted as a fundamental requirement of Y2K project management. FFIEC's Year 2000 audit, for example, includes a specific inquiry about the independent evaluation of Y2K project status. FFIEC believes that the reliability of the reporting will be suspect unless some periodic, random review is performed either by a group of employees or an independent contractor with the knowledge and skills to understand and effectively assess the departmental management's efforts.

If assurances are not obtained that Y2K status reports and project plans are materially reliable, then decisions made by the State's executive management, based on status report data (such as criticality, achievability, and cost) may be faulty. Since time and resources are so limited in Vermont's Y2K project, incorrect or misleading information by a single agency could result in significant problems for a much larger segment of state government.

RECOMMENDATION B.3. The CIO should engage in independent verification of the information contained in the monthly Y2K status reports submitted by state offices. A review should be accomplished without delay, since time and resources may be in critically short supply.

FINDING B.4. Contingency planning for possible Y2K failures should be increased considerably.

As of September 1998, when the Secretary of Administration aggregated Y2K progress reports from individual offices, contingency plans were in place for only 28 (9 percent) of the 308 mission-critical systems identified by the 41 responding offices. This would suggest the development and testing of contingency plans has not been a priority. The State's own deadline for full Y2K compliance is June 30, 1999; with little time remaining, it is simply not best practices management for 91 percent of the identified mission-critical systems to be without contingency planning.

Contingency planning may sound like an emergency measure, but it is actually prudent preparation for the distinct possibility of Y2K failures. In addition to experts such as Gartner, who are predicting some inevitable failures in mission-critical systems, other states are emphasizing the need for contingency planning. According to the August-September 1998 newsletter issued by the Minnesota Y2K Project Office: "In spite of our best efforts, the risk of failure due to the 'millennium bug' will increase greatly over the next [15] months. In fact, given the size and scope of the State's information resources and firmware, there is a strong likelihood that some failures will occur."

The following statistics from the Secretary of Administration's September Year 2000 Status Reports to state government offices indicate that contingency planning should be emphasized as soon as possible.

1. **The State's Y2K projects are significantly behind schedule.** According to the Secretary's September 28 status reports, Y2K remediation projects in all departments were scheduled to have been 50 percent completed. In fact, the reports indicated that, on average, departments' projects were only 33 percent completed.
2. **Twenty-five offices were a total of 7,555 hours behind in meeting their estimated Y2K project time.** The offices that were furthest behind were the Department of Motor Vehicles (1,075 hours), the Department of Environmental Conservation (839 hours), the Department of Public Safety (821 hours), the Treasurer's Office (773 hours), the Department of Health (687 hours), the Lottery Commission (512 hours), and the Department of Personnel (454 hours). In addition to making up this deficit, each of these offices also were to spend their previously budgeted Y2K time each month going forward. There is no measure of whether these offices have sufficient resources to accomplish this.
3. **Statewide, offices must complete 3,692 hours of Y2K work each month to stay on schedule. For some departments, this may amount to a significant commitment of resources, amounting to the equivalent of several full-time employees taken away from other duties.** For example, the Tax Department has budgeted 792 hours monthly; the Agency of Transportation, 469 hours; Social Welfare, 408 hours; Buildings and General Services, 346 hours; Motor Vehicles, 270 hours; and Health, 195 hours. By any measure, this represents a serious diversion of staff resources from core tasks to Y2K compliance activities. Should any of these departments be unable to meet these ambitious schedules, Y2K failures may be more likely.
4. **State offices may be underbudgeting for Y2K testing.** Minnesota, Pennsylvania, and Washington state Y2K Web sites report that testing should comprise 20 to 50 percent of the Y2K project. Experts such as Gartner suggest that 30 to 40 percent of project time should be devoted to testing. However, Vermont state offices' Project Status Reports for September 1998 show that they have budgeted only 15,582 hours (or 20 percent) of 77,500 total Y2K project hours for testing and validation. Insufficient testing may increase the Y2K risks.

Since there often is confusion about what a contingency plan should include, it is important that the CIO issue parameters concerning contingency planning. Some experts suggest that Y2K contingency plans should resemble emergency plans (e.g., what do to in a power failure); others suggest simply focusing on replacing the functions of mission-critical computing systems.

In any event, best practices suggest that all contingency plans should focus on how an office would continue to fulfill its primary business functions and its primary mission in the event of Y2K failure. Whether that primary function or mission is issuing payroll checks, processing tax returns or ensuring environmental quality, plans should be in place to enable offices to carry on their primary missions without interruption in the event of computer failure. Conceivably, this may involve reverting to manual systems and processes for some period of time.

RECOMMENDATION B.4. The CIO should direct all offices to complete contingency plans for mission-critical systems as soon as possible. The CIO should offer parameters for planning and, to the extent possible, review individual plans, particularly for certain key offices.

FINDING B.5. A complete and accurate estimate of the costs for agencies to reach Y2K compliance and for emergency budgeting for Y2K failures has not been prepared, consistent with the purposes set out by the Government Accounting Standards Board (GASB). As a result, Vermonters have no assurance that adequate resources have been made available to deal with Y2K. They also cannot know whether adequate provision has been made to cover those needs from which resources have been diverted to achieve Y2K compliance, or may be diverted in the future to deal with Y2K failures.

As described in the beginning of this report, GASB issued Technical Bulletin No. 98-1 (Disclosures About Year 2000 Issues) in October 1998 [see Appendix 1]. It is effective for audited financial statements dated after October 31, 1998. The new GASB standards require the State to disclose significant commitments of resources to Y2K compliance, the objective being to enhance public assessment of "the level of services that can be provided by the government and its ability to meet its obligations as they become due."

To date, Vermont has not assembled or reported a comprehensive estimate relating to the cost of Y2K remediation. For example, in the Five-Year Technology Plan issued by the CIO in February 1998, agencies reported \$47,269,730 worth of IT budgeting for FY1999. Of this amount, only \$825,000 (1.7 percent) was earmarked for Y2K projects and only six agencies included Y2K work as a budgeted item.

In responding to our May review, the CIO contended that there was no need for separate Y2K budgeting since most offices had worked Y2K remediation costs into existing IT budgets. We disagree. A recent report by the National Association of State Information Resource Executives indicates that Vermont is one of only five states failing to identify such costs.

As recently as the September monthly Y2K meeting, the representative of the Office of Communications & Information Technology asked what the CIO could do to assist agencies in procuring funding for additional services and equipment in order to reach

Y2K compliance by June 30, 1999. Statements such as this would suggest unbudgeted Y2K needs. Further, as we noted above, one of the serious constraints Vermont faces may be related to adequate personnel resources. As experienced state managers know, devoting significant amounts of personnel to unscheduled projects may result either in unexpected overtime costs or failure to fulfill all mandated activities. In either scenario, acquiring the necessary personnel resources to fully comply with Y2K remediation requirements will impact budgets of individual offices.

It is essential, therefore, that offices estimate fully and disclose all Y2K costs, from IT hardware and software to personnel resources. The time frame is critically brief. **If any office requires supplemental funding, policy makers, including the Legislature, should be informed as quickly as possible.**

RECOMMENDATION B.5. Consistent with the purposes of GASB Technical Bulletin 98-1, the State should accurately report the significant costs of Y2K compliance, beginning with FY1998. For FY1999 and FY2000, these estimates should be prepared for Legislative consideration in the context of the FY1999 supplemental budget and the FY2000 budget.