STATE AUDITOR'S REPORT ON VERMONT'S YEAR 2000 PREPAREDNESS

FOR THE PERIOD ENDING APRIL 1, 1998

- - - -

EXECUTIVE SUMMARY

BACKGROUND

Many of Vermont's computing systems and operating systems that use embedded computer chips are at risk for failure because of a wide-spread inability of many of them to process dates beyond the Year 2000. Ensuring that computers and chips can recognize and process dates beyond the Year 2000 -- or be "Year 2000 compliant" -- has become a critical management issue in both the public and private sector. Vermont's Year 2000 compliance implicates every aspect of its financial operations, every aspect of quality and internal controls, and every aspect of state services relied upon by Vermonters.

Awareness of the necessity of Year 2000 compliance and public sector response has been rapidly growing. In January, for example, President Clinton appointed John Koskinen to head the President's Council on Year 2000 Conversion and direct all federal compliance activities. Since January 1997, the federal Office of Management and Budget has also been monitoring federal compliance efforts at the federal department level. At the state level, most states have well-established Year 2000 compliance efforts under way. Meanwhile, the General Accounting Office has recently urged our office to monitor and communicate information regarding Vermont's Year 2000 compliance. Additionally, within recent months a number of state auditors have issued formal reports concerning Year 2000 compliance progress in their respective states.

The State Auditor's Office conducted a review of the state's response to the Year 2000 (Y2K) computer date issue and has assessed the status of Vermont's efforts to-date to ensure that all state systems reach Year 2000 compliance. Our review has focused particularly on the leadership and efforts of the Chief Information Officer (CIO), because the CIO is responsible for Vermont's Information Technology (IT) policies.

Year 2000 Compliance is a Project Management, not an Information Technology issue.

Our review has emphasized that despite its technological roots, Year 2000 compliance is a project management problem, a view widely held throughout the public sector. Our review has found that best practices for project management have been adopted by most of the public sector in responding to Year 2000 compliance. Most states have also delegated responsibility for Year 2000 compliance to a central office and delegated to it broad responsibilities and authority to ensure state-wide compliance. Contrary to this accepted practice, our review has found Vermont has a decentralized response to Y2K compliance and that this decentralized approach results in serious risk to the State's overall Y2K compliance efforts. Particularly because of inadequate centralized monitoring of progress towards full compliance, we have found State agencies have disparate levels of awareness and ability to cope with this problem. Yet the State does not appear to be providing sufficient leadership, guidance or assistance to ensure all State offices will be compliant.

Vermont Faces Serious Risks if it is not Year 2000 Compliant

Year 2000 noncompliance is, in our view, not an option for state government. Noncompliance and the resulting disruption of state services could result in annoying consequences to users of state services, such as delayed tax refunds, or it could have potentially serious consequences, such as tens of thousands of Vermonters unable to receive food stamps or heat assistance. Similarly, failures of embedded chips could be relatively minor -- perhaps an elevator might not work -- or at the extreme, they could approach catastrophic -- perhaps a dam could release water at an inappropriate time and cause a flood.

Potential Problems for the State in Becoming Year 2000 Compliant

Vermont faces a risk that critical portions of its Year 2000 compliance efforts may fail. Aside from the short time remaining, the state faces these challenges:

- Determining the extent of the Y2K problem: Our review has found some offices have yet to undertake an inventory of affected systems and even for those that have, finding all the possible places where a date field may reside is a difficult challenge.
- Shortage of skilled personnel: Qualified IT personnel to assess and work on Y2K issues are already scarce and will only become more so.
- Rising costs: There is a shortage of Y2K consultants, qualified programmers and IT personnel; costs for compliance related-work is literally going up daily. Those state offices that have not already secured Y2K compliance services may find they are far more expensive than anticipated.
- Failure to meet project deadlines: The national average for large scale computing projects being on-time and within-budget is less than 20%.

Response of the CIO and State Auditor Follow-Up

The CIO has indicated that by and large she feels the State's approach and progress towards Y2K compliance is adequate. However, the State Auditor feels there remain serious risks to the State inherent in Y2K non-compliance and that significant portions of the State are at risk for non-compliance. Therefore, it is the intention of the State Auditor to follow-up this report with future reports on the State's progress towards Y2K compliance.

HIGHLIGHTS OF FINDINGS AND RECOMMENDATIONS

1. FINDING: Project management for state-wide Year 2000 compliance efforts is inadequate. Vermont currently has a "hands off" approach to management of Y2K for compliance by individual state agencies and departments.

Responsibility for recognizing and addressing Y2K problems has been entirely delegated to individual agencies, which are expected to assess, plan and implement Y2K solutions on their own. As a result, some state offices are lagging far behind in Y2K compliance. Therefore, we believe that Vermont's decentralized approach to Y2K compliance may result in disruption of some state services, unless appropriate remedial steps are taken. We have noted in our review that the State of Virginia, tried and abandoned as unworkable a similar decentralized approach to Y2K compliance.

RECOMMENDATION: The Governor should mandate that all state offices be Year 2000 compliant by June 30, 1999 and that the CIO or some other state-level office should be clearly designated to direct all state government Y2K activities.

2. FINDING: The present reporting system for progress towards Y2K compliance is inadequate. As a result, the CIO does not have a realistic assessment of the State's status or progress toward Y2K compliance.

Beyond verbal assurances from some state offices that certain "mission critical systems" have been assessed and will be Y2K compliant by 1999, the CIO currently receives no detailed, regular reports concerning Y2K compliance from state offices. Verbal assurance of progress is insufficient accountability. Regular reports on Y2K activities are needed to ensure that all state offices are aware of the Y2K problem and are on track with compliance projects.

RECOMMENDATION: A regular and rigorous Y2K status report of all state agencies and offices should be implemented immediately.

3. FINDING: To date, there is no state-wide monitoring of state systems and equipment with embedded chips.

Failure of embedded chips could cause serious problems for the State. The issue faces every state office. Currently, however the CIO has no authority over the issue and the response by State Buildings, which potentially has the largest number, is inadequate.

RECOMMENDATION: The Y2K office should direct every state office to undertake a thorough review of Y2K compliance of systems and computers with embedded chips.

4. FINDING: Individual offices have not separately reported Y2K compliance costs to the Legislature. In some cases, they do not know likely costs associated with Y2K activities. As a result the state could face significant unforeseen compliance costs in upcoming budgets.

A significant weakness of the state's current Information and Technology Five-Year Plan is that state offices have not been required to report planned Y2K-related expenditures. As a result, some state offices have likely neglected to budget (and plan) for Y2K activities. Although it is impossible for us to estimate future costs, it is clear that the state faces significant expenditures in the near-term for Y2K compliance activities. For example, DMV does not yet know the extent of its task of bringing 11 mission critical systems into compliance. Other offices which have not undertaken adequate inventory, assessment or planning activities will almost certainly face unexpected Y2K compliance-related costs. We believe that state offices should estimate costs for unbudgeted Y2K compliance as soon as possible.

RECOMMENDATION: All state offices should complete an assessment of expected Y2K costs as soon as possible and report them to the Governor and the Legislature, so that the State can react appropriately.

5. FINDING: When compared to other public entities, our survey suggests that Vermont lags behind in addressing the Y2K problem. There is reason to believe that key offices, including DMV and State Buildings, will not be Year 2000 compliant in time.

When compared to other public entities, overall, indicators suggest that Vermont lags behind in key Y2K compliance activities. In particular, DMV and State Buildings are at serious risk for noncompliance, unless appropriate remedial steps are taken.

RECOMMENDATION: The Y2K office should identify and assist those state offices that are most in need of assistance in order to achieve compliance.

PURPOSE

The State Auditor's Office has conducted a review of the state's response to the Year 2000 (Y2K) computer date issue. The purpose of this review was to assess the State's internal controls and compliance over Year 2000 compliance, which is itself crucial to the effective state operations and to the State's government-wide internal controls. Year 2000 compliance implicates every aspect of Vermont's financial operations and every aspect of state services relied upon by Vermonters.

We have reviewed the State's overall awareness and preparations to ensure that its computing systems and computer chip-dependent equipment are compliant. This review assessed the State's progress towards ensuring that all state computer systems will be Year 2000 compliant on time. This review has also attempted to assess systems that are at risk for non-compliance. An additional purpose of this review was to assess how

Vermont is faring when compared to other public sector entities that are also preparing for the Year 2000 computer date issue.

A primary purpose of our review was to assess the awareness and preparedness of the State's Chief Information Officer (CIO) with regards to Year 2000 compliance. The CIO is responsible for the State's overall strategic decision making concerning information technology and therefore has the lead role in the State's response to the Year 2000 (Y2K) computer date issue. In particular, our review has focused on internal controls and compliance by the CIO with regard to her responsibilities as outlined in 3 V.S.A. §§ 2222(a)(9) and (10), delegating responsibility to the CIO for planning the State's short-term and long-term information technology strategy.

This review was conducted as part of the Internal Controls segment of the State Auditor's annual General Purpose Financial Statements Audit, and has applied internal control standards contained in the Statement on Auditing Standards No. 78. It should be noted that since computing technologies are an integral part of the State's financial reporting mechanism, internal controls over these, including Year 2000 compliance, are critical to the well-being of the State.

SCOPE

This assessment included a review of Year 2000 awareness and preparedness by the office of the Chief Information Officer (CIO) as well as a review of awareness and preparedness at selected key state offices.

AUTHORITY

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

METHODOLOGY

We reviewed the State's Y2K compliance activities as of April 1, 1998. Our methodology included a survey of 20 state offices concerning their Year 2000 preparedness and follow-up interviews as necessary. (The review survey is included in Appendix A.) We reviewed these offices because they administer programs that, if disrupted by computer failure, would have serious repercussions for the State and/or the public. As an example, should the state's computer system that supports determination for eligibility for social welfare systems become non-operational, a possible consequence is that tens of thousands of Vermonters would not receive social welfare benefits such as food stamps and Medicaid. As part of this portion of our review, we also interviewed and corresponded with several information technology directors/administrators from key state offices. We also reviewed results of a recent General Accounting Office survey (GAO) that was completed by those state offices which have significant interactions with the federal government.

Our review particularly focused on the awareness and preparedness of the State's Chief Information Officer (CIO). The CIO is responsible for the State's overall strategic decision making concerning information technology and therefore has the lead role in the state's response to the Year 2000 (Y2K) computer date issue. We reviewed the CIO's published policy and strategic direction concerning Year 2000 compliance and reviewed all four editions of the Information Technology Five-Year Plan (5YP), which have been published since 1995. We also interviewed and corresponded with the CIO.

Since our review includes a comparative assessment of Vermont's preparedness when contrasted with other public entities, we conducted an extensive review of Year 2000 compliance efforts undertaken by the federal government and selected state and local governments. This portion of the review included review of several state and federal government Internet Year 2000 compliance-specific sites (25) that are actively maintained to address and share Year 2000 information and resources. We also interviewed selected officials from such states, reviewed a variety of reports prepared by other states concerning Year 2000 issues in their own states, as well as reports prepared by the GAO and the federal Office of Management and Budget. Finally, we undertook an extensive literature search of news article data bases to better understand the global impact of the Year 2000 compliance problem.

In conducting our evaluation of the State's Year 2000 compliance preparedness, we adapted the problem-solving approach suggested by both the Gartner Group, an internationally-regarded information technology consultant and the Office of Management and Budget (OMB). This evaluation approach was also recently used by the State Comptroller of New York and the State Auditor of Massachusetts in reviews each of their offices undertook of Year 2000 compliance efforts in their respective states.

BACKGROUND

It is estimated that on January 1, 2000, millions of computers and perhaps billions of computer chips may fail because they will be unable to tell whether it is the Year 1900 or the Year 2000, if appropriate remedial steps are not undertaken. Many automated systems and electronic devices that use dates will fail to recognize and properly process dates designated by the year 2000 (and thereafter) because they were developed to assume that a two-digit date field represents a date in the 20th century (19XX). The resulting inability to process these dates may lead to widespread computer crashes and failures of electronic devices with embedded computer chips.

Source of the Year 2000 computer problem: use of 2 characters instead of 4 to represent the year.

This problem was intentionally created during the early years (the 60's, 70's and 80's) of automated system development to conserve electronic data storage space which was sparse and expensive. To save money, programmers decided to represent years with the last two digits instead of the full four, and for reasons of both costs and inertia, this remained the industry standard until very recently. At the time of development, programmers and other information technology (IT) personnel probably could not have expected that these systems would still be in use in the Year 2000.

This abbreviated method for storing dates was fine as long as it was assumed that the years in question were all in the 20th century. Beginning several years ago, certain systems for insurance, licensing, forecasting, etc., which were using expiration dates beyond December 31, 1999, began to miscalculate or to refuse to operate. These situations called attention to the problem within the insurance industry, in particular, and entities using these systems proceeded with conversion projects to enable their systems to handle dates in the year 2000 and beyond. Despite the experience of the insurance industry, the rest of the private and government sectors have been slow to respond to the Year 2000 issue. However, within the past 12 months it has become widely understood by IT managers that any computer or any embedded computer chip which can not distinguish between the 20th and the 21st century is in danger of crashing when the clock ticks from December 31, 11:59:59, 1999 to January 1, 12:00:00, 2000. World-wide, reprogramming computers so they can recognize dates beyond the Year 2000 -- making them “Year 2000 compliant,” as it is referred to -- has become an urgent problem with a potential for far-reaching economic impacts. Current estimates put the world-wide cost for Year 2000 compliance between $300 billion and $1 trillion. Costs for the federal government are currently $4.7 billion; other examples of estimated costs public entities include $100-$200 million for the state of Maryland , $25 million for the state of Minnesota and $9 million for the city of San Diego.

Vermont’s Year 2000 compliance problems include more than its old mainframes; they include every computer the state owns, any interface between computers and potentially any piece of equipment with an embedded chip.

Non-compliance is not an option for the State because of the risk of disruption of crucial state services.

Year 2000 computer date recognition obviously has serious repercussions for state government which relies heavily on computing technology. Here in Vermont, Year 2000 (Y2K) compliance may be perceived to apply only to the state’s older mainframes and to only some of its personal computer technology. But, Y2K issues exist wherever there are interactions between internal and external computer systems (e.g., bank systems where the state uses direct deposit; federal or state payment systems where electronic fund payments are used). Both the internal and the external computer must be Y2K compliant in order for these kinds of transactions to continue uninterrupted. Additionally, within state government, even if a “mission critical” computing system (an automated system upon which a given state office relies to provide primary service to customers and clients) is Y2K compliant, if it receives or relies on data generated by another system that is not Y2K compliant, the mission critical system will likely fail. The State also has potential Y2K problems with any activity that is controlled by an embedded chip with a hard-coded date in so-called “smart systems,” such as doors, alarms, HVAC systems, traffic lights, elevators, fax machines, even dams. Potential problems caused by embedded chips may occur when the chips reference dates (e.g. the chip erroneously calculates an inspection deadline has been missed and as a safety precaution causes electronic systems to shut down). Another potential problem can occur when the chip performs a mechanical operation based on an erroneous date calculation or elapsed time calculation (e.g. shutting down elevator systems, bank vaults etc. for security reasons on a weekend.)

Year 2000 noncompliance is, in our view, not an option for state government. Noncompliance and the resulting disruption of state services could result in annoying consequences to users of state services, such as delayed tax refunds, or it could result in problems ranging from tens of thousands of Vermonters unable to receive food stamps or heat assistance, state funds threatened by problems with bank and pension accounts, tens of thousands of Vermonters without valid driver's licenses, lost data on the locations and clean-up status of hazardous waste sites, to name just a few. Failures of embedded chips in smart systems could also be relatively minor or they could be quite serious: perhaps an elevator might not work in a particular building; on the other hand -- at the extreme -- perhaps a dam could release water at an inappropriate time and cause a flood. What is clear is that the risks for Year 2000 noncompliance are very real and potentially very serious. At the very least, any disruption of state services caused by Year 2000 noncompliance could undermine the confidence in state government of those Vermonters affected.

Project Management Approaches to Solving the Year 2000 Compliance Problem

Year 2000 compliance is a Project Management, not an Information Technology issue.

There is one common theme (emphasized in our findings below) observed during our survey of the approaches of other public entities to solving Y2K compliance: Year 2000 compliance is a project management problem. Although the problem is clearly technical in origin, based on our review, it is clear that a best practices model of successful management of Year 2000 compliance by public entities involves the following steps:

· **Inventory:** The mandatory first step to determine the scope of the potential problem. State government should inventory hardware, package software, custom applications, interfaces, firmware (software logic set permanently or semi-permanently in the read-only memory of a hardware device); in short, any device that is plugged in, has wires, or runs on a battery that may have an embedded chip and may use a date.

· **Assess:** After Inventory, the Y2K compliance status of each piece of inventory must be determined. In many cases, this will be by vendor inquiry (for most hardware and package software). However, programmers will have to examine custom applications, which are relatively common in state government. Additionally, any interfaces between systems must be assessed.

· **Plan:** After Assessment, a Conversion Strategy, based upon sensible business decisions, preferably using a cost/benefit analysis tool must be developed. Options for the Conversion Strategy are:

Renovate: Fix the information resource to accept four-digit years.
Replace: Replace the information resource with a Year 2000 compliant asset.
Upgrade: Purchase and install an upgrade to the resource.
Retire: Stop using information resource because it is no longer needed.
No Action: Keep status quo.

· **Implement:** Best practices of automated systems project management should be used for the implementation phase, including an effective project management tool which can handle the detail and provide easy-to-use summary reports and charts, designation of project team leaders who meet regularly and close monitoring of progress by senior management and independent observers, such as auditors. (See Minnesota's Y2K Best Practices in Appendix B for a detailed example of best practices approach to Implementation.)

· **Test:** No system can be presumed to be Year 2000 compliant until it is thoroughly tested. Adequate time for testing of systems must be built into the State's Year 2000 compliance plan.

· **Certify:** Once tested, management should confirm that the system's Year 2000 compliance is reliably certified.

Potential Problems for the State in Becoming Year 2000 Compliant

Challenges for Vermont: size of the problem, shortage of personnel, rising costs, potential for missed deadlines.

Vermont, as our report indicates, faces the risk that critical portions of its Year 2000 compliance efforts may fail. Aside from the short time remaining, the state faces these challenges:

· Determining the extent of the Y2K problem

For those offices who have not undertaken an inventory and even for those that have, finding all the possible places where a date field may reside is a difficult challenge. Records maintained by human service agencies, for example, could have a dozen or more date fields in each automated record. Many departments will have to identify thousands of date references on chips embedded in their infrastructure.

· Shortage of skilled personnel

Qualified IT personnel to assess and work on Y2K issues are already scarce and will only become more so. Many of the IT staff who built the original programs and worked with the older languages have retired. Vermont, in fact, has already experienced difficulty in attracting and keeping IT personnel to work on Y2K compliance. One well-qualified programmer in the local area has been pursued by the Communications and Information Technology office (CIT) and the Department of Motor Vehicles (DMV) but their attempts to contract with the programmer as a “sole source” for the duration of the time before Year 2000 conflicted with state Personnel policy and they were unable to enter into a contract with the programmer. Meanwhile, the programmer has been contacted for a long term and better paying job with a Midwest IT project and may depart from the central Vermont market.

Concurrent with this review, the state Personnel Department is attempting to reclassify state IT jobs so that state offices can offer competitive compensation to attract and retain technology personnel. However, even with this reclassification, the State faces the very real danger that the skilled IT professionals it has could be lured away by much more lucrative compensation. Noteworthy in this regard, is that according to CIT, there were recently seven vacant IT positions within the state and CIT is having difficulty attracting candidates -- indicative of the scarcity and the competition for skilled IT personnel.

· **Rising costs**

Because of the shortage of Y2K consultants, qualified programmers and IT personnel, costs for compliance related-work is literally going up daily. Demand already far outstrips supply and the situation will only get worse. The market for programming talent, whether experienced or just out of college, is anticipated to be such an aggressive seller's market that private business has already developed “stay” or “end-of-project” bonuses to try to keep good programmers on their mission critical projects. Those state offices that have not already secured Y2K compliance services may find they are far more expensive than anticipated.

· **Failure to meet project deadlines**

The national average for large scale computing projects being on-time and within-budget is less than 20%. Vermont’s recent experiences in implementing such projects do not indicate our state has fared significantly better than the national norm. Without rigorous monitoring, there is a risk that some significant portion of the State’s Year 2000 compliance efforts will not be completed on time.

Response of the CIO and State Auditor Follow-Up

The CIO has indicated that by and large she feels the State’s approach and progress towards Y2K compliance is adequate. (The CIO’s response is included as Appendix D; the State Auditor’s comments concerning the CIO’s response are included as Appendix E.) As we indicate in Appendix E, the State Auditor feels there remain serious risks to the State inherent in Y2K non-compliance and that significant sectors of the State are at risk for non-compliance. Therefore, it is the intention of the State Auditor to follow up on this report with future reports concerning the State’s progress towards Y2K compliance. As part of this effort, we intend to comprehensively survey all state offices concerning Y2K activities and report these results before the Fall of 1998.

FINDINGS AND RECOMMENDATIONS

A. Project Management of Year 2000 Compliance

Ensuring that the State is Year 2000 compliant, although a highly technical problem in origin, is ultimately a project management issue. In that sense, it is similar to other large scale changes the State has undertaken in recent years, such as the recent state-wide change in financial reporting from a cash basis to generally accepted accounting principles (GAAP) basis, or the institution of the many new welfare requirements and programs as part of the State's welfare reform efforts.

In each of these examples, systems that needed changing, updating or replacement are first identified, detailed planning to institute the changes are undertaken, and then the plans are implemented. In order for projects to be successfully completed, top management has to ensure that each project phase is adequately undertaken and that necessary co-ordination and information exchange take place within and between agencies. Tools to monitor the status and progress of such projects are crucial to the top management responsible for project implementation. Goals are set and management measures project progress and success against goals of quality, time and cost.

Year 2000 compliance is probably the largest IT project the State has ever undertaken.

Year 2000 compliance is probably a much larger project than either of these two examples, yet the State has not brought the necessary project management skills to bear on this crucial challenge. Although the Chief Information Officer (CIO) is charged with general oversight of information technology within state government and as such, her purview includes the Year 2000 compliance for all of state government, the CIO is not acting as a project manager for the Y2K problem in any traditional sense. Instead, the CIO is currently using a "decentralized" model of project management, relying almost totally on individual state offices to recognize, plan and then implement necessary Y2K compliance activities.

It is noteworthy that in our review of Year 2000 compliance activities by other public sector entities (federal, state and local government), we found that almost all have adopted strong, centralized project management and say that it is crucial to ensure accountability and efficiency. Elements these successful compliance projects share -- all lacking in Vermont -- are:

· a directive from the Chief Executive/Legislature mandating Y2K compliance by all state offices;
· a centralized Y2K office directing the project that speaks with the authority of the Chief Executive;
· clearly spelled-out expectations concerning what individual offices are to accomplish;
· deadlines for completion of each phase of the project;
· on-going monitoring of Y2K compliance work, including, reporting status to the Y2K office at regular intervals.

FINDING A.1. Need for a Central Y2K Office

Project management for state-wide Year 2000 compliance efforts is inadequate. Vermont currently has a “hands off” approach to management of Y2K for compliance by individual state agencies and departments. Although the State has an Information Technology Five-Year Plan, the Plan has not been adequate to ensure that all state offices have undertaken the necessary steps to prepare for Y2K compliance. As a result, certain state departments and agencies may not be Y2K compliant in time, unless remedial action is taken.

Although the CIO and her staff are quite aware of the significance of mainframe and personal computer Y2K issues, our review has found serious deficiencies with regard to the oversight of overall Y2K compliance. Beyond taking steps to ensure that the State’s central financial accounting system (FMIS) will be Year 2000 compliant, the Agency of Administration, through the CIO, has exercised little leadership or oversight of Y2K issues within the rest of state government. Instead responsibility for recognizing and addressing Y2K problems has been delegated to individual agencies. Individual agencies are “on their own” -- they are expected to assess, plan and implement Y2K solutions on their own.

Vermont’s decentralized approach to Y2K compliance, if uncorrected, may result in disruption of some state services.

Arguably, for agencies with strong Information Technology (IT) staff/resources, Vermont’s current lack of centralized control over Y2K may have some advantages. Offices and departments are free to turn to sources that they deem most appropriate for Y2K compliance projects. While this freedom is an advantage for offices with a strong IT component, as our survey indicates (see Section C., below), other offices are lagging far behind in Y2K compliance -- indicative that this decentralized approach has meant that some offices are not aware of the seriousness of the problem and are in need of assistance. As a result, some agencies may not be fully Year 2000 compliant and there may be a resulting disruption of some state government services and functions, unless steps are taken to ensure that they become compliant.

The CIO has informed us that she has adopted this “decentralized” style since that is consistent with the nature of Vermont state government and because of the lack of CIO resources. She also notes that agencies through the Information Technology Five-Year Plan (5YP) have had a planning vehicle to address Y2K issues. Although it may be argued that the 5YP may force entities to plan for their IT development -- and, in fact, our review suggests that the 5YP may not be sufficient enough a “stick” to force all entities to seriously address Y2K issues -- strategic direction concerning preparation of individual offices plans has been minimal from the CIO, especially in relation to the critical and sizable Year 2000 problem. As a result -- as the CIO has acknowledged -- if offices have not been aware of any or parts of the Y2K problem until this fiscal year, then they may be too late to get specific funding for Y2K compliance work prior to the millennium. Although they were given the authority and the responsibility for Y2K preparation, many offices may not have been adequately informed about the problem and may not have previously sought funding for Y2K work. (It is noteworthy for example, that to date, there has been no state-wide seminar for IT and business managers to address Y2K issues. If managers are not aware of Y2K issues, the State has made no efforts to ensure that they become so.) Such offices may have no funding for Y2K projects until FY'00, when it will likely be too late.

The State of Virginia had initially adopted the same decentralized approach to Y2K compliance as Vermont. As in Vermont, individual agencies were charged with solving the Year 2000 problem, with no central office coordinating or monitoring the effort. The Gartner Group, an internationally-regarded information technology consultant, reviewed the status of Virginia's year 2000 compliance in late 1997 and recommended that Virginia create a Year 2000 project office under a true statewide coordinator to refocus the efforts of the state's confederation of separate projects into a more cohesive and efficient effort.

Virginia also had a decentralized approach to Y2K compliance, but has since abandoned it in favor of designating one office as responsible for coordination, monitoring and communication.

Virginia has followed the recommendation of the Gartner Group and now has a designated Y2K office within an existing central administrative office. The Virginia Y2K office is charged with coordination, monitoring and communication; at the same time individual offices still remain responsible for actual compliance efforts.

This is the same model we are advocating for Vermont. Virginia officials in interviews with us stressed the dangers in Vermont's current approach: Until the statewide coordinator in Virginia recently conducted a detailed survey of agencies, there was no statewide information about the scope of the problem across all of the agencies nor was there a mechanism to achieve the economies of effort in sharing how to recognize and solve the problem. Virginia officials also indicated that their recent survey and monitoring efforts have led to a greater understanding that the magnitude of Y2K issues was greater than initially believed. We believe Vermont faces the same danger: lack of knowledge is likely obscuring the true magnitude of Vermont's Y2K problems.

Vermont's current approach to Y2K management may mean the State is unaware of some Y2K problems.

While accepting that the CIO obviously does not have adequate resources to manage each Y2K compliance project at each office, we recommend several steps below that would significantly improve project management, even without allocation of significant additional resources to the CIO. In our view, many of these recommendations could already have been accomplished within Vermont's current IT management processes -- what has been lacking to-date is awareness and state-wide leadership. We also emphasize that the hallmarks of strong project management do not include the requirement that the CIO be responsible for actual performance of the Y2K compliance activities at the individual departments; **rather the CIO's crucial role in Y2K compliance is**

leadership and management of the project: defining the problem, setting the goals and monitoring progress.

RECOMMENDATIONS

A.1.a. The Governor should mandate that all state offices be Year 2000 compliant by June 30, 1999.

There should be a clear directive from the highest levels of state government that Y2K compliance is a serious issue that must be dealt with by state managers. As such, the directive needs to come from the Governor. The directive should make it clear that Y2K compliance is a requirement, not an option for the state and that Y2K compliance is a business issue, not just a technology problem. Ideally, all offices should be compliant by December 31, 1998, in order to have a full year to test systems. However, we do not think many departments can realistically meet this goal.

A.1.b. The CIO or some other state-level office should be clearly designated to direct all state government Y2K activities.

State managers need to be accountable to one office which needs to act as a clearinghouse for all Y2K activities. The current 5YP has a section entitled "Assignment of responsibility for (Y2K) compliance." The section states that "it is expected that a significant portion of [the assistant CIO] position will support Y2K activities." However, this statement does not clearly commit the CIO to managing the entire Y2K issue and it is clear from the CIO's response to our draft report, that she does not believe that she has the authority to do so -- especially with regard to embedded chips.

Vermont's Y2K office does not need to have all of the information or make all of the decisions about Y2K, but it must manage the Y2K problem from the state level, and it must have authority to manage the entire scope of Y2K issues. Even in a "decentralized" model in which the Y2K office does not perform many of the Y2K compliance activities, it has several crucial tasks to play. As the Arizona Y2K office describes itself: "[our] primary role will be leadership, coordination and oversight." In our view that is the role a Vermont Y2K office should play. Specifically, a Y2K office should do the following:

First and foremost the Y2K office should set the agenda: setting deadlines with individual offices for timely completion of each phase of their Y2K compliance project activities: inventory, assessment, planning, implementation and testing. These should include a detailed specification of the kinds of activities that make up each phase of a Y2K compliance project: what needs to be inventoried, how to conduct assessments, what should be incorporated in planning for Y2K activities, how to manage implementation and how to ensure testing is adequate.

The next important task for the Y2K office is collection, maintenance and distribution of information that will support individual offices. The Y2K office does not have to be the technological center of the effort, but it does need to facilitate the effort. Currently, Vermont's Y2K efforts are occurring without co-ordination and without a vigorous communication network through which to exchange information. Sharing information resources among state IT managers and others who are working on the Y2K problem would be more cost-effective and more efficient than continuation of many uncoordinated efforts. The kinds of information the office can maintain include:

· the experience of individual state offices with Y2K issues;
· the expertise resident in state offices on Y2K issues;
· Web sites and other contacts for key Y2K issues, such as listings of Y2K compliant equipment, contractors and consultants.

Thirdly, the Y2K office must monitor. The Y2K office must be accountable for oversight of the Y2K IT duties that it assigns. In order to see where the State stands in reaching compliance and to gauge progress toward that goal, the Y2K office must establish standards for effective periodic status reports and must actively identify and challenge management to address compliance problems.

Finally, the Y2K office should communicate issues vertically. Senior management, the Executive Branch and the Legislature all need to be informed and updated concerning the State's Y2K compliance progress. It is important that policy makers and the public understand that this is a business problem and not just a technology problem, and that the consequences for failure are severe. It is equally important that policy makers and the public know about Y2K likely failures and the consequences of those failures, so they can make informed decisions.

FINDING A.2. Need for Comprehensive Status Reports

The present reporting system for progress towards Y2K compliance is inadequate. As a result, the CIO does not have a realistic assessment of the State's status or progress toward Y2K compliance.

Currently, no state offices report to the CIO in any detailed or regular basis concerning the progress of their Y2K compliance. The CIO has received verbal assurances from some state offices that certain "mission critical systems" have been assessed and will be Y2K compliant by 1999. However, there is really nothing substantive other than general assurances that the work will be done and on time. As our surveys show, 11 mission critical systems (310 programs) in the Department of Motor Vehicles (DMV) have yet to be assessed; DMV also does not know what will be required for compliance activities once the assessment has been completed.

Without an inventory, assessment and an established implementation project time line, it is difficult, if not impossible, to identify a project completion date. In addition, without regular status reports, it is difficult, if not impossible, to gauge progress toward the deadline or to identify delays and missed deadlines or potential failure in terms of Y2K compliance before Year 2000.

The current form of reporting in the 5YP demonstrates the weakness of not using an effective project reporting tool. In the third edition of the 5YP, published in January 1997, the Tax Department identified two important milestones for the Vermont Integrated Revenue Collection Information System (VIRCS) for FY'98: (1) January 1998 implementation of Individual Income Tax and (2) April 1998 implementation of the audit and collection processes for the Individual Income Tax. In the next edition of the 5YP, published in January 1998, these same milestones are listed for January 1999 implementation. This represents delays of one year and eight months respectively for the two implementations. Meanwhile, the Tax Department maintains that both of these projects are on time.

In the case of DMV, which has yet to complete its assessment, it should be stressed that Y2K consulting resources are already very scarce at this late date, approximately 15% of all software projects finish an average of six to seven months behind schedule, and DMV has a very narrow window of time in which to accomplish the entire range of Y2K activities. There is a significant risk that these mission critical systems at DMV will not be compliant in time. Yet, the CIO feels that the state as a whole will be compliant by Year 2000.

Regular reports on Y2K activities will ensure offices are aware of the Y2K problem and are on track with compliance projects. They will also protect the State from unexpected project delays or system failures.

As this example makes clear, verbal assurance of progress or status is insufficient accountability. Failure to require regular detailed project reporting permits at least the following four weaknesses:

1. The CIO has no assurance that offices **are aware and have inventoried** the full range of potential Y2K compliance problems:

· are all information-source personal computers (PC's) and other systems that feed into mission critical systems Y2K compliant?
· are vendors, banks, subrecipients or other business partners that provide information or access a state office computer through an interface or diskette, Y2K compliant?
· are crucial pieces of support equipment such as communications, security, public safety and alarm systems, power utilities, and elevators compliant?

Even if the "mission critical systems" are compliant, non-compliance in any of these supporting or peripheral systems, can cause a mission critical system to fail and/or cause serious disruption to the state office in question.

2. The CIO is not informed about all project deadlines for Y2K compliance activities. Therefore, **the possibility of late projects, missed deadlines or concern for problems is unknown** outside the office conducting a particular Y2K activity. Without the big picture, senior state management cannot anticipate when and where critical events will be occurring -- such as the likely non-compliance of some DMV mission critical systems.

3. The CIO is not regularly informed about the progress of all projects. Therefore, **problems with Y2K compliance projects that could have statewide impacts can not be identified** nor can such projects receive special attention from senior management.

4. Finally the failure to require reporting from state offices means the CIO has **no assurance that offices have tested to ensure that systems are Y2K compliant**. (See Finding A.3).

RECOMMENDATION A.2.

We recommend that a regular and rigorous Y2K status report of all state agencies and offices should be implemented immediately.

The Federal government through the Office of Management and Budget (OMB) has required such a report from all federal agencies since January 1997 on a quarterly basis. These reports have enabled OMB to:

1. Require accountability from agency management;
2. Be timely informed about which and when agencies are behind on Y2K activities;
3. Look for trends in the Y2K situation;
4. Anticipate revisions to contingency plans;
5. Monitor and revise estimated costs for federal government Y2K compliance. (**If there is one lesson the OMB reports illustrate, it is that Y2K activities take longer and cost more than managers originally estimate.** Estimates provided to OMB for the quarterly report on February 15, 1998 show a 20% increase in the estimate of total Y2K costs since the November 1997 quarterly progress report.)

No area of state government is unaffected by Y2K compliance. Within each state office, one specific IT or business manager should be identified and charged with responsibility to report to the Y2K office on compliance progress. **The first of these reports should be prepared by this summer.** They should include a realistic and quantified appraisal of where the office stands with regard to each phase of Y2K activities, timetables for completion and testing as well as realistic cost estimates for each phase.

FINDING A.3. Need for Testing.

Even among offices that report that they are Y2K compliant, the CIO has inadequate verification that adequate testing of "compliant" systems has taken place. Unless best practice testing occurs, some systems deemed "compliant" will fail.

Testing is the most critical component of Y2K activities. In addition to individual computing systems, system interfaces must also be tested.

It is generally understood throughout the information technology industry that even when systems are thought to be Y2K compliant (because Y2K remediation has been performed by knowledgeable personnel according to project plans or because software has been recently purchased), some will fail, because they have not been tested at all, have not been properly tested or because the vendor's assertion of compliance was unreliable. Testing of system interfaces is especially critical. The Y2K problem can act like a computer virus which may be created by a non-compliant format in one machine which is passed through a network into a compliant machine where it then creates chaos and shuts down an entire system. For these reasons, testing and verification of compliance is a significant concern in preparing for Year 2000.

RECOMMENDATION A.3.

The Y2K office should require that all "compliant" systems be properly tested and that verification of testing be submitted to the Y2K office. Certification that the system is Y2K compliant should only be issued by the Y2K office after review of such submissions.

Underestimating the amount and scope of testing has been identified as one of the 10 worst pitfalls of the Year 2000 problem. Good project management requires sufficient testing. "Industry experts agree that testing is 50-60% of the [Y2K] effort." In Vermont's case, the inherent complexity of the Y2K problem is compounded by the state's fragmented approach to the Y2K problem and the variation in IT skill levels within individual offices. Proper testing and verification of that testing is critical for the success of Vermont's Y2K compliance efforts. Connecticut's Y2K program manager recently emphasized that "testing is the real proof of things working." Both testing and verification should be overseen by the Y2K office. Further, since automation project testing usually consumes more than 40% of project time, the Y2K office should assure that project schedules reflect this and that the test time is used. Saving time in testing has not been found to be worthwhile by other entities who have engaged in Y2K compliance projects.

FINDING A.4. Need for Contingency Plans

There has not been adequate review and verification of contingency plans for Y2K issues.

The CIO has stated that state offices should have recognized the need for contingency planning and should be prepared in case their own or other systems with which they interact are not Y2K compliant by January 1, 2000. However, no one at a senior level has required verification nor reviewed these contingency plans for adequacy or measured them against contingency plan best practices. This approach again illustrates the problem of leaving agencies to their own devices: only those offices with staff familiar with the possibility of failure have prepared plans. And even then, these plans may or may not address the variety of failure scenarios suggested daily on Y2K Web sites and news groups. Obviously, agencies that are unaware of failure scenarios will fail to devise contingency plans, unless a Y2K office requires them to do so.

In Vermont, there is a significant likelihood that many agencies or offices are relying on the implementation of the new FMIS system (state's central financial and accounting computing system) before Year 2000 to cure their own Y2K ills. However, it is now believed that implementation of the new FMIS will not occur before Year 2000 and agencies relying on a new FMIS may be thrown into a desperate situation to assure their own compliance or survival beginning at this late preparation date.

RECOMMENDATION A.4.

The Y2K office should advise state offices to prepare, document and have their contingency plans reviewed by the Y2K office as soon as possible. Contingencies should include the possibility that the state will not have a new FMIS system operational by July 1, 1999.

Vermont must have contingency plans in place in case Y2K compliance work is not completed.

Minnesota, which, in our review, has one of the best Y2K projects among the 50 states has emphasized the importance of contingency planning. As the Minnesota Project Y2K Manager says, "No matter how well agencies have planned for Year 2000 conversions, failures may occur as the result of unanticipated errors, or non-compliant service providers and business partners. ... [G]iven the short time remaining and the amount of work ahead, contingency plans are essential. Agencies should revisit the priority status of mission-critical systems and make sure that adequate back-up plans exist and are well documented." It should be noted that all of Minnesota's state offices completed an inventory of systems in 1997. As we note, several Vermont state offices have not even completed this crucial first step, making it all the more important for development of contingency plans.

The Y2K office should suggest standard contingency situations for planning, such as: not discovering embedded computer chips, failure of non-mission critical systems, non-compliant business partners, or failure of vendor-supplied or verified systems and/or software.

Individual offices then need to assess their own unique risks and respond to them with contingency planning. The ability to identify risk may require assistance from outside of the specific office.

FINDING A.5. Need for Warranty

Currently, there is no requirement from the CIO that all state offices use standard enforceable warranty language in contracts with Y2K compliance consultants.

The need for warranty protections in Y2K consulting contracts is important. The State, for example, needs assurances and protections in the event a consultant fails to finish a project on time, or fails to render systems Y2K compliant. State managers should assume that something can and will go wrong, and make sure the State has contractual recourse. In general, the risks the State faces in purchasing Y2K compliance consulting include:

· the contractor will not provide the finished product in time;
· the contractor's compliance testing will fail to detect non-compliant aspects of an IT system;
· the vendor will not honor the contract warranty to make the product compliant;
· the vendor will have gone out of business or be unreachable;
· Vermont will have a liability obligation for not providing service because of a Y2K compliance failure caused by a vendor.

Despite such possibilities, currently, the CIO has not obtained legal advice on or published policy requiring uniform RFP language to ensure that all Y2K contracts adequately safeguard state interests in terms of ensuring timely completion, quality of deliverables and limitations on State liability for Y2K compliance failure.

RECOMMENDATION A.5.

A Y2K office should require enforceable Year 2000 warranty language in all new vendor contracts and RFP's for IT products and services. The Y2K office should seek assistance of the Attorney General's office in drafting such language.

The State of Vermont should address the Y2K liability issue with legal assistance in the most effective and efficient manner to minimize the State's exposure to this significant risk. Departmental resources are not necessarily available or aware of the issues surrounding Y2K litigation.

As the noted in the Minnesota Year 2000 Project newsletter, "if a vendor is unwilling to warrant Year 2000 compliance, it is appropriate to question whether or not the state should do business with that vendor." Clearly, to protect itself and its citizens, the state should enact such safeguards, which in Minnesota were drawn up by the Attorney General. (The Minnesota Year 2000 warranty and dispute resolution language is attached in Tab 9 of the Appendix B.)

FINDING A.6. Embedded Chips

To date, there is no state-wide monitoring of state systems and equipment that may be adversely affected by non-compliant embedded computer chips.

When we first met with the CIO prior to initiation of this review, she indicated that she was not aware of, nor had she directed any review of, embedded chips in state systems or equipment for Y2K compliance. Subsequent to this initial meeting, the CIO has contacted State Buildings to alert them to the issue. Although State Buildings has begun an inventory, to-date, there is no plan that has been requested or reviewed by the CIO that details how State Buildings will inventory, assess and ensure that equipment and systems with embedded chips are Y2K compliant. As noted in the Background section of this review, embedded chips are potentially present in almost every piece of electronic equipment or “smart” system extending from telephones to elevators to security systems and alarms.

Embedded chips may cause serious problems. The issue faces every office in the State.

Further, the potential for problems with embedded chips extends beyond State Buildings, likely including agencies such as the Agency of Transportation and the Agency of Natural Resources (ANR), whose IT manager reported to us during the course of this review, that our request for information concerning Y2K compliance progress by ANR had prompted him to realize for the first time that the State’s dams could possibly have a problem with embedded chips. Importantly, the embedded chip problem affects every state office.

RECOMMENDATION A.6.

The Y2K office should direct that every state office should undertake a thorough review of Y2K compliance of systems and computers with embedded chips.

For many pieces of equipment, this will involve checking with vendors and manufacturers for Y2K compliance of each particular piece of equipment. It would be helpful, therefore, that as individual make and models are certified as Y2K compliant, that these be listed on a Vermont Y2K Website by the Y2K office. This will save some duplication of effort in tracking down vendors and verification by individual state offices.

B. COSTS OF Y2K COMPLIANCE

Costs for Y2K compliance may represent the biggest potential problem for policy makers. (Some economic analysts believe that world-wide costs in the public and private sector may trigger an actual recession.) Costs in general for Y2K work are escalating rapidly and the public sector is finding that it is being forced to rapidly alter its estimates of expected costs for compliance. As we have already indicated, costs for individual offices that have not begun significant Y2K work are likely to rise precipitously in the months ahead. Some numbers to ponder:

· OMB estimates the current cost for Y2K compliance for the federal government is currently at $4.7 billion as of February 15, 1998. In November 1997, the estimate was $3.9 billion. All federal agencies completed inventory and assessment as of January 1998, with almost all having completed those tasks as of 1997. Some key Vermont state offices (see Section C., below) have not yet completed the inventory phase of Y2K activities.

· Several smaller states (as of April 1997) are reporting widely varying estimates for Y2K compliance costs:

Alabama: $85 - $100 million
Arizona: $70 - $100 million
Idaho: $15 million
Kentucky: $12 million
Minnesota: $25 million
Nebraska: $22 million
Nevada: Under $10 million
North Dakota: $3.2 million
Tennessee: $12 -$15 million

It is clear that the one consistency in the above numbers is the inconsistency. Given the age of these estimates (a full year), it is likely that as states gain experience and refine their estimates, some estimates will go up, some down. The state of Connecticut's Year 2000 Program Office, for example, has found that for some agencies, Y2K compliance for mainframe and PCs is progressing better than projected, costing much less than some state or consultant personnel had estimated. However, the Connecticut office is cautious as it begins to test the fixes on the state's key computer systems and to investigate the state's tens of thousands of mechanical devices that use computer chips. Savings realized in the mainframe and PC area are expected to be redistributed for testing and for embedded chip solutions.

Vermont may face currently unknown and potentially large costs associated with Y2K compliance.

For Vermont, what is clear is that the cost of Y2K compliance for the State is not clear and could have significant impacts on state budgets for the next two or more fiscal years. Significantly, this potential drain on state funds coincides with the requirement for significant investment of new state funds to support state efforts to increase state aid to local education as part of Act 60. **Policy makers need to be very aware of potential Y2K costs as they make budgetary decisions in the future.**

FINDING B.1. Reporting of Y2K Compliance Costs

Individual offices have not separately reported costs for Y2K activities to the Legislature. In some cases, they do not know likely costs associated with Y2K activities. As a result, the State could face significant unforeseen compliance costs in upcoming budgets.

A significant weakness of the State's current Information and Technology Five-Year Plan is that state offices have not been required to report planned Y2K-related expenditures. Based upon our review, we find no evidence that all state offices are aware of and have separately reported these costs in their budget submissions to the Legislature. As a result, some state offices have likely neglected to budget (and plan) for Y2K activities. And, there is no question that policy makers have been left in the dark concerning Y2K costs incurred to date.

As the OMB quarterly reports demonstrate, Y2K costs tend to go up as projects progress and more problems are identified. In Minnesota, IT personnel thought they had remediated all “dates” identified in 40 out of 400 programs in their Cost Accounting System (installed in 1972). But testing uncovered 20 more program and subsequent testing uncovered another 20 programs, meaning that there were 100% more programs than had initially been identified that needed to be remediated -- work which had not been budgeted for time or cost.

Although it is impossible for us to report on the likely amount of Y2K expenditures to-date, it is clear that the State faces significant expenditures in the near-term. For example, DMV does not yet know the extent of its task of bringing 11 mission critical systems into compliance. Other offices which have not undertaken adequate inventory, assessment or planning activities will almost certainly face unexpected Y2K compliance-related costs in the near term.

RECOMMENDATION B.1.

All state offices should complete an assessment of expected Y2K costs as soon as possible and report them to the Governor and the Legislature, so that the State can react appropriately.

The Governor and Legislature must be informed about Y2K costs as soon as possible.

We believe that it is critical that for the Governor and Legislature be presented with the most accurate estimate for unbudgeted Y2K compliance related costs, as soon as possible. This would allow the Legislature -- as it considers the FY’99 supplemental budget bill -- to decide if it wishes to make funds available in the second half of FY’99 for currently unbudgeted Y2K compliance activities. Obviously, if this information is available in the Summer or Fall of 1998, the Emergency Board could also take action, as it deemed appropriate.

FINDING B.2. State Resources for Y2K Compliance

The State has not devoted adequate resources to Y2K project management.

The office of the CIO is currently a two-person office, with the second position of assistant only recently created and filled. Irrespective of improvements that could be made by the CIO, the fact is that this level of resources devoted to directing and monitoring state-wide Y2K compliance is far from adequate. **Given the short time remaining until the Year 2000, more, not less, resources need to be devoted to project management.**

RECOMMENDATION B.2.

The State must <u>immediately</u> significantly increase resources dedicated to Y2K project management.

Whether policy makers decide that the Y2K office should reside within the office of the CIO or be housed separately, we believe that the State will, at a minimum, need to devote several times the current level of support to Y2K project management.

C. PROGRESS TOWARDS Y2K COMPLIANCE BY INDIVIDUAL STATE OFFICES

We present below the results of our Y2K compliance survey of 20 selected state offices which was completed on February 16, 1998. The survey is by no means exhaustive. We emphasize that Y2K issues effect every office in state government -- no matter how small. The offices below are representative of those where disruption of services caused by non-Y2K compliance will likely be detrimental to overall functioning of state government or cause interruption and/or disruption in the delivery of essential services.

Impact of Failure to Have Reporting Requirements

As we have noted above, Vermont has not established reporting standards nor required any kind of formal reporting by state offices concerning Y2K compliance activities. Our survey is the first attempt that we know of to actually aggregate and present this information.

However, the fact that the CIO and top state management have set no standards nor required agencies to report their progress using the same standards, hampers our ability to objectively assess the limited data we have been able to gather during this review. For instance, almost every office we have surveyed has indicated they completed an inventory (with the exception of the Department of Public Safety and the Tax Department). However, in follow-up inquiries with IT personnel, we discovered that what was meant by an inventory varied widely. Some offices conducted the same kind of formal inventory as the SAO; others (Department of Agriculture and the Department of Health) reported to us they had engaged in a “mental” inventory of key systems. Without a comprehensive inventory, problems can be invisible, and progress cannot be estimated or evaluated. A requirement that all offices engage in the same kind of formal inventory, using the same kind of inventory instrument, would allow us (or the Y2K office) to actually identify those offices that have completed this crucial first step, and those that lag dangerously behind.

Until reporting standards are in place and standard Y2K compliance reports are issued, it should be assumed the State is at risk for non-compliance.

This lack of reporting standards affects all aspects of Y2K compliance evaluation. Therefore, we have attempted to rate offices from the information that we have received in our survey -- which we should stress was entirely voluntary. This survey has obvious limitations: unlike Minnesota, for example, which is able to accurately report the percentage of vendor supplied hardware and software that is compliant as well as the percentage of custom software that is compliant, no compilation of such information exists in Vermont. This lack of information is a serious risk to the State. It is not sufficient for the State to simply say it is unaware of any Y2K problems. **Policy makers should understand and assume that State is in jeopardy until some standards are mandated and set, and results that are comparable between entities and consistent between report periods are generated. Therefore, as we have indicated, we intend to issue follow-up reports on the State's progress towards full Y2K compliance.**

However, even without the ability to formally analyze state Y2K compliance progress, we can make two significant findings concerning state progress towards Y2K compliance which back up this assertion.

FINDING C.1. Vermont's Y2K Compliance Status

When compared to other public entities, our survey suggests that Vermont lags behind in addressing the Y2K problem. There is reason to believe that key offices will not be Year 2000 compliant in time, without a significant increase in efforts.

It is clear from our review, particularly in follow-up interviews with state IT personnel, Y2K awareness varies widely. This fact, in and of itself, suggests that certain offices will not be compliant because they will not have identified the problem.

Overall, indicators suggest that Vermont lags behind in key Y2K compliance activities.

Also, when compared to other public entities, it is clear that Vermont faces a daunting challenge. For example:

· **Inventory:** When compared to the federal government and states like Minnesota, Vermont lags behind. Two key agencies or 10% of the offices we surveyed have not begun this crucial first step, and as we noted above, there is reason to believe the quality of inventory conducted by some offices has not been comprehensive. (CIT, for example, responsible for all Agency of Administration computing, has not completed its inventory and does not plan to do so until this summer.) **The rule of thumb is that in order to realistically meet Y2K goals, this step should have been completed at least 12 months ago.**

· **Assessment:** OMB reports that every federal agency finished assessment last year. Minnesota reports all state assessment was completed in January 1997 and that project planning was completed in June 1997. Our survey shows that 1/3 of agencies responding in Vermont have not completed Y2K assessment.

· **Y2K compliance of mission critical systems:** OMB in its most recent assessment (February 15, 1998) of federal agency progress towards Y2K compliance reported that 35% of mission critical systems are already compliant, but "while good progress is being made, it is not rapid enough overall." By comparison, our review suggests that in Vermont, of the 29 mission critical systems about which we have information (ANR did not report on its mission critical systems), only 9 or 31% are Y2K compliant. (We should stress these results are based on self-reporting, only, and this information does not include all mission critical systems, only the biggest ones.) If we adopt the OMB standard, Vermont's progress lags, especially when it is recalled that 11 DMV mission critical systems are currently non-compliant.

RECOMMENDATION C.1.

As noted above (Recommendation a.2.), rigorous reporting needs to start immediately. The Y2K office must then identify and assist those state offices that need help, based on established priorities.

FINDING C.2. Key Agencies That Are at Risk

At least 2 key state agencies, Department of Motor Vehicles and Department of State Buildings, are in serious danger of not being Year 2000 compliant, unless progress is greatly accelerated. Our review also suggests that there is cause for concern about the progress of several others.

Following the OMB reporting model, we have ranked Vermont offices based on their responses to our survey. a summary of the completed surveys is attached as Appendix A.

Tier 1 - The office is not successfully accomplishing mission critical tasks and phases within the project to assure that the project will be successfully completed on time. ("On time" usually means by a deadline well before January 1, 2000 for Y2K compliance. In some cases, the deadline must be before July 1, 1999.) Our assessment is that Tier 1 offices may not be compliant and may experience interruption and/or disruption in operations and/or delivery of services, unless there is a significant acceleration of Y2K compliance progress.

Tier 2 - Y2K compliance tasks are being accomplished, but there is some concern about timely accomplishment or the reliability of the final product. It should be stressed that accomplishment of Y2K tasks without reliable Y2K technology as an end product is not success at all. Some of these offices are at risk for Y2K non-compliance, without better project management and project oversight.

Tier 3 - The office is aware of the Y2K problem, may have no technology concerns or where the work is progressing smoothly and there is no present concern with schedule. These offices expect to be Y2K compliant on time.

Tier 1 - Insufficient Progress or High Risk: Likely Failure

State Buildings: Has just started statewide infrastructure process inventory and is therefore quite late; unfamiliar with concept; danger Department will not accept responsibility for Y2K compliance without top level mandate from Executive.

DMV: 11 major automation systems to assess and plan for compliance. Likely staffing problems in contracting for outside expertise and/or procuring dedicated Automated Services staff.

Tier 2 - Progress but Concerns: Some Failures Possible

CIT: Bears responsibility for all major automation systems (e.g. FMIS) within Agency of Administration as well as support for external systems (non-Agency of Administration); significant staff cuts from 40 to approximately 12 FTE's since 1996; problem with filling programming positions; inventory not yet complete.

Transportation: Significant workload; concerns about staffing; will be replacing two old Fortran systems in 1999 which leaves insufficient time for testing.

Tax: Is engaged in the entire replacement of its mission-critical systems (four systems), but has not inventoried other systems; concerns about contingency planning.

Developmental & Mental Health: Is aware and active but is reliant on upgrades and compliance of a variety of external systems: ACCESS, EDS claims, and FMIS -- all of which may be questionable.

Finance & Mgmt.: New FMIS scheduled to come on line, but will likely not be ready by Year 2000. Major upgrade (old FMIS) required, completed, testing status for compliance may not be sufficient. Many potential problems due to number of other systems that feed into FMIS.

Employmt. & Trng.: Dependent on federal decisions concerning support for state systems; cost may approach $1 million.

Public Safety: Has yet to begin inventory; significant interface with non-state government partners; crucial role in Public Safety.

Soc. & Rehab. Svcs.: Just beginning assessment phase for ACCESS system in which approximately 3,563 programs need to be reviewed for compliance

Tier 3 - Little or No Concern: Systems Likely to be Compliant

Aging and Disab.: No mainframe; aware and active

Agriculture: Minor automation; will replace equipment

Courts: Minor automation; aware

Econ. Opport.: Minor automation; progressing

Education: Aware and active

Natural Resources: Y2K activities in process; no delays; projects deferred to department level

Health: Activities on schedule

Payroll: Activities on schedule

Foster Care: Major systems are Y2K compliant

Medicaid Mgmt.: Major systems are Y2K compliant

RECOMMENDATION C.2.

The Y2K office must assist all Tier 1 state offices and closely monitor all the remainder.

Note: Future State Auditor reports on Y2K compliance will attempt to report on the progress of Tier 1 offices in particular.

D. INTERNAL CONTROLS

This review has applied internal control standards contained in the Statement on Auditing Standards No. 78: "Internal control is a process - effected by an entity's board of directors, management, and other personnel - designed to provide reasonable assurance of achievement of objectives in ... financial reporting, effectiveness and efficiency of operations, and compliance with applicable laws and regulations."

A. Control Environment: "The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. The control environment encompasses the following factors: 1) integrity and ethical values; 2) commitment to competence; 3) Board of Directors participation; 4) management's philosophy and operating style; 5) organizational structure; 6) assignment of authority and responsibility; and 7) human resource policies and procedures"

FINDINGS

1) We observed a high degree of integrity and ethical values in the CIO office;

2) The CIO is very committed to excellence and to the concept of developing strategic directives for state information technology. However, we found that serious problems exist in establishing and communicating goals for Y2K compliance and in failure to use best practice project management standards, both of which affect the competency of the State's overall Y2K compliance response;

3) No findings;

4) Management has chosen to allow state agencies the freedom to make independent decisions. However, management has been slow to establish statewide Y2K policy and has relied on the annual Information Technology Five-Year Plan, a passive budgetary reporting tool, to communicate Y2K information and policy. The decentralized form of Vermont state government fails to provide the proactive leadership required for the rather complex problem of Y2K compliance in the limited time remaining;

5) The decentralized organizational structure of Vermont state government has resulted in inadequate communication about the Y2K problem, slow development of statewide Y2K IT policy, and ineffective, generalized tracking of the state agencies' status of and progress in addressing the Y2K issue;

6) Authority and responsibility for the entire Y2K problem has not been clearly assigned at either the CIO or the department level in Vermont state government's decentralized environment. This lack of leadership or accountability hides the significant risk of business disruption if Y2K failures occur;

7) The CIO acknowledged that she had been unable to support Y2K compliance activities until hiring an assistant CIO, which she did in March of 1998. Our review also found that some agencies face significant challenges in securing Y2K compliance services from IT staff. These situations indicate that human resource policies and procedures may be challenged in the short time remaining to quantify and address the Y2K problem.

RECOMMENDATIONS

· The State should mandate that a plan be developed immediately to provide state offices with competency regarding the entire Y2K problem as soon as possible.

· The State should require that a single manager should be given the authority and the responsibility to direct a time-essential program to manage Vermont state agency efforts to attain Y2K compliance. The management style should be pro-active, utilizing best practice project management principles and processes, based on excellence in coordination, monitoring and communication. Recognition should be given to the fact that Vermont state government is decentralized and that efficiencies and economies can be obtained by organizing and by requiring state-wide office participation.

B. Risk Assessment. Risk assessment includes identification, analysis, and management of risks relevant to the organization.

FINDINGS

Our contacts with agencies during the review lead us to believe that there is a substantial possibility that some state automated systems could fail due to Y2K problems and that there could be a disruption of state services, without remedial action. Management has failed to adequately identify and assess this risk.

RECOMMENDATIONS

On-going assessments of risk should be performed by all entities with any automation. Assistance with the risk assessment process should be available from the Y2K office.

C. Control Activities: "Control activities are the policies and procedures that help ensure that necessary actions are taken to address risks to achievement of the entity's objectives." Control activities usually include performance reviews, information processing, physical controls, and segregation of duties.

FINDINGS

The absence of best practice project management controls (like a designated Y2K officer) and agency auditors (to provide independent testing and verification of Y2K projects and processes) was evident in many of the survey responses. This likely means less than adequate control and accountability for Y2K activities.

RECOMMENDATIONS

Departments should initiate controls and self-inspections regarding Y2K plans and projects to the maximum extent possible. The Y2K office should install management controls for coordination and monitoring.

D. Information and communication: At base, this element of internal controls is about whether existing information systems can generate information sufficient for the entity to manage itself effectively.

FINDINGS

Communication of the Y2K issue verbally at senior management or at Information Resource Management Advisory Committee (IRMAC) meetings and through the Information Technology Five-Year Plan is inadequate. Both policy makers and individual office managers are inadequately informed concerning the extent and seriousness of Y2K compliance issues. Current reporting methods concerning agency Y2K compliance status are also inadequate.

RECOMMENDATIONS

Communication about the Y2K issue, best practices for addressing the problem, and regular and vigorous status reporting on resolving the Y2K problem must be communicated in a clear, concise and timely method. Rigorous and regular status reports concerning agency Y2K compliance status must be generated and reviewed by the Y2K office. Y2K information must be shared with policy makers and with office managers responsible for Y2K compliance.

E. Monitoring: "Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls on a timely basis and taking the necessary corrective actions. This process is accomplished through ongoing monitoring activities, evaluations, or a combination of the two"

FINDINGS

Monitoring of the Y2K problem and its resolution is currently inadequate. There are no regular reports or other detailed reporting mechanism in place. The CIO is not independently verifying testing nor reviewing contingency plans.

RECOMMENDATION

The Y2K office must receive regular and rigorous status reports on Y2K compliance progress. Additionally, it must monitor and verify the efficacy of testing and contingency plans.