

# **LBA Special Report Summary:**

Year 2000 Computing Crisis Special Report Update - July 1999

---

This special report evaluates and reports on Year 2000 readiness progress, and continuity and contingency plans for critical functions performed by State agencies since issuing our first report in March 1999. Our earlier report, entitled Year 2000 Computing Crisis Special Report, was presented in March 1999 to the joint Legislative Fiscal Committee. At that time, we found that State agencies had Year 2000 compliance work to complete before they could certify their ability to provide critical government functions dependent upon automated computing, data exchange, and embedded systems. Additionally, we found agencies were deficient in Year 2000 contingency planning. Upon reporting the above findings, we were directed by the joint Legislative Fiscal Committee to provide this update. In addition to updating the reported information regarding Year 2000 compliance of critical State functions, we were specifically directed to include the Department of Corrections, as well as to grade contingency planning for these functions.

## Scope, Objectives, And Methodology

Our analysis utilized the same tier approach as in the March 1999 report. We divided State functions into three tiers depending on their criticality. We defined Tier 1 systems as those related to ensuring the immediate life, health, or safety of the State's residents. Tier 2 systems are those related to providing immediate benefits to the State's residents, which includes wage and benefit payments, and revenue collection for which the State is responsible. Generally, we set a minimum threshold of \$25 million in annual revenue for a system to be included in Tier 2. Finally, Tier 3 systems are those related to agencies performing their missions and maintaining public confidence in the State's government. These missions consist of oversight of entities, regulation and licensing, and several areas of service provision.

We focused our efforts on functions and systems in Tiers 1 and 2 which included 18 State agencies and 50 functions. We conducted on-site interviews with agency personnel and reviewed agency Year 2000 remediation documentation regarding computing, data exchange, embedded systems, and continuity and contingency plans.

According to the Department of Administrative Services, Division of Information Technology Management, the State has adopted the Year 2000 project management methodology used by the federal government. This approach was developed by the federal General Accounting Office and culminates in Year 2000 compliance using the following five phases: awareness, assessment, correction or renovation, validation or testing, and implementation. Letter grades range from "A" through "F" depending upon where the critical function falls within the five-phase conversion model. A similar grading system was developed for continuity and contingency planning efforts based on the General Accounting Office's publication *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*.

## Findings

Our current findings indicate State agencies have made progress since our March 1999 report. While half of the functions can now be considered compliant, there is more work to be done for the remaining functions. We found a great deal of time and effort continues to be spent remediating computing and embedded systems. This is a concern because continuity and contingency planning should now be the focus rather than remediation. Authoritative sources indicate there is not enough time to properly correct and test systems at this late date. More effort needs to be made in developing continuity and contingency plans that will enable critical State functions to operate in the event of computing systems, embedded systems, or infrastructure failure.

Another area of concern is what may be excessive focus on January 1, 2000. Some agencies have tested the roll-over and little else. Many agency continuity and contingency plans assume that date to be the only critical date and develop contingencies based on knowing when a failure will occur. Authoritative sources have noted many other dates that may pose substantial threats to critical functions. Some of these dates are in 1999, such as the beginning of fiscal years and September 9, 1999 and dates beyond the roll-over, such as leap year in 2000 and 2004, and non-leap year dates in 2001. Both Year 2000 remediation plans and continuity and contingency plans should also address these potentialities.

Finally, as noted in our March 1999 report, Year 2000 readiness among the State's critical functions changes regularly. Additionally, agencies appear to be making steady improvements in their continuity and contingency planning efforts. Therefore, readiness is likely to continue to change.