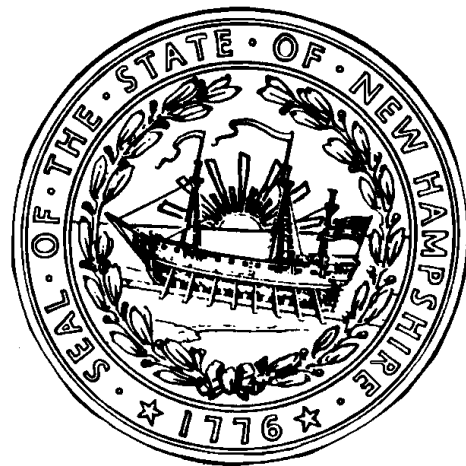


**STATE OF NEW HAMPSHIRE
YEAR 2000 COMPUTING CRISIS**

**SPECIAL REPORT
MARCH 1999**

**Office of Legislative Budget Assistant
107 North Main Street Rm. 102
Concord, NH 03301-4906
(603) 271-3161**



THIS PAGE INTENTIONALLY LEFT BLANK

TO THE FISCAL COMMITTEE OF THE GENERAL COURT:

We have conducted a review of the Year 2000 readiness of New Hampshire State Agencies which provide critical services to the residents of the State to address the recommendation made to you by the Legislative Performance Audit and Oversight Committee.

The purpose of this special project was to evaluate and report on Year 2000 readiness for critical functions performed by State agencies. We were asked to identify and rank critical State functions, evaluate their Year 2000 readiness, as well as contingency planning, and issue a "report card" grading remediation efforts by the agencies responsible for the functions.

This report is the result of our evaluation of the information noted above and is intended for the information of the Fiscal Committee of the General Court. This restriction is not intended to limit the distribution of this report, which upon acceptance by the Fiscal Committee is a matter of public record.

Office of Legislative Budget Assistant
OFFICE OF LEGISLATIVE BUDGET ASSISTANT

March 1999

THIS PAGE INTENTIONALLY LEFT BLANK

**STATE OF NEW HAMPSHIRE
YEAR 2000 COMPUTING CRISIS**

TABLE OF CONTENTS

TRANSMITTAL LETTER	i
1. INTRODUCTION.....	1
1.1 Project Mandate	1
1.2 Findings.....	1
1.3 The Year 2000 Problem.....	1
1.4 Computing Systems	2
1.5 Data Exchange	2
1.6 Embedded Systems	2
2. POTENTIAL IMPACT ON NEW HAMPSHIRE STATE GOVERNMENT.....	5
2.1 New Hampshire's Response To The Year 2000.....	5
2.2 Scope, Objectives, And Methodology.....	6
3. CRITICAL SYSTEMS UNDER STATE CONTROL	9
3.1 Tier 1: Systems Related To The Life, Health, Or Safety Of The State's Residents	9
3.2 Tier 2: Systems Related To Wage And Benefit Payments And Revenue Collection	10
3.3 Tier 3: Systems Related To State Departments Performing Their Missions And Maintaining Public Confidence	11
3.4 Focus On Tier 1 And Tier 2 Functions	11
4. ASSESSING THE STATE'S READINESS FOR THE YEAR 2000	13
4.1 Tier 1 And Tier 2 Agency Responses To DITM Readiness Surveys.....	13
4.2 Defining Year 2000 Compliance	13
4.3 Interviews With Key Agency Personnel	14
4.4 Reviewing Agency Documentation Regarding Progress In Making Computing, Data Exchange, And Embedded Systems Year 2000 Ready	14
4.5 Special Considerations For Embedded Systems.....	15
5. RATING THE STATE'S READINESS FOR THE YEAR 2000.....	17
5.1 Defining The Rating System.....	17
5.2 Setting Critical Dates And Implementing The Rating System	17

TABLE OF CONTENTS (Continued)

6. CONTINGENCY PLANNING FOR COMPUTING, DATA EXCHANGE,
AND EMBEDDED SYSTEMS 23

6.1 The Contingency Planning Process 23

6.2 Evaluating Contingency Plans 25

6.3 Contingency Planning Needs Improvement..... 26

7. CONCLUSION 27

APPENDICES

Critical Testing Dates..... A

Other Agency Responses..... B

Validation And Testing Checklist..... C

Detailed Status Report Of Year 2000 Readiness D

Contingency Planning Compliance Checklist E

LIST OF TABLES

Table 1: State Functions And Systems Related To Ensuring The Immediate Life,
Health, Or Safety Of The State's Residents – Tier 1..... 9

Table 2: State Functions And Systems Related To Providing Immediate Direct
Benefits To State Residents And Revenue Collection Of
Significant Amounts – Tier 2 10

Table 3: Year 2000 Report Card For Critical State Functions - Tier 1 20

Table 4: Year 2000 Report Card For Critical State Functions - Tier 2 21

ABBREVIATIONS

DITM	Division of Information Technology Management
GAO	General Accounting Office
Y2K	Year 2000

STATE OF NEW HAMPSHIRE YEAR 2000 COMPUTING CRISIS

1. INTRODUCTION

1.1 Project Mandate

In November 1998 the joint Legislative Performance Audit and Oversight Committee and the joint Legislative Fiscal Committee directed the LBA Audit Division to: 1) assess information on Year 2000 readiness provided to the Department of Administrative Services, Division of Information Technology Management; 2) identify and rank the State's critical systems; 3) determine whether agencies have developed contingency plans to continue operations should systems fail; and 4) replicate at the State level the Year 2000 "report card" that has been used by the federal government. This quarterly reporting mechanism has been employed by the federal Subcommittee on Government Management, Information, and Technology to rate federal agency progress in becoming Year 2000 compliant. By submitting this special report to the Fiscal Committee in March 1999 we are meeting the deadline requested by the Legislative Performance Audit and Oversight Committee.

1.2 Findings

Our findings indicate that State agencies still have work to do before being able to certify their ability to provide critical government functions which are dependent upon automated computing, data exchange, and embedded systems. We found that a great deal of time and effort has been expended on identifying and remediating computing and data exchange systems. However, documentary evidence for testing and contingency planning is generally insufficient, and not enough attention has been paid to the issue of embedded systems.

1.3 The Year 2000 Problem

The "Year 2000 problem," or "Y2K problem," is most often identified as the inability of computer systems to accurately recognize and calculate dates beginning with January 1, 2000 and beyond. Calculations which require dates in the 21st century will be incorrect and some automated functions may fail to operate.

Potential problems associated with Y2K actually exceed difficulty with calculating dates in the year 2000 and beyond. Additional problem dates, including some in 1999, have been identified (Appendix A). Embedded systems are also problematic. The scope of the Y2K problem increases further when one considers the number of linkages and data exchanges characteristic of many computing systems.

The Year 2000 problem, while technical in nature, is primarily a business problem. If computing and other automated functions fail, even partially, services may be disrupted causing problems for consumers, whether interacting with the government or the private sector.

1. Introduction (Continued)

1.3 The Year 2000 Problem (Continued)

No matter where problems occur, repairing the damage caused by a Year 2000 failure may take anywhere from a few days or less, to weeks or even months. In addition, fixing known problems beforehand often proves to be time and labor intensive.

1.4 Computing Systems

The programming or code behind many computer systems developed prior to the late 1990s used only two digits rather than four to express years; meaning these systems cannot distinguish between the years 1900 and 2000. Therefore, the ability of these systems to accurately calculate dates beginning in the year 2000 is seriously compromised.

Repairing the problem involves assessing the computing hardware, operating systems, and specific program applications. Hardware fixes may include replacing machines or upgrades to components such as internal clocks and Basic Input Output Systems (BIOS). Software repairs may involve rewriting or patching millions of lines of code, or replacing entire applications. Some older applications are written in COBOL (Common Business Oriented Language) or FORTRAN (FORmula TRANslation), first generation programming languages which are not often in current use and may present difficulties with finding programmers who are able to work with them. Repair operations require enormous amounts of time to identify, rewrite or replace, and test.

1.5 Data Exchange

Many computer operated business functions are inter-related. That is, they depend on accurate information exchange, processing, calculations, and run commands between multiple computing systems located both within and external to the organization to properly operate. Repairing one component of a system within an information sharing and processing network is insufficient. For the data exchange system to function properly all hardware and software must be Year 2000 compliant. Data from a non-compliant source may cause otherwise compliant systems to fail. Even inconsistently remediated systems may cause each other to fail in a data exchange environment. State agencies and business entities should be aware of all their internally and externally linked systems and ensure that all essential components receive adequate attention.

1.6 Embedded Systems

Embedded systems are internal electronic devices, often referred to as “chips,” used to control or monitor equipment or machinery. Embedded systems are found in almost all electronic devices. They are commonly found in security systems, fire alarm and sprinkler systems, prison control systems, elevators, automobiles, respirators and defibrillators, telephone systems, and fax machines. The Subcommittee on Government Management, Information, and Technology reports that although many embedded chips are not date-dependent they may still have date-dependent calculations.

1. Introduction (Continued)

1.6 Embedded Systems (Continued)

The Institution of Electrical Engineers (IEE), reports that no one knows how many embedded systems there are or where they are located. Their very nature makes them difficult to identify, access, or test. In many instances it may be more economical to replace non-compliant items.

According to the General Accounting Office, Year 2000-related embedded system failures can be caused by:

- the clock feature not handling the year properly,
- a timer that does not handle the rollover properly, or
- programming in the chip that does not handle the year properly.

The IEE estimates that between one percent and five percent of these systems worldwide will fail to operate properly for the Year 2000 event (between 4 million and 2.5 billion). While the likelihood of failure in a critical device is relatively low, the consequences of a single such failure could be catastrophic.

THIS PAGE INTENTIONALLY LEFT BLANK

STATE OF NEW HAMPSHIRE YEAR 2000 COMPUTING CRISIS

2. POTENTIAL IMPACT ON NEW HAMPSHIRE STATE GOVERNMENT

The Y2K problem could seriously compromise necessary State government functions. Examples of activities that may be affected include financial calculations used in revenue collections, accounts receivable and payable, and benefit determinations and payments, as well as building systems and inventory. Also health, safety, and emergency services are potentially affected.

2.1 New Hampshire's Response To The Year 2000

The Year 2000 problem has been widely recognized within New Hampshire State government. Unfortunately there is no quick fix available for some State agencies. The numerous computing systems operating within State agencies are of varying size, vintage, and complexity. Some agencies maintain multiple independent systems. Some agency applications share space on the same mainframe computer that is owned by yet another agency. In some agencies several independent systems can be accessed by personal computers located in district offices and linked through wide area networks. In other cases, data exchange networks link agencies to financial institutions, the Department of Administrative Services, the State Treasury, as well as to federal, county, and local governments.

Recently, the problems presented by embedded systems have become more widely known. Some State agencies have not adequately considered this problem. From the State's perspective, properly working embedded systems are essential for such items as business and emergency communication systems, vehicles and aircraft, back-up generators, local and wide area networks, and alarm and security systems in State buildings.

Chapter 255 of 1998 Laws of New Hampshire has:

1. Made it the responsibility of management in State agencies to assess Year 2000 readiness and bring essential systems into compliance, devise replacement or contingency plans, and protect systems from contaminated data from non-compliant data exchange partners.
2. Required agencies to develop Year 2000 work plans in accordance with guidelines furnished by the Department of Administrative Services.
3. Mandated full cooperation by State agencies and reporting to the Department of Administrative Services.
4. Required quarterly reporting relative to the Year 2000 problem by the Commissioner of Administrative Services.
5. Allowed the Commissioner of Administrative Services to suspend new computer-related purchases for State agencies until they demonstrate adequate Year 2000 compliance.

2. Potential Impact On New Hampshire State Government (Continued)

2.1 New Hampshire's Response To The Year 2000 (Continued)

As of March 1999, the Commissioner of Administrative Services has issued five quarterly reports through the Division of Information Technology Management (DITM) summarizing the status of Year 2000 compliance by agencies.

The DITM reports demonstrate a wide range of preparedness among agencies. In the January 1999 report only two agencies, the Adjutant General, and the Department of Health and Human Services, reported systems which were in the awareness, or initial, phase of compliance. Fifteen State agencies reported being fully Year 2000 compliant. However, none of the agencies we visited were fully compliant under the criteria we applied.

2.2 Scope, Objectives, And Methodology

The DITM reports provide a basis for assessing the current Year 2000 readiness among State agencies. However, the DITM process relies upon self-reported information from agencies. Although the division provided guidelines for agencies regarding the reporting format and defining Year 2000 project phases, DITM did not verify the agency self-reported information. The Legislature has decided to require such verification, which is the purpose of this special report.

The methods we used to evaluate the State's response to the Year 2000 problem included:

- background research into the problem utilizing both government and private sector information sources;
- reviewing agency reports to DITM regarding Year 2000 remediation efforts, as well as agency Information Technology Plans;
- identifying and categorizing critical state functions;
- conducting on-site interviews with agency personnel and reviewing agency Year 2000 remediation documentation regarding computing, data exchange, embedded systems, as well as contingency planning efforts; and
- following up with agency personnel by submitting memoranda to verify and confirm our understanding and judgement of their Year 2000 readiness.

In conducting our fieldwork, we sought to answer two main questions regarding how well agencies were prepared to meet the Year 2000 problem. The first question addressed agency remediation efforts, while the second question addressed agency planning to manage Year 2000 failures:

1. *Have State agencies sufficiently validated and tested their computing, data exchange, and embedded systems for Year 2000 compliance?*

2. Potential Impact On New Hampshire State Government (Continued)

2.2 Scope, Objectives, And Methodology (Continued)

2. *Have State agencies prepared, tested, and validated comprehensive business continuity and contingency plans to ensure the continued delivery of critical services to citizens regardless of unforeseen, unanticipated, or unpredictable failures of information technology, embedded, or external systems and infrastructure associated with the Year 2000 issue?*

Based on our analysis of the interview information and remediation documentation, we developed a grading system for the Year 2000 readiness of the State's critical functions. The grading system was adapted from the federal Subcommittee on Government Management, Information, and Technology and is found in Section 5 of this report.

THIS PAGE INTENTIONALLY LEFT BLANK

**STATE OF NEW HAMPSHIRE
YEAR 2000 COMPUTING CRISIS**

3. CRITICAL SYSTEMS UNDER STATE CONTROL

When identifying how to proceed with addressing and repairing the Year 2000 problem, much of the literature focuses on identifying so-called mission critical systems, or those necessary to keeping an entity's functions operating. This approach makes sense from the perspective of a single entity. However, the State has a myriad of responsibilities to its residents and the functions it performs are numerous. As a result, identifying the State's critical functions, as well as the automated systems supporting those functions, appears to provide more value to policy makers than the basic agency-exclusive mission critical approach. Therefore, we developed criteria for ranking the State's most critical functions and identifying the systems required to fulfill those functions.

3.1 Tier 1: Systems Related To The Life, Health, Or Safety Of The State's Residents

We defined Tier 1 systems as those related to ensuring the immediate life, health, or safety of the State's residents. The State provides several services in these areas (Table 1). The functions of the systems identified for Tier 1 are related to emergency services without which the life, health, or safety of residents could be placed in immediate danger or risk.

Table 1

State Functions And Systems Related To Ensuring The Immediate Life, Health, Or Safety Of The State's Residents - Tier 1

Department/Agency	Function
Adjutant General	Emergency Response and Disaster Recovery
Administrative Services	Enhanced 9-1-1
Environmental Services	1) Hazardous Waste Management 2) Dam Operations
Fish and Game	Search and Rescue
Governor's Office of Emergency Management	1) Telecommunications 2) Emergency Alert System
Health and Human Services	Emergency Medical Devices
Safety	1) Criminal History 2) Radio Communications 3) State Police Ground Vehicles 4) State Police Aircraft
Transportation	1) Ground Traffic Safety 2) Air Navigation Safety 3) Highway Maintenance

Source: LBA analysis.

3. Critical Systems Under State Control (Continued)

3.2 Tier 2: Systems Related To Wage And Benefit Payments And Revenue Collection

We defined Tier 2 systems as 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. The functions of these systems include processing and distributing welfare and other support benefits, the State payroll, unemployment compensation, retirement benefits, and revenue collection (Table 2). Generally, we set a minimum threshold of \$25 million in annual revenue for a system to be included in Tier 2.

Table 2

State Functions And Systems Related To Providing Immediate Direct Benefits To State Residents And Revenue Collection Of Significant Amounts - Tier 2

Department/Agency	Function
Administrative Services	1) State Accounting 2) State Personnel Management 3) General Services
Employment Security	1) Unemployment Compensation 2) Unemployment Tax Collection 3) Mail Operations
Governor's Energy Office	Fuel Assistance
Health & Human Services	1) Child Abuse/Neglect Management and Claims 2) Eligibility Determination 3) Child Support Enforcement 4) Medicaid 5) Women, Infants, and Children 6) Mailing System 7) Networks
Insurance	Revenue Collection
Liquor Commission	1) Revenue Collection 2) Store Operations
Retirement System	Annuity Payments
Revenue Administration	Revenue Collection
Safety	1) Motor Vehicle Financial System 2) Road Toll Collection (Gas Tax)
Sweepstakes Commission	Revenue Collection
Transportation	Turnpike Toll Collection
Treasury	1) Investment and Debt Management 2) Cash Management 3) General Fund Distribution

Source: LBA analysis.

3. Critical Systems Under State Control (Continued)

3.3 Tier 3: Systems Related To State Departments Performing Their Missions And Maintaining Public Confidence

We defined Tier 3 systems as 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.

Examples of these functions include various professional licensing boards, the Pari-Mutuel Commission, and the Bank, Real Estate, and Human Rights Commissions. Also in Tier 3 are other functions performed by the Adjutant General, the Liquor Commission, and the departments of Administrative Services, Employment Security, Labor, Health and Human Services, Revenue Administration, Safety, Transportation, and Fish and Game that do not fall into Tiers 1 or 2. Most functions within the departments of Corrections, Education, Environmental Services, Highway Safety, Insurance, Resources and Economic Development, and Youth Development Services are in Tier 3.

3.4 Focus On Tier 1 And Tier 2 Functions

Given the report date for this special project was March 1999, we focused our efforts on functions and systems in Tiers 1 and 2. During our fieldwork we visited 16 State agencies and reviewed Year 2000 readiness for computing, data exchange, and embedded systems for 41 functions. In addition, we received a letter from the Public Utilities Commission regarding its role in ensuring Year 2000 compliance among utility companies in the State, as well as letters from the New Hampshire Veterans Home and the Department of Corrections, regarding security and health care issues within their facilities (Appendix B). We chose to communicate with the Public Utilities Commission by letter because of its regulatory authority regarding utility companies, and the need for the public to be assured of uninterrupted service after January 1, 2000. We contacted the Department of Corrections and the Veterans Home by mail because we had previously received information regarding automated security and medical devices which we wished to verify.

THIS PAGE INTENTIONALLY LEFT BLANK

STATE OF NEW HAMPSHIRE YEAR 2000 COMPUTING CRISIS

4. ASSESSING THE STATE'S READINESS FOR THE YEAR 2000

According to the Division of Information Technology Management (DITM) 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 (GAO) and culminates in Year 2000 compliance using the following five phases:

- 1) *Awareness*, the entity is aware of Year 2000 issues and has executive level support.
- 2) *Assessment*, core systems have been identified, systems have been inventoried, analyzed, and prioritized for correction, contingency plans exist, and resources have been committed.
- 3) *Correction or Renovation*, systems have been converted, replaced or retired.
- 4) *Validation or Testing*, corrected systems have been tested for compliance and program modifications have been tested.
- 5) *Implementation*, corrected systems have been put into production, users have been trained, and documentation has been updated.

To assess the readiness of the functions and systems identified as being in Tier 1 and Tier 2, we reviewed agency responses to DITM readiness surveys and interviewed key agency personnel. Wherever possible, we also reviewed documentation supporting the agency's self-reported Year 2000 readiness and compliance.

4.1 Tier 1 And Tier 2 Agency Responses To DITM Readiness Surveys

As indicated earlier, DITM has issued five quarterly reports on Year 2000 readiness for State agencies. These documents identify the agencies' self-reported current Y2K phase for the systems supporting critical State functions. For the functions in Tier 1 and Tier 2 we began by reviewing the agency's self-reported Year 2000 status submitted to DITM. We examined additional documentation at the DITM office, where available, particularly agency Information Technology Plans and Year 2000 Work Plans. We used these information sources to familiarize ourselves with the systems supporting the critical functions and to determine what level of compliance we might find.

4.2 Defining Year 2000 Compliance

To assess Year 2000 readiness, or compliance, we selected a working definition that includes all aspects of the Year 2000 problem. We believe this definition meets the criteria identified by the GAO report, "Year 2000 Computing Crisis: A Testing Guide," published in November 1998. The definition we used was quoted from a June 1998 publication by the California Department of Information Technology entitled "California 2000 White Paper External Interfaces." According to this publication:

4. Assessing The State's Readiness For The Year 2000 (Continued)

4.2 Defining Year 2000 Compliance (Continued)

(T)he term Year 2000 compliant is defined as the capability of a system, component, or product to perform its intended function or functions without interruption, malfunction, or performance degradation, including the loss, corruption or generation of inaccurate data as a result of internal date/time computations relating to the transition from years 1999 to 2000 and beyond, and including computations relating to the occurrence of leap years.

4.3 Interviews With Key Agency Personnel

Each agency site visit included interviews with key agency personnel. These structured interviews were designed to:

- 1) define our mandate from the Legislature and the scope of our review,
- 2) discuss and clarify functions which we identified as Tier 1 and Tier 2,
- 3) discuss and clarify the agency's self-reports to DITM, and
- 4) establish the existence of documentation needed to verify self-reported readiness and contingency planning.

For the purpose of these interviews, the term key agency personnel was defined as meaning the chief information technology employee and the Year 2000 coordinator (if not the same person) for the agency. These personnel at a minimum were expected to participate in the interview. Other agency personnel, such as the department commissioner, division or bureau director, or other agency-identified key personnel, were also invited to participate in the interview at their discretion.

4.4 Reviewing Agency Documentation Regarding Progress In Making Computing, Data Exchange, And Embedded Systems Year 2000 Ready

The self-reported readiness status of an agency's critical functions determined the content of the documentation we sought and the level of review we conducted for the systems supporting those functions. In all cases we looked for documentation indicating the agency had considered computing, data exchange, and embedded systems. For all Tier 1 or Tier 2 functions, no matter which phase the agencies reported, we also looked for contingency plans detailing how the agency will continue operation should computing, data exchange, or embedded systems fail. For agencies claiming that their systems were in the assessment or corrections phase we sought documentation supporting those claims. We also were particularly interested in when those agencies estimated they would become Year 2000 compliant.

Of primary concern to our review were those systems which were claimed to be Year 2000 compliant, or were in the testing or implementation phases. For these systems, we sought complete supporting documentation in one or more of the following formats:

- test plans, criteria, and results;
- unqualified vendor certifications; or

4. Assessing The State's Readiness For The Year 2000 (Continued)

4.4 Reviewing Agency Documentation Regarding Progress In Making Computing, Data Exchange, And Embedded Systems Year 2000 Ready (Continued)

- unqualified written statements or letters from independent testing firms/contractors.

To verify and validate sufficient agency testing for Year 2000 compliance, we expected to find agencies maintaining detailed documentation on testing procedures, testing criteria, and testing results for each test phase. Verification was based on an agency being able to provide evidence it had successful validation and testing results. We developed a compliance checklist to determine which steps of the validation and testing phase an agency had completed (Appendix C). The checklist was developed using GAO documents as well as from information obtained from the DITM.

4.5 Special Considerations For Embedded Systems

An important consideration for embedded systems is remediation. Often embedded systems can not be reprogrammed. In general, the most practical option is to upgrade or replace critical devices. To establish whether agencies had adequately considered the issue of embedded devices, we sought to answer the following questions:

- Is management aware of the embedded systems issue and identified all agency equipment with embedded systems?
- How does management plan to resolve Year 2000 embedded system problems?
- Are new equipment purchases being examined for Year 2000 compliance in their embedded systems?

THIS PAGE INTENTIONALLY LEFT BLANK

STATE OF NEW HAMPSHIRE YEAR 2000 COMPUTING CRISIS

5. RATING THE STATE'S READINESS FOR THE YEAR 2000

The Legislature has requested a "report card" or grading system, as one of the products of this project. To that end, we have used a modified version of the report card model developed for the U.S. Congress. Our report card grades critical State functions in Tier 1 and Tier 2 as of February 26, 1999. We chose this date as it represents the last day of our fieldwork for this special project and it was the last date we accepted additional documentation from agencies. However, it should be noted that the grades we assigned to the different functions should change as time progresses. We expect that the level of Year 2000 compliance will increase throughout the remainder of 1999.

5.1 Defining The Rating System

The report card approach used at the federal level assigns letter grades "A" through "F" to agencies as a whole. The federal Subcommittee on Government Management, Information, and Technology uses the Office of Management and Budget-designated date of March 1999 (six months prior to the beginning of federal fiscal year 2000) as the deadline for agency Year 2000 compliance. The latest "report card," issued February 22, 1999, grades federal agencies according to the level of compliance among mission critical systems on February 12, 1999.

Our report card departs from the federal model in certain key respects. First, we rated critical State functions, not entire agencies. Second, our prime date was set as July 1, 1999, the actual beginning date of the State's fiscal year 2000. Third, letter grades were assigned according to which phase of remediation the agency could document that a function was in as of the writing of this report. The term "phase of remediation" refers to the five-phase GAO model presented on page 13 of this report.

5.2 Setting Critical Dates And Implementing The Rating System

From the State's perspective, the year 2000 comes six months in advance of the calendar year. That is because State fiscal year 2000 begins July 1, 1999. For that reason we have set that date as the critical date for which the systems supporting the State's critical functions must be ready. Our "report card" awards an "A" grade only to those functions whose computing, data exchange, and embedded systems can be sufficiently documented to be Year 2000 compliant by that date. Due to the wholesale inadequacy of contingency planning as reported in the previous section, we have not included contingency plans as part of the grading system.

Information technology personnel in several agencies stated that their systems would be compliant by July 1, 1999. We have no reason to doubt what agency personnel reported to us regarding their remediation efforts. However, we could not accept verbal statements alone as verification of Year 2000 compliance, and the critical functions in these agencies were not awarded an "A" grade without written documentation. Likewise, we accepted

5. Rating The State's Readiness For The Year 2000 (Continued)

5.2 Setting Critical Dates And Implementing The Rating System (Continued)

vendor or manufacturer certifications as documentary evidence of compliance, but without documentation of prudent in-house testing, we did not award a full grade for the system.

Similar to the federal report card and grading model, our letter grades range from "A" through "F" depending upon where the critical function falls within the five-phase conversion model. Our evaluation of Year 2000 readiness and the resulting grades are shown on Tables 3 and 4. As the grades indicate, there are many Tier 1 and Tier 2 functions still need additional work. More detail regarding the Year 2000 remediation status of the systems supporting each critical function, as well as other agency systems, may be found in Appendix D. We recommend readers of this report review Appendix D, as it represents our understanding of the level of Year 2000 remediation that could be adequately documented for each critical function. The information in Appendix D also has been reviewed, verified, and concurred with by the agencies responsible for these critical functions, unless otherwise noted in an agency response.

Some critical functions we reviewed were not dependent upon automated systems. These functions include dam operations and hazardous waste management (both Tier 1) within the Department of Environmental Services, emergency medical devices (Tier 1) within the Department of Health and Human Services, air navigation safety within the Department of Transportation (Tier 1), and revenue collection (Tier 2) by the Insurance Department. For these functions, no letter grade has been applied.

For all other functions, the letter grade as of February 26, 1999, was dependent strictly upon the function's Year 2000 remediation phase. The grade for each function represents the least compliant phase of any system supporting the function. Therefore, it is possible for a function to receive a lower grade because only one system is at a lower stage of remediation than all the others; for example, the Enhanced 9-1-1 function systems are compliant except for telephone systems. In these cases the letter grade may be expressed as a "+" rather than as a whole grade. In addition, functions close to moving into the next phase of remediation also received a "+" rather than a whole grade.

Functions reported and sufficiently documented to be compliant earned a base grade of "A" unless there was reason to modify the grade. Therefore, the only three functions reported and sufficiently documented as compliant – unemployment compensation under Employment Security, and revenue collection under the Liquor Commission and the Department of Revenue Administration – received grades of "A-" because the agencies had not conducted complete independent testing of the systems as of February 26, 1999. The Department of Employment Security reports the unemployment compensation system will be independently tested by June 21, 1999. The Liquor Commission accepted vendor certification but did not independently test its financial management system. Likewise, the Department of Revenue Administration did not independently test the vendor-certified minicomputer and operating system for its Tax Information Management System.

5. Rating The State's Readiness For The Year 2000 (Continued)

5.2 Setting Critical Dates And Implementing The Rating System (Continued)

Functions reported and documented to be in testing or implementation phases earned a "B" grade. Documentation for the two functions in this category, unemployment tax collection and child abuse/neglect management and claims, supports a reasonable expectation that each will be Year 2000 compliant by July 1, 1999.

Functions reported and documented to be in the correction phase earned a grade of "C." Several of these systems – the New Hampshire Integrated Financial System and Enhanced 9-1-1 under the Department of Administrative Services, the emergency alert system, two functions under the Department of Health and Human Services, store operations under the Liquor Commission, revenue collection under the Sweepstakes Commission, and ground traffic safety and turnpike toll collection under the Department of Transportation – could be Year 2000 compliant by July 1, 1999, assuming that corrective measures and subsequent testing and implementation occur with few complications.

Functions reported and documented to be in the assessment phase earned a "D" grade, while those that were in the awareness phase received an "F." Once again, the detail provided in Appendix D will show why these grades were assigned to the functions listed on Tables 3 and 4.

5. Rating The State's Readiness For The Year 2000 (Continued)

5.2 Setting Critical Dates And Implementing The Rating System (Continued)

Table 3

Year 2000 Report Card For Critical State Functions - Tier 1

Agency	Manual	Awareness	Assessment	Correction	Testing	Implementation	Compliant	Grade	Agency's Estimated Completion Date
Adjutant General									
Emergency Response and Disaster Recovery			✓					D	October 1999
Administrative Services									
Enhanced 9-1-1			✓					C+	April 1999 ¹
Environmental Services									
Hazardous Waste Management	✓							†	N/A
Dam Operations	✓							†	N/A
Fish and Game									
Search and Rescue						✓		A	N/A
Governor's Office of Emergency Management									
Telecommunications			✓					D+	Unknown
Emergency Alert System						✓		A-	Unknown
Health and Human Services									
Emergency Medical Devices	✓							†	N/A
Safety									
Criminal History			✓					C	March 1999 ²
Radio Communications						✓		A	N/A
State Police Ground Vehicles						✓		A	N/A
State Police Aircraft		✓						F	Unknown
Transportation									
Ground Traffic Safety			✓					C+	Unknown
Air Navigation Safety	✓							†	N/A
Highway Maintenance				✓				C	Unknown

¹No grade awarded, manual system
Source: LBA analysis of agency data.

See Page 22 for footnotes.

5. Rating The State's Readiness For The Year 2000 (Continued)

5.2 Setting Critical Dates And Implementing The Rating System (Continued)

Table 4

Year 2000 Report Card For Critical State Functions - Tier 2

Agency	Manual	Awareness	Assessment	Correction	Testing	Implementation	Compliant	Grade	Agency's Estimated Completion Date
Administrative Services									
State Accounting			✓					C+	June 1999 ³
State Personnel Management			✓					C+	June 1999 ³
General Services			✓					C+	June 1999
Employment Security									
Unemployment Compensation						✓		A-	June 1999
Unemployment Tax Collection				✓				B+	June 1999
Mail Operations		✓						D	Unknown
Governor's Energy Office									
Fuel Assistance		✓						D+	March 1999
Health and Human Services									
Child Abuse/Neglect Management and Claims				✓				B+	May 1999
Eligibility Determination			✓					C+	June 1999
Child Support Enforcement			✓					C	September 1999
Medicaid			✓					C	June 1999
Women, Infants, and Children			✓					C	Unknown
Mailing System						✓		A	N/A
Network			✓					C+	July 1999 ⁴
Insurance									
Revenue Collection	✓							†	N/A
Liquor Commission									
Revenue Collection						✓		A-	N/A
Store Operations			✓					C+	June 1999
Retirement System									
Annuity Payments			✓					C	May 1999 ⁵
Revenue Administration									
Revenue Collection						✓		A-	August 1999
Safety									
Motor Vehicle Financial System		✓						D	June 1999 ⁶
Road Toll Collection (Gas Tax)			✓					C	May 1999
Sweepstakes Commission									
Revenue Collection			✓					C+	June 1999 ⁷
Transportation									
Turnpike Toll Collection			✓					C+	June 1999 ⁸
Treasury									
Investment and Debt Management		✓						D+	June 1999
Cash Management		✓						D+	June 1999
General Fund Distribution		✓						D	June 1999

†No grade awarded, manual system
 Source: LBA analysis of agency data.

See Page 22 for footnotes.

5. Rating The State's Readiness For The Year 2000 (Continued)

5.2 Setting Critical Dates And Implementing The Rating System (Continued)

Footnotes To Tables 3 and 4

¹ Bureau of Emergency Communications reports its systems will be Year 2000 compliant by April 1999. However, Bell Atlantic reports it will not complete critical system renovation efforts until June 1999. Therefore, the earliest the Enhanced 9-1-1 function could be fully compliant is June 1999.

² The Department of Safety reports that its criminal history application will be compliant by March 1999. The agency also reports network routers will not be replaced until May 1999 and that personal computers are not scheduled for purchase until State fiscal year 2000. Therefore, the earliest the department's criminal history function, which relies on the network, could be fully compliant is sometime in State fiscal year 2000.

³ Financial Data Management reports the Integrated Financial System (IFS) will be compliant by June 1999 and the Government Human Resources System (GHRS) will be compliant by December 1999. Components of GHRS that use the State fiscal year will be compliant by June 1999 according to the agency.

⁴ The Department of Health and Human Services (DHHS) reports that its routers will be compliant in February 1999. They also report that personal computers used in the network will not be fully compliant until July 1999. Therefore, the earliest the DHHS network will be fully compliant is July 1999.

⁵ The New Hampshire Retirement System reports that the mainframe annuity payroll relies on will be compliant by May 1999. The application for annuity payroll does not have a determined date of compliance, however. Therefore, a date for full compliance of the annuity payroll function can not be determined.

⁶ The Department of Safety reports that motor vehicle licensing and registration will be compliant by June 1999 but also reports that some testing will last until July 1999. Therefore, the earliest that the function could be fully compliant is July 1999.

⁷ The Sweepstakes Commission reports that their systems will be compliant by June 1999. However, the agency has established August 1999 as the completion date for renovating any minor noncompliant elements. Therefore, the revenue collection function may not be fully compliant until August 1999.

⁸ The Department of Transportation reports its turnpike toll collection system will be compliant by June 1999. However, the agency does not plan to complete the replacement of its non-compliant personal computers (PCs) until December 1999. Therefore, the earliest the turnpike toll collection function will likely be fully compliant is December 1999 as they rely on these PCs.

STATE OF NEW HAMPSHIRE YEAR 2000 COMPUTING CRISIS

6. CONTINGENCY PLANNING FOR COMPUTING, DATA EXCHANGE, AND EMBEDDED SYSTEMS

The Year 2000 problem, while technical in nature, is primarily a business problem and the responsibility of senior management. Agencies are generally attempting to ensure functions critical to the citizens of the State are ready for the challenges of Year 2000 and beyond. However, at any stage of Year 2000 compliance some functions could still fail to provide important State services. Correction efforts that were not well underway by fall 1998 may not be completed in time. This includes correction plans that rely on replacement hardware, as well as repairs to operating systems and program application software. Additionally, renovated and tested systems thought to be compliant may still encounter unanticipated Year 2000 problems from internal and external sources.

Agencies should be actively addressing ways to reduce the risk and potential impact of Year 2000-induced failures on their essential functions through rigorous business continuity planning. Every agency needs to ensure the continuity of essential functions by identifying, assessing, managing, and mitigating Year 2000 risks. As good business management practices, agencies should already have business continuity plans in place to address all types of failure from natural and man-made disasters. As such, continuity and contingency planning is a major part of any Year 2000 effort. It is perhaps the most difficult aspect of solving the Year 2000 problem because it involves a disciplined investigation into all aspects of an agency's operations to locate those points where significant risk can occur which could affect critical State functions.

This effort can not be limited to the risks posed by the Year 2000-induced failures of internal information systems, but must include the potential Year 2000 failures of others, including data exchange and business partners, as well as infrastructure service providers such as power, water, transportation, and voice and data telecommunications. Due to the difficulty of testing embedded systems, the best means to address the Year 2000 problem for embedded systems is to develop contingency plans so that critical functions can be maintained even if vital equipment fails. One weak link in the chain of critical dependencies and even the most successful Year 2000 program will fail to protect against major disruption of essential functions.

6.1 The Contingency Planning Process

We found that many federal and other states' agencies had adapted business continuity planning, contingency planning, and risk management to address the Year 2000 problem. In general, the primary objectives of a continuity and contingency plan are:

- to provide the agency with a tested vehicle which, when executed, will permit an efficient, timely resumption of the interrupted business operations;
- to ensure the continuity of the organization's business;

6. Contingency Planning For Computing, Data Exchange, And Embedded Systems (Continued)

6.1 The Contingency Planning Process (Continued)

- to minimize the inconvenience and potential disruption to customers and clients; and
- to minimize the impact to the agency's public image.

This planning process transcends information technology systems and encompasses all aspects of an agency's operation.

In the context of a Year 2000 program, the business continuity plan includes a risk mitigation strategy, contingencies, and recovery procedures, to ensure the organization's business processes continue in spite of disruptions to infrastructure and/or support systems.

Contingency plans are an element of continuity planning. Federal and other states' contingency plans are focused on ensuring the continuity of a system in the event of the loss or degradation of essential resources such as mission critical software, a computer system, local area and wide area network connectivity, or other communications device or interface. These contingency plans necessarily describe the steps the agency would take, including the activation of manual or contract processes, to ensure the continuity of its business processes due to a Year 2000 system failure.

These plans also recognize the duality of contingency planning. First, the need for contingency planning during Year 2000 renovation activities to focus on alternatives to control developmental risk. Second, during the operational phase to focus on addressing viable alternatives to overcome an unexpected, unanticipated, or unpredictable failure.

Agencies need to tailor their Year 2000 business continuity planning efforts in response to their unique needs within their business environment to achieve necessary results in the most cost efficient manner. These plans emphasize dealing with the consequences rather than with the causes of failures. Contingency planning is also concerned with the effects of failures that are beyond the control of the agency, including failures on the part of business partners and public infrastructure.

Testing the contingency plan to ensure that all the processes will work in the event of an emergency is required. Agencies and departments need to ensure they are capturing the essential aspects of their critical processes and have a way to recover them from a disruption when normal conditions return. Comprehensive and detailed work-around plans should be developed, documented, tested, and placed in pre-defined accessible areas in anticipation of the day they will be needed. Necessarily, plans must be rehearsed and well understood by all members of an agency.

The primary value of continuity and contingency planning is that planning has taken place before the crisis, maximizing time by identifying alternatives in a non-crisis mode. Contingency planning is a proactive effort.

6. Contingency Planning For Computing, Data Exchange, And Embedded Systems (Continued)

6.1 The Contingency Planning Process (Continued)

GAO and several states conclude that due to the risks posed by the Year 2000 problem, agencies must have business continuity and contingency plans to ensure continuity of services. Planning safeguards an agency's ability to produce a *minimum acceptable level* of outputs and services in the event of failures of internal or external mission critical information systems and services. It also links risk management and mitigation efforts to the agency's Year 2000 program and helps to identify alternate resources and processes needed to operate the agency core business processes.

According to GAO, risk management is "[a] management approach designed to prevent and reduce risks, including system development risks, and lessen the impact of their occurrence." Business continuity and contingency planning links risk management and mitigation efforts to the agency's Year 2000 program, and helps to identify alternate resources and processes needed to operate the agency's essential business functions. Risk management focuses on maintaining critical government operations and minimizing exposure to consequences. The way to manage risks is to first identify them, evaluate their potential consequences, and, if possible, find a way to avoid them.

6.2 Evaluating Contingency Plans

As indicated earlier, we sought contingency plan documentation for all the systems we reviewed that are related to critical functions. We expected, as recommended by the GAO, that even critical functions with systems reported to be Year 2000 compliant would have contingency planning documents in place to safeguard against unforeseen system failures.

Because no one can predict which embedded systems will fail, it is imperative for management to develop and implement contingency plans for critical embedded systems as well. Agency contingency plans were reviewed to determine whether devices with embedded systems had been included.

Using GAO standards as a baseline, we developed a compliance checklist to assess agency business continuity and contingency plans for the State's Tier 1 and Tier 2 functions (Appendix E). The checklist was used to help assess:

- 1) initiation processes,
- 2) business impact processes,
- 3) contingency planning processes, and
- 4) testing processes.

We also integrated industry standard risk management processes to ensure they were applied to the agencies' efforts.

6. Contingency Planning For Computing, Data Exchange, And Embedded Systems (Continued)

6.3 Contingency Planning Needs Improvement

Unfortunately, the level of contingency planning we encountered was far less than our expectations. Although we received from several agencies written “contingency” plans, disaster recovery plans, and other documents, nothing we received met the standards recommended by the GAO or our compliance checklist. As a result, we have concluded that insufficient attention has been paid to the business continuity and contingency planning concept as a whole.

There were some notable exceptions to the above general statements. For example, the Department of Employment Security has a federal Department of Labor-approved contingency plan for the unemployment benefits system. This plan was developed under federal guidelines, however, the GAO standards appear to impose a higher level of planning effort than the federal Department of Labor. For that reason we concluded the unemployment benefits contingency plan was insufficient. Likewise, the Liquor Commission presented a draft contingency plan that met most of the standards on our checklist. This plan was probably the most complete of any that we reviewed. However, the manual procedures for store operations the agency relies upon for business continuity were not completely documented and the plan had not been approved by the commission as of February 26, 1999. If the commission remains on course with the plan’s development, it could serve as a model for other agencies to follow. Finally, the Department of Revenue Administration submitted its disaster recovery plan, which it maintains is sufficient for “department wide daily deposit Year 2000 problems.” The department reported using the disaster recovery plan on occasion when computer systems were unavailable. Our position is that while the department’s disaster recovery plan may appear to encompass Year 2000 issues, the GAO contingency planning standard and our checklist indicated several areas that are not addressed. As a result, the department’s disaster recovery plan in our opinion did not qualify as a Year 2000 contingency plan.

We believe all agencies providing critical State functions should have Year 2000-specific contingency plans regarding each critical function for which the agency is responsible. These plans should be developed with the guidance and involvement of top agency management.

**STATE OF NEW HAMPSHIRE
YEAR 2000 COMPUTING CRISIS**

7. CONCLUSION

As a result of this special project, the Legislature should now be aware of the current status of Year 2000 readiness among the State's critical functions. We found a few agencies were very close to Year 2000 readiness for their critical functions, but many others still have a great deal of work to do. We also found contingency planning efforts need to be markedly improved across the board. Finally, it appears to us that more direct guidance and coordination among agencies should be coming from a centralized source. We believe that this centralized source should have the responsibility and resources to review documentation regarding agency remediation efforts, as well as actively assist agencies in contingency planning, particularly those agencies which are likely not to have their critical functions compliant by the critical date.

It must be emphasized that the level of Year 2000 readiness among the State's critical functions changes weekly. Therefore, the grade we reported for several functions may change for the better as the critical date of July 1, 1999 approaches. As such, the centralized source recommended above should keep the Legislature apprised of changes in Year 2000 readiness for critical functions.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

CRITICAL TESTING DATES

SOURCE: U.S. Army Year 2000 Project Office, via the Internet at http://www.army.mil/army-y2k/Testing_Dates.htm.

Date	Problem
January 1, 1999	Ensure that the digits "99" do not trigger a red flag, other program subroutine(s), or cause a processing error for business and industry.
July 1, 1999	First day of State fiscal year 2000
August 22, 1999	Overflow of "end of week" rollovers (e.g. GPS)
September 9, 1999	(9/9/99 or possibly 9999) - ensure that the digits "99" or "9999" do not trigger a red flag, other program subroutine(s), or cause a processing error
October 1, 1999	First day of federal fiscal year 2000
January 0, 2000	Ensure that this date is NOT processed (some applications do have this problem and counts January 0 as the day before the 1st)
January 1, 2000	Key date in any compliance testing
January 3, 2000	First full work day in the new year
January 10, 2000	First 7 character date
February 28, 2000	Ensure the leap year is being properly accounted for
February 29, 2000	Ensure the leap year is being properly accounted for
February 30, 2000	Ensure that this date is NOT processed
February 31, 2000	Ensure that this date is NOT processed
March 1, 2000	Ensure date calculations have taken leap year into account
October 10, 2000	First 8 character date
December 31, 2000	366th day of the year
January 1, 2001	First day in the 21st Century
February 29, 2001	Ensure that this date is NOT processed as a leap year
After January 1, 2002	Ensure no processing errors occur in backward calculations and processing of dates in the 1980s and the 1990s at this point in time
February 29, 2004	Ensure that this date is processed as a leap year
January 1, 2010	Overflow ANSI C Library
September 30, 2034	Overflow of Unix time function
January 1, 2037	Rollover date for NTP systems
January 19, 2038	Overflow of Unix systems
September 18, 2042	Overflow of IBM System/360
February 28, 2100	Last day of February - NOT a leap year

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B
OTHER AGENCY RESPONSES

STATE OF NEW HAMPSHIRE



CHAIRMAN
Douglas L. Patch
COMMISSIONERS
Susan S. Geiger
Nancy Brockway

PUBLIC UTILITIES COMMISSION
8 Old Suncook Road
Concord, N.H. 03301-7319

EXECUTIVE DIRECTOR
AND SECRETARY
Thomas B. Getz
TDD Access: Relay NH
1-800-735-2964
Tel. (603) 271-2431
FAX No. 271-3878

February 3, 1999

Ms. Catherine A. Provencher
Director of Audits
Office of Legislative Budget Assistant
State House, Room 102
Concord, NH 03301

Re: Year 2000 Preparedness

Dear Ms. Provencher:

The Public Utilities Commission has been involved with Year 2000 (Y2K) issues as they affect regulated utilities in New Hampshire for some time on a variety of levels. For example, the Engineering Division has informally monitored industry developments and in August, 1997 notified utilities of a concern with embedded software and required utilities to examine how date-sensitive embedded software could affect operations. Subsequently, in March, 1998, the Commission initiated a formal investigation of utility Y2K issues generally and opened Docket No. IR 98-039.

As part of IR 98-039, the Commission directed each utility to file by April 1, 1998 a memorandum explaining how Y2K issues would affect its ability to provide safe and reliable service. In addition, the Commission required each utility to explain how it intended to ensure that service would be maintained. To assist the Commission in the review of utility plans and implementation efforts, a nationally recognized consultant specializing in utility related Y2K issues was engaged.

Mr. Rick Cowles and Cyberservices America were hired to conduct an investigation and issue a series of reports. The first report will review the adequacy of utility plans and is due during the first week of March, 1999. The second report is due during the first week of June and will examine utility efforts to implement the plans. The final report, due the first week of September, 1999, will examine overall levels of preparedness including contingency planning.

Most recently, Governor Shaheen has issued an Executive Order creating a Task Force on Y2K issues. Commission Chairman Douglas Patch was named Co-Chairman of the Task Force

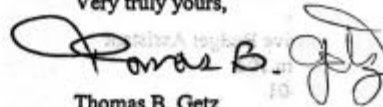
Appendix B - Other Agency Responses (Continued)

Ms. Catherine A. Provencher
February 3, 1999
Page two

along with Mr. Fred Kocher from the High Technology Council. The goal of the task force is to heighten awareness of Y2K issues and to encourage ongoing efforts to assure that State systems and critical infrastructure are prepared with respect to those issues.

If you have any additional questions, please do not hesitate to call me or Ms. Kate Bailey, Assistant Chief Engineer, at 271-2431.

Very truly yours,

A handwritten signature in black ink, appearing to read "Thomas B. Getz". The signature is stylized with a large, looping initial "T" and a cursive "G".

Thomas B. Getz
Executive Director & Secretary



Barry E. Conway
Commandant

New Hampshire Veterans Home

P.O. Box 229, 139 Winter Street
Tilton, New Hampshire 03276-0229



February 3, 1999

Telephone 603-286-4412
FAX # 286-2416

Catherine A. Provencher
Director of Audits
Office of Legislative Budget Assistant
State House, Room 102
Concord, NH 03301

Dear Ms. Provencher:

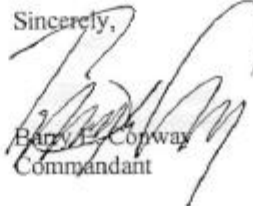
In response to your inquiry regarding the Veterans Home's readiness for the Year 2000, we offer the following responses to your questions:

1. Should electric power go off due to a Year 2000-related problem, what happens to the secure areas of the Veterans Home? *The Home has a generator with emergency outlets throughout the building which come on automatically within 5-10 seconds of a power failure. The generators are checked weekly and put into service for 20 minutes to test their output.*
2. Do secure areas that are automated default to a locked or unlocked position in the event of a failure in the automated controls? *Due to the emergency generators being activated within 5-10 seconds of a power failure, the locking system in the secure areas is not effected. At the present time, we do not have any Date and Time sensitive devices in the facility.*
3. Does the Veterans Home have any life support or other medical equipment, such as respirators or defibrillators, that depend on electronic devices? *Emergency generators at the Home are able to provide power to maintain the defibrillators in operation during a power failure. Oxygen tanks are also kept in supply as a backup, which do not require power.*
4. What type of evaluation has the Veterans Home conducted to assess: a) the extent to which its automated functions related to security or life support will be affected by the Year 2000 problem, and b) that critical equipment will continue to operate on January 1, 2000? *The Veterans Home's backup generators are not Time or Date sensitive and are not affected by the Year 2000.*

Catherine A. Provencher
Director of Audits
Office of Legislative Budget Assistant
Page Two
February 3, 1999

5. Has the Veterans Home developed contingency plans to address the potential failure of its automated functions? *Any potential failure of automated functions can be handled manually at the present time. Additional manpower would be brought into the Home to meet the needs of the residents.*

Please contact me if you have any questions or if I can be of further assistance to you.

Sincerely,

Barry E. Conway
Commandant

BEC:amb



JEANNE SHAHEEN
GOVERNOR

State of New Hampshire

DEPARTMENT OF CORRECTIONS
OFFICE OF THE COMMISSIONER

105 PLEASANT ST., MAIN BLDG., 4TH FLOOR
P.O. Box 1806
CONCORD, NH 03302-1806
(603) 271-5600
FAX (603) 271-5643
February 5, 1999

HENRY RISLEY
COMMISSIONER

EDDA S. CANTOR
ASSISTANT COMMISSIONER

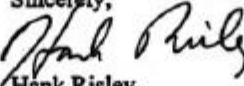
Catherine A. Provencher
Director of Audits
Office of Legislative Budget Assistant
State House, Room 102
Concord, NH 03301

Dear Ms. Provencher:

This letter is in response to your request regarding readiness for the year 2000.

1. Should electric power go off due to a year 2000 related problem, all secure areas such as cell & housing units, sally ports and gates within each DOC facility would automatically go on generator back up operation within ten (10) seconds, generators are operated with diesel fuel, additionally, all secure areas are backed up with manual locking systems.
2. In the event of a failure in the automated controls, all secure areas would remain in the position they were in at the time of default and would require manual operation for the first ten (10) seconds preceding generator kick in.
3. The department has consulted with contracted vendors to ensure year 2000 operation within secure housing areas and has also self tested some areas.
4. As previously discussed, the secure areas within each facility would revert to generator back up and manual locking systems. The department does not have a disaster recovery plan for its automated information systems and local area networks. Power failures would be backed up by generator power.

I would be most happy to answer any further questions you may have.

Sincerely,

Hank Risley
Commissioner

cc: Don Venio

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C

VALIDATION AND TESTING CHECKLIST

Agency or Department:

Function(s) and System(s):

Compliance Point Questions	Software Unit Testing		Software Integration Testing		System Testing		End-to-End Testing		Comments
	Yes	No	Yes	No	Yes	No	Yes	No	
Have test procedures been developed?									
Have baseline data been generated?									
Have exit criteria for tests been defined?									
Have tests been conducted?									
Was current date testing performed to verify dates are correctly determined and used for the remainder of the century?									
Was testing performed to verify correct changes from State fiscal year "1999" to "2000"?									
Was testing performed to verify correct changes from federal fiscal year "1999" to "2000"?									
Was testing performed to verify the correct year field changes using the following dates:									
12/31/1999?									
1/1/2000?									
1/3/2000? (First business day of Y2K)									
1/10/2000? (First seven digit date field)									
1/31/2000?									
2/29/2000? (First Y2K leap day)									
3/1/2000? (First day in March, after leap day)									
3/2/2000? (Second day in March, after leap day)									
3/31/2000?									
12/31/2000?									
1/1/2001?									
1/10/2001? (First seven digit date field for 2001)									
1/31/2001?									
2/28/2001?									
3/1/2001?									
3/31/2001?									
Was testing conducted to verify correct leap year calculations for Year 2000?									
Was testing conducted to verify correct leap year calculations for Year 2004?									
Was testing conducted to verify correct date calculations for non-leap years, such as 2001 and 2002?									
Was testing conducted to verify date-related mathematical functions are correctly performed?									

Appendix C - Validation and Testing Checklist (Continued)

Did the date-related mathematical function testing include multiyear projections forward and backward?									
Has any other date related testing been performed, such as date sorting or for any other special dates (i.e. 9/9/1999)?									
Have test results been documented?									
Have defects identified during tests been corrected?									
Is documentation available supporting the correction of defects during testing?									
Have test exit criteria been satisfied?									
Has there been independent quality assurance or verification and validation for each phase of testing?									
Additional questions for end-to-end testing:									
Have system boundaries for end-to-end testing been determined?									
Have relevant data exchange partners committed to participating in end-to-end testing?									
Has an interorganization end-to-end team been established?									
Has the telecommunications infrastructure been confirmed as Year 2000 compliant?									
Has an end-to-end test plan and schedule been agreed to by relevant data exchange partners?									
Is the agreed upon test plan and schedule documented?									

Staff Accountability

Completed by:

Reviewed by:

Date
:

Date
:

APPENDIX D

DETAILED STATUS REPORT OF YEAR 2000 READINESS

Note: The status reported for the systems listed below has been presented in memo form to each agency, and we have received written statements of concurrence except where indicated by an *Agency Response*.

Adjutant General

Emergency Response and Disaster Recovery (Military Support to Civil Authorities)

Status: Non-Compliant. Assessment Phase.

- ◆ Local and wide area network upgrades have been installed; certified Year 2000 compliant by vendor.
- ◆ Aviation assets (rotary and fixed wing) that may be required for use in emergencies contain non-compliant systems that would prevent flying in zero visibility conditions. Air traffic control systems at the Concord Airport have not been assessed for readiness.
- ◆ Ground mobility assets that may be required for use in emergencies do not contain date-sensitive microchips.
- ◆ Tactical frequency modulation (FM) communication systems are believed compliant and are managed at the national/federal level. No compliance documentation is on hand.
- ◆ High frequency (HF) communications are believed compliant but no compliance documentation is on hand.
- ◆ Back-up power to Armories is being addressed but presently if there is a power grid failure, State Armories do not have back-up power. The purchase of generators and power conditioners is under consideration.
- ◆ A contingency plan is being drafted and expected to be tested before October 1999.

Guard Administration

- ◆ System serves as a centralized purchasing point and handles benefits of members when in an active duty status.
- ◆ Systems have been inventoried and non-compliant systems identified.
- ◆ Once replacement systems have been acquired, agency will be in the correction/renovation phase.

Other Issues

- ◆ Embedded systems are not an issue as most building controls are analog.
- ◆ Security alarms on Armory weapons vaults are compliant but most rely on telecommunications infrastructure to communicate with monitoring services. Compliance certification is not documented.
- ◆ Utilities have been contacted and about two-thirds have responded. If the utilities that have responded are correct in their claims of Year 2000 readiness,

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Adjutant General (Continued)

- most facilities should have utilities available with the possible exception of Littleton.
- ◆ Testing is called for in the agency's Year 2000 plan. Test results are available in summary format for personal computers and hardware related to the local area network.
 - ◆ The federal level National Guard Bureau has led the Year 2000 effort for non-State systems. No documentation on compliance is on hand.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Administrative Services, Bureau Of Emergency Communications

Enhanced 9-1-1 **Status:** Non-Compliant. Correction Phase.

Public Safety Answering Point **Status:** Compliant.

- ◆ The Public Safety Answering Point (PSAP) answers and routes all emergency phone calls (including voice, cellular, digital, and teletypewriter for people who are deaf, hearing impaired, or speech disabled) to local police, fire, and medical service agencies. Approximately 1,200 emergency 9-1-1 calls are answered by the PSAP each day.
- ◆ Hardware - Hardware supporting PSAP consists of two Compaq servers and 19 Compaq workstations. Agency contacted and received vendor certification of compliance.
- ◆ Software - The PSAP uses Windows NT 4.0 with Service Pack 3 as a network operating system and uses specialized software (Vesta version 1.2) for Enhanced 9-1-1 function. Vesta provider certified Year 2000 compliance on Windows NT with Service Pack 3 installed.
- ◆ Bureau also conducted Year 2000 tests on workstations.
- ◆ Contingency plan exists for Enhanced 9-1-1 function.

Telephone Systems **Status:** Non-Compliant. Correction Phase.

- ◆ Reliance upon Bell Atlantic and other telephone providers' network. Bureau monitoring telephone providers through New Hampshire Public Utilities Commission to determine Year 2000 readiness. Bureau contacted Bell Atlantic directly. Bell Atlantic expects to become compliant by June 30, 1999.
- ◆ Enhanced 9-1-1 system designed for redundancy: uses two switches (one from Manchester, one from Concord). If one switch fails, calls automatically routed through other switch.

Other Issues

- ◆ Potential reliance on generator in case of electrical outage. Vendor certification has not been sought or obtained.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Administrative Services, Financial Data Management

NH Integrated Financial System (IFS)/Government Human Resources System (GHR) **Status:** Non-Compliant. Correction Phase.

- ◆ Agency has been addressing Year 2000 related issues since at least 1996. This has dealt exclusively with computing system and has not fully addressed embedded systems or external interfaces.
- ◆ Agency has not had formal discussions with customer agencies regarding compliance of local area networks and other interfaces used to access IFS and GHR.
- ◆ Agency asserts that General Services within the Department of Administrative Services is wholly responsible for any infrastructure and telecommunications related compliance issues. No formal intra-agency contact has occurred. A loss of telecommunications infrastructure will constitute collapse of system.
- ◆ Agency has mechanism in place to exchange information internally on Year 2000 issues that include business and information technology people.
- ◆ Agency has a detailed work plan with dates associated with events. This plan forms the basis for an "issues list" that tracks any issue related to the project from discovery to completion. This is used to inform Year 2000 team members of statuses and assign work.
- ◆ Test plan for mainframe computing system exists and has been implemented. The agency is in the process of testing major systems. Results are available and demonstrated that functions/systems tested thus far have produced identical information as baseline data. Test results have been verified by Bureau of Accounting.
- ◆ Testing plan for desktops has not been formalized.
- ◆ No business continuity plans exist. Contingency planning consists of slack time embedded into schedules and fall-backs onto old applications in the interim period. The data center has been expected to accomplish business continuity planning without complete business process owner involvement. Agency has requested funding for business continuity planning without success.
- ◆ A training packet is being assembled to aid in the transition from the old systems to the new systems. It will be tested and validated before dissemination.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Administrative Services, Bureau Of General Services

Telecommunications Systems **Status:** Non-Compliant. Correction Phase.

- ◆ The State telephone system (Centrex) is not fully compliant. Certain features, such as automatic call forwarding, voice mail, and detailed messaging, will not be available due to Year 2000 problems. These features reportedly are not commonly used by agencies. Basic voice telephony will be unaffected by the Year 2000 according to the vendor. Agencies were informed of Year 2000 status and allowed to make independent decisions on whether to use the noncompliant system or purchase a new system.
- ◆ General Services has contacted the data services vendor and was informed that data networks will be fully compliant by June 30, 1999.

Building Systems **Status:** Non-Compliant. Correction Phase.

- ◆ Energy management systems are centrally controlled and run automatically. If the automatic controls fail, a technician can set each system to run manually. There is a contract in place to install a new computer control to be Year 2000 complaint.
- ◆ The only "smart" fire system is in the State Library and the agency will provide documentation on the system.
- ◆ Emergency generators are wholly controlled by electromechanical devices and have no Year 2000 issues.
- ◆ Uninterruptable power supplies are not the responsibility of the bureau.
- ◆ Security systems are not presently compliant but efforts are underway to make systems compliant by June 1999.

Other Issues

- ◆ Agency has no formal Year 2000 or business continuity planning group.
- ◆ Agency has no formal business continuity or contingency plans.
- ◆ No independent verification or testing of items reported as compliant by vendors.
- ◆ If there is a major power failure (Capital Area), the only State functions (housed in buildings managed by General Services) that will continue are Enhanced 9-1-1 and the State Police communications center. All others have back-up power to run a mainframe but not support business functions.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Employment Security

New Hampshire Unemployment System **Status:** Compliant.

- ◆ Developed in 1994 to be Year 2000 compliant. Date fields use CCYYMMDD format. Approximately \$32 million in benefits paid in calendar year 1998.
- ◆ System calculates unemployment benefits and cuts checks to recipients.
- ◆ Preliminary independent verification and validation conducted; system deemed Year 2000 ready. Full-scale independent verification and validation contract awarded. Report due June 21, 1999 (contract also includes Accounting Contribution Tax System). In-house testing conducted for all transactions processed by system with dates in the Year 2000.
- ◆ Formal written contingency plan developed and approved by federal Department of Labor.

Unemployment Tax System **Status:** Non-Compliant. Testing Phase.

- ◆ Collected approximately \$25 million from employers in 1998.
- ◆ COBOL system currently used until new system implemented.
- ◆ New system (New Hampshire Accounting Contribution Tax System) determines employer liabilities and sends the bill to employer. Implementation planned for February 16, 1999. New system replaces older COBOL system and was designed with date fields which use CCYYMMDD format.
- ◆ Full-scale independent verification and validation contract awarded. Report due June 21, 1999 (contract also includes New Hampshire Unemployment System independent verification and validation).
- ◆ No contingency plan. Plan expected to be completed by June 4, 1999.

Mail Operations **Status:** Non-Compliant. Assessment Phase.

- ◆ Mailing equipment is not Year 2000 compliant; department plans to replace. No formal written contingency plan for mailing system other than manual mailing. Request for federal funds to purchase new mailing system was submitted in November 1998. Received approval March 8, 1999. Agency reported it will be issuing request for proposal to purchase equipment in two to three weeks.

Other Issues

- ◆ No agency-wide disaster recovery plan.
- ◆ Critical date is April 1, 1999 (beginning of benefit year).

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Environmental Services

Hazardous Waste Management: No Status - Manual System.

- ◆ Environmental Services does not control or manage hazardous wastes. Local agencies such as fire department personnel are first responders to hazardous waste spills and incidents. Environmental Services personnel advise, assist, and monitor local agency efforts.
- ◆ Manual paper system used to track movement of hazardous wastes from “cradle to grave.” Electronic database compiles and organizes information.
- ◆ Year 2000 contingency and business continuity plan developed.

Dam Operations: No Status - Manual System.

- ◆ Department regulates approximately 3,175 dams statewide. Most dams are manually operated, but approximately two dozen dams are remotely operated and may contain embedded technology. Letter sent to regulated dam operators discussing potential Year 2000-related problems with dams.
- ◆ Department operates and maintains 268 State-owned dams. State operated dams are manual.
- ◆ Rainfall and streamflow data collected and transmitted by electronic devices. Year 2000 certifications from vendors obtained by the department.
- ◆ Year 2000 contingency and business continuity plan developed.

Other Issues

- ◆ Year 2000 management plan developed.
- ◆ Year 2000 management committee consisting of all levels of Environmental Services management and staff discuss Year 2000 issues.
- ◆ Telephone system issues have not been investigated. Office of Emergency Management will be utilized if telephone system fails.
- ◆ Heating, ventilation, security, and fire systems have not been examined for Year 2000 compliance.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Fish And Game

Search And Rescue **Status:** Compliant.

- ◆ Not reliant on computer systems for search and rescue function.
- ◆ Reliant on vehicles, radio communications (including pagers), and global positioning system for search and rescue function.
- ◆ Letters received from vehicle vendors regarding Year 2000 certifications. Newly purchased off road vehicles have a Year 2000 certification as part of the purchase agreement.
- ◆ Letters received from communication vendors regarding Year 2000 certifications.
- ◆ Dive computers are Year 2000 compliant based on vendors' letters.
- ◆ No knowledge or documentation of global positioning system (GPS) compliance.
Agency Response: GPS is not critical to search and rescue. Map and compass as explained is acceptable.
- ◆ No formal written contingency plan.
- ◆ No formal written test plan.
Agency Response: The Written Test Plan is part of OEM [Office of Emergency Management] drills of which we are a part for search and rescue functions.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Governor's Office Of Emergency Management

Telecommunications Status: Non-Compliant. Assessment Phase.

- ◆ Telephones - Vendor documentation states phone system no longer supported; expected to be non-compliant. New phone system requested in capital budget; awaiting approval. Once approved, system will take three months to install.
- ◆ Pagers - Used to contact employees in emergency situations. Compliant based on vendor's certification.
- ◆ Radio communications - Radio communications relied on heavily during emergency operations. The two-way radio systems are essential. Multiple radio systems for redundancy. Compliant based on vendor certifications.
- ◆ No formal written Year 2000 contingency plan.
Agency Response: This agency operates under an Emergency Operations Plan, which guides agency responses to all emergency conditions. We believe the EOP serves as the de facto contingency plan for this agency. NHOEM is preparing to deal with potential public safety consequences of Y2K, so we have external as well as internal concerns about this issue. Our responses to both will be governed by the EOP.

Emergency Alert System Status: Compliant.

- ◆ Emergency Alert System (EAS) alerts public of emergency situations. Vendor certification states system will function properly except for user display, which Emergency Management does not rely upon.
Agency Response: Software has been ordered to address this issue. The display does not, however, affect the operation of the system; therefore, it is considered compliant. EAS is fully compliant; however, the software to correct date display will be installed for documentation purposes.

Other Issues

- ◆ Not reliant on computer systems for emergency management function.
Agency Response: The statement that the agency is "not reliant on computer systems for emergency management function" is not accurate. Computers are an important asset in rapidly and efficiently carrying out emergency management functions. As with every other agency in state government, there was a time when we functioned without computers and we could do that again if absolutely necessary. We do rely on computers now to carry out agency functions. Our computers and internal network are Y2K compliant.
- ◆ Building security system is not Year 2000 compliant. New system requested in capital budget.
- ◆ Potential reliance on generator in emergency situations. Can operate entire emergency management function for 28 days. Generator uses a mechanical timer; no electronic date/time function. Vendor certification has not been sought or obtained.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Governor's Energy Office

Low Income Home Energy Assistance **Status:** Non-Compliant. Assessment Phase.

- ◆ The agency has augmented its Year 2000 effort by supplementing information contained in its information technology plan with Year 2000 specific tasks, timelines, and responsible persons.
- ◆ The agency has begun to address embedded systems by contacting vendors and providers of service to obtain compliance assurances.
- ◆ No business continuity plan exists.
- ◆ Agency has initiated formal contacts with the community action programs and has solicited numerous documents to support their Year 2000 efforts.
- ◆ Agency has tested desktops with numerous dates. Other roles for agency in testing are under discussion with the Division of Information Technology Management.
- ◆ Entire Year 2000 program is expected to be completed by March 31, 1999.

Building Systems

- ◆ No electronic access or security system exists.
- ◆ Agency has queried the owner of the building to determine fire alarm and suppression system and heating, ventilation, and air conditioning (HVAC) system compliance. Status remains indeterminate.
- ◆ Agency is dependent upon utilities for heat and water.
- ◆ No formal written disaster recovery, contingency, or business continuity plan exists.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Health And Human Services

Emergency Medical Devices: No Status - Manual System

- ◆ New Hampshire Hospital & Glencliff - patients not dependent upon embedded systems for medical issues. Critical care patients are served in local hospitals. New Hampshire Hospital has an emergency back up generator that can operate for approximately one month. Hospital has not determined whether generator contains embedded technology. Glencliff generates its own power. Glencliff personnel stated power generation plant was very old and therefore does not contain embedded technology.

New Hampshire Bridges **Status:** Non-Compliant. Testing Phase.

- ◆ Used by the Division for Children, Youth and Families for case management and claims processing.
- ◆ Housed on a Hewlett Packard 9000 Unix mainframe, Bridges is a client/server application using Oracle database version 7.3.
 - Hardware is certified compliant by the manufacturer.
 - Unix operating system is certified compliant by the manufacturer.
 - PowerBuilder version 6.5 and Oracle database are certified compliant by the manufacturers.
- ◆ Unit testing currently being conducted. Formal written test plans and scripts developed. Test plan includes interfaces.
- ◆ Final Bridges version expected to be implemented in May 1999.
- ◆ No formal written contingency plan.

New Heights **Status:** Non-Compliant. Correction Phase.

- ◆ Determines eligibility for many programs department-wide including Medicaid, Temporary Assistance to Needy Families, Child Care, Food Stamps, Old Age Assistance, Aid to the Permanently and Totally Disabled, and Aid to the Needy Blind. New Heights was implemented on December 1, 1998.
- ◆ Application housed on the International Business Machines (IBM) mainframe (ES/9000) operated by the Department of Administrative Services, Administrative Services Data Center (DAS, ASDC). (This mainframe also houses the New England Child Support Enforcement System, Government Human Resource System, and Integrated Financial System).
 - Hardware - The IBM ES/9000 is certified as Year 2000 compliant by the manufacturer.
 - Operating system is not Year 2000 compliant. DHHS is waiting for DAS, ASDC to upgrade the operating system to a compliant version. DAS reports operating system upgrade planned to be completed April 26, 1999.
 - New Heights application was designed to be Year 2000 compliant. No testing has been completed due to non-compliant operating system. Overall test plan, including Year 2000, expected to be completed by the end of February 1999.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Health And Human Services (Continued)

- ◆ Twenty-two interfaces, six of which are considered critical (NH Bridges, MMIS, Citibank, Citizens Bank, State Treasury, and Check File). Department reports only Citibank was contacted regarding Year 2000 compliance. (Department personnel stated Citibank is Year 2000 ready.)
- ◆ Department reports expected compliance date is June 1999.
- ◆ No formal written contingency plan.

New England Child Support Enforcement System (NECSES) **Status:** Non-Compliant. Correction Phase.

- ◆ Used to collect, distribute, and disburse child support payments related to child support enforcement.
- ◆ Application housed on the IBM mainframe (ES/9000) operated by the Department of Administrative Services, Administrative Services Data Center (DAS, ASDC). (This mainframe also houses New Heights, Government Human Resource System, and Integrated Financial System.)
 - Hardware - The IBM ES/9000 is certified as Year 2000 compliant by the manufacturer.
 - Operating system is not Year 2000 compliant. DHHS is waiting for DAS, ASDC to upgrade the operating system to a compliant version. DAS reports operating system upgrade planned to be completed April 26, 1999.
 - Core Middleware is not Year 2000 compliant.
 - Application is not Year 2000 compliant.
- ◆ Contract with American Management Systems, Inc. (AMS) to remediate Year 2000 problem.
- ◆ Year 2000 analysis of NECSES completed August 13, 1998.
- ◆ Eighteen interfaces; none verified Year 2000 compliant.
- ◆ Department expects NECSES to be Year 2000 compliant by September 1999.
- ◆ No formal written contingency plan.

Medicaid Management Information System (MMIS) **Status:** Non-Compliant. Correction Phase.

- ◆ System makes payments to approximately 10,000 medical providers, including pharmacies.
- ◆ System developed and maintained by Electronic Data Systems (EDS) with oversight by New Hampshire DHHS.
- ◆ Client/Server based system running Solaris operating system.
 - Hardware - Sun Sparc Center 2000 is not Year 2000 compliant.
 - Operating System - Solaris is not Year 2000 compliant.
 - Application - NH Advanced Information Management System is not Year 2000 compliant.
- ◆ Interfaces with New Heights; interface with New Heights not verified Year 2000 compliant.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Health And Human Services (Continued)

- ◆ EDS plans to upgrade hardware, software, and application to be Year 2000 compliant by June 30, 1999.
- ◆ Working on finalizing a test plan.
- ◆ No formal written contingency plan. Representatives stated a manual payout system could be used while the system is down and enter the data later. This manual system is used once or twice per year due to system outages.

Women, Infants, and Children System Status: Non-Compliant. Correction Phase.

- ◆ Women, Infants, and Children (WIC) system determines eligibility and generates food vouchers. Currently housed on a Wang VS 100. Neither hardware nor operating system is Year 2000 compliant. Bureau reports the WIC application is Year 2000 compliant but unable to thoroughly test because of non-compliant hardware and operating system.
- ◆ Initial bureau plan was to wait for Department of Environmental Services computer to become available and to upgrade the operating system. However, as of February 19, 1999, Environmental Services was still utilizing this system. Bureau representatives indicated they are in the preliminary stages of purchasing a new server.
- ◆ No formal written contingency plan developed.

Automated Insert Mailing System Status: Compliant.

- ◆ Stuffs and seals envelopes and places postage on all department mail including benefit payments. Can process up to 10,000 pieces of mail per day.
- ◆ Year 2000 vendor certification obtained.

Personal Computer/Networking Status: Non-Compliant. Correction Phase.

- ◆ Department has approximately 2,500 personal computers (PCs) of which 800 are not Year 2000 compliant. Department has a PC lab which it used to test all PC models used by the department. Norton 2000 test program used to determine Year 2000 compliance. Department plans to replace all non-compliant personal computers by July 1999.
- ◆ Department critical applications are interconnected through a wide area network.
- ◆ Network operating systems used are Windows NT, Novell Netware, and Sun Solaris.
 - Department currently uses Windows NT with service pack 3 which is not Year 2000 compliant for its application. Plan to install service pack 4 which will make Windows NT Year 2000 compliant.
 - Department also uses Sun Solaris version 2.5.1 which requires a patch to make it Year 2000 compliant.
 - Department uses NetWare 4.11 for its file and print servers which require a patch to become Year 2000 compliant.

Appendix D - Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Health And Human Services (Continued)

- ◆ Hardware:
 - Servers - Department uses Compaq and Hewlett Packard Servers. All are certified compliant by manufacturers.
 - Hubs/Firewall - Vendor certifications obtained. Some fixes required for Year 2000 compliance.
 - Routers - All routers are Year 2000 compliant except for the 12 routers at the district offices. Department currently upgrading district office routers; expects to be completed by end of February 1999.
- ◆ No formal written contingency plan.

Embedded Systems

- ◆ Access/Security Systems - Department unsure of Year 2000 status. Buildings accessible by manual keys. New Hampshire Hospital and Glencliff uses manual keys.
- ◆ No formal written contingency plan.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Insurance Department

Insurance Premium Tax: No Status - Manual System

- ◆ Tax payment checks from insurers are processed manually; not reliant on computer systems for processing.
- ◆ Tax payment checks arrive in March, June, September, and December.

Building Systems

- ◆ No electronic access or security systems.
- ◆ Have fire alarm and suppression systems but unknown whether embedded technology used.
- ◆ No emergency generator (dependent upon utilities for heat & water).
- ◆ No formal written disaster recovery plan.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Liquor Commission

Financial Management - Masterpiece Accounting **Status:** Compliant.

- ◆ Masterpiece is reported to be fully compliant. A vendor provided letter constitutes compliance. System is reported to be functioning properly.

Store Operations - Point of Sale **Status:** Non-Compliant. Correction Phase

- ◆ Point of sale will be replaced by ACR2000 that has just completed a pilot test and been accepted for deployment. Deployment is scheduled for June 1999.
- ◆ Vendor reports compliance but independent testing is not documented.

Warehouse - Warehouse Inventory Management **Status:** Non-Compliant. Correction Phase.

- ◆ Law Warehouses reports that as of January 1999, they are 80 percent complete with their Year 2000 program.
- ◆ Internal warehouse management relies on an internally developed program that has not yet been renovated.

Other Issues

- ◆ Building Systems - Electronic access or security systems will be renovated through a contract for which the request for proposal is planned to be released in March 1999. The status of fire alarm and suppression systems is unknown but believed to pose no Year 2000 problem. Vendor certification has not been obtained.
- ◆ Business Continuity - Agency has a draft disaster preparation and business recovery plan that remains in development. It may be ready for December 1999. A subset of this effort that deals with Year 2000 issues is scheduled to be in place by June 1999 but work has not yet begun. The agency should ensure completion of its continuity and contingency plans by the identified critical dates.
 - Agency has no formal written disaster recovery plan.
 - External supplier failure can lead to the Liquor Commission's inability to perform its critical business functions.
 - Loss of telecommunications can severely inhibit the commission's ability to perform its critical functions.
 - Agency links formal risk assessment and business impact assessment to continuity and contingency planning process.
- ◆ Agency is approximately six weeks behind in its efforts. This is reportedly due in large part to staff turnover.
- ◆ Agency will be creating a Year 2000 test machine to validate compliance of critical systems.
- ◆ No formal test plans have been developed and only limited test results of those tests completed exist. A comprehensive test plan should be developed and fully documented.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Liquor Commission (Continued)

- ◆ Agency has not formally developed contingency plans for Year 2000 efforts should remediation efforts fail. The agency should develop and document such contingencies.
- ◆ Manufacturer reports mainframe is compliant.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Retirement System

Annuity Payments **Status:** Non-Compliant. Correction Phase.

- ◆ Currently replacing non-compliant mainframe computer system with compliant client/server system (Administrative Information System (AIS)). Completion date unknown. Retirement management choosing to temporarily halt AIS development to make mainframe Year 2000 compliant at a cost of \$216,000. Vendor (and staff resources) same as AIS, making simultaneous development impossible. Vendor has history of not delivering projects on time.
- ◆ Mainframe remediation reported to take 12 weeks to complete. Completion date reported to be May 31, 1999. No contract with vendor as of February 5, 1999.
- ◆ No formal written test plan.
- ◆ No formal written contingency plan.

Automatic Data Processing (ADP) **Status:** Compliant.

- ◆ ADP processes tapes to generate annuity payroll checks for retirees.
- ◆ Application called ADP PCPERS (Payroll Processing & Communications) used. Correspondence from vendor states application is “century enabled” using a windowing technique.
- ◆ No formal written test plan. No testing completed.
- ◆ No formal written contingency plan.

Other Issues

- ◆ Bottomline Checkwriting - Testing revealed application did not work after Year 2000. Once system date was rolled back to 20th Century application worked. Only problem was report date - reports did not show the correct date.
- ◆ Critical date - July 1, 1999 (Beginning of State fiscal year 2000).
- ◆ Year 2000 issues discussed by NHRS technology group consisting of all levels of NHRS management and staff along with outside consultants.
- ◆ Employees informed of Year 2000 issues.
- ◆ Year 2000 issues currently being re-examined by consultant (Compaq Services).

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Revenue Administration

Tax Information Management System **Status:** Compliant.

- ◆ Revenue is collected quarterly (March, June, September, and December) except for the Tobacco Tax and Meals and Room Tax (collected monthly).
- ◆ Revenue collected by the department is processed through the Tax Information Management System (TIMS). TIMS is housed on an IBM AS/400 version 4.2 minicomputer. Hardware and operating system are vendor certified compliant. All TIMS applications examined by department staff, corrected, and tested.
- ◆ The AS/400 version 4.2 minicomputer has not been independently tested by DRA. DRA has obtained vendor certification for the AS/400.
- ◆ No formal written Year 2000 business continuity/contingency plan.
Agency Response: The department implemented the use of one of the state's first comprehensive Disaster Recovery Plans, which includes business recovery for critical applications at DRA, in 1994. Since that time the plan has been engaged on occasion when the computer systems were unavailable to process daily deposit timely. It has been our position that this is a sufficient recovery plan for department wide daily deposit Year 2000 problems.
- ◆ Formal written Year 2000 test plans used for testing. Department stated TIMS compliant after re-testing; however complete documentation unavailable.
Agency Response: Due to a change in user liaison leadership last spring, a misunderstanding of what needed to be filed during program implementations occurred and most of the actual test plans were not saved by IS. Users usually save this information for their records but discarded it during our move. Our SDM regularly, rigorously demands compliance by users to use approved test plans as a basis for, and to be submitted with implementation authorization sign-offs. Nonetheless, your statement remains accurate to this item.
- ◆ If TIMS is not operating, the department can manually deposit revenue into the banks. This has occurred several times in the recent past.

Other Issues

- ◆ All computer software and hardware has been tested for Year 2000 compliance.
- ◆ Formal written disaster recovery plans exist for each division.
- ◆ Vendor certification for security system has been received.
- ◆ Letter obtained from Administrative Services regarding Year 2000 status of the Centrex telephone system.
- ◆ Letters from data exchange partners have been received.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Safety

Criminal History/State Police Online Tracking System (SPOTS) **Status:** Non-Compliant. Correction Phase.

- ◆ Currently being rewritten.
- ◆ Expect to begin testing in early February.
- ◆ No formal written test plan.
- ◆ No formal written contingency plan.

Radio Communications (including pagers and cell phones) **Status:** Compliant.

- ◆ Compliance assumed - no actual knowledge.
- ◆ No vendor certifications sought or obtained.
- ◆ No formal written contingency plan.

State Police Motor Vehicles (aircraft) **Status:** Non-Compliant. Awareness Phase.

- ◆ Unsure of Year 2000 compliance.
- ◆ No vendor certifications sought or obtained.
- ◆ No formal written contingency plan.

State Police Motor Vehicles (automobiles) **Status:** Compliant.

- ◆ Vendor certifications obtained.

Motor Vehicle Financial System **Status:** Non-Compliant. Assessment Phase.

- ◆ Have not started Year 2000 work on this system. Dependent on completion of the National Motor Vehicle Title Information System.
- ◆ Completion date expected June 1999. Project will take a couple months and requires minor tweaking.
Agency Response: The two months is not for minor tweaking but for full date expansion. Minor tweaking is an alternative.
- ◆ No formal written test plan.
- ◆ No formal written contingency plan.
- ◆ Department has adequate resources to complete work.

Road Toll System **Status:** Non-Compliant. Correction Phase.

- ◆ Replacing hardware (on-hand) and rewriting software developed by PricewaterhouseCoopers. No request for proposal has been issued. Plan to amend previous \$25,000 contract with PricewaterhouseCoopers to add Year 2000 work at an additional cost of \$160,000.
- ◆ No formal written test plan.
- ◆ No formal written contingency plan.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department of Safety (Continued)

Sexual Offenders System **Status:** Non-Compliant. Assessment Phase.

- ◆ Not Started. Dependent upon completion of criminal history system and changes in law. No timeframe for completion set.
- ◆ No formal written test plan.
- ◆ No formal written contingency plan.

Other Issues

- ◆ Telephone System - Obtained memo from Department of Administrative Services stating telephones are compliant. Use redundant, identical systems. No formal written contingency plan.
- ◆ Building Systems - Unsure of Year 2000 compliance. No formal written contingency plan.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Sweepstakes Commission

Lottery Management System **Status:** Non-Compliant. Correction Phase.

- ◆ System is wholly the responsibility of GTECH.
- ◆ Testing, validation, and correction are ongoing concurrently. Commission needs to complete testing of system and provide documented test results.

Retail Terminals **Status:** Non-Compliant. Correction Phase.

- ◆ System is wholly the responsibility of GTECH.
- ◆ Testing, validation, and correction are ongoing concurrently. Commission needs to complete testing of system and provide documented test results.

Ticket Vending Machines (TVMs) **Status:** Non-Compliant. Testing Phase.

- ◆ TVMs have been tested and are Year 2000 compliant. Commission needs to document testing performed and provide documentation for review.

Other Issues

- ◆ Credit Card Validator - Testing, validation, and correction are ongoing concurrently. Commission needs to complete testing of system and provide documented test results.
Agency Response: ...the credit card validator...should not have been included as a critical system. The number of transactions that are processed on the credit card validator are minimal, and if necessary, these could be processed manually over the telephone as a contingency. As additional point of assurance, we have received confirmation from the manufacturer/supplier of the credit card validation system certifying that it is Year 2000 compliant.
- ◆ Mail Subscription System (MSS) - Subsystem is wholly the responsibility of GTECH. Testing, validation, and correction are ongoing concurrently. Commission needs to complete testing of system and provide documented test results.
- ◆ GTECH - Overall system controlled by an outside service provider who is required to have a SAS 70 audit. Commission needs to monitor service provider and obtain Year 2000 assurance from service provider when testing is complete.
Agency Response: GTECH has assured [the Commission] that all of their systems will be compliant by June 30th, 1999.
- ◆ Building Systems and Transportation - Year 2000 compliant except for the fire suppression system. Commission is waiting for vendor assurance and written documentation for review. Need to monitor providers of gasoline, natural gas, electricity, etc. and provide written assurance for review.
- ◆ No formal written Year 2000 contingency plan.
Agency Response: ...we do not currently have a comprehensive Business Continuity Plan. As stated, we do have a Disaster Recovery Plan, however, we have not yet developed a formal Business Continuity Plan for our entire agency.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Sweepstakes Commission (Continued)

We have, however, begun documenting contingencies for all of our core business functions as part of our Year 2000 planning. The information that is gathered during our Year 2000 project should provide us with most of the information that will be needed to develop a Business Continuity Plan. It is our plan to develop this plan in conjunction with our Strategic Business Plan. The Strategic Business Plan should provide the basis for which all of our other plans (Business Continuity Plan, Strategic Information Technology Plan, Disaster Recovery Plan, and Year 2000 Plan) should support. We have set a target completion date of October 31st, 1999 to accomplish this task.

- ◆ Commission should produce comprehensive test plan for overall Year 2000 testing program.

Agency Response: ...we are in the process of developing a comprehensive test script for all lottery systems. This plan will account of all NH Sweepstakes Commission systems; however, the items will be prioritized to ensure that all critical systems are tested first. We are coordinating our test script with GTECH, and the testing will include “minimum standards” tests identified by the Multi-State Lottery Association. Additionally, we will make certain that we have included all of the applicable Critical Year 2000 Testing Dates that you provided to us as an attachment to your memorandum. As the test script is executed, we will document the tests conducted and the results achieved. This documentation will be made available to you as soon as it has been completed.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department Of Transportation

Traffic Signals Status: Compliant.

- ◆ Department operates approximately 315 traffic signals.
- ◆ Three vendors provide traffic signals to the State. Department has obtained vendor certifications for all manufacturers.
- ◆ Testing currently to confirm traffic signals are Year 2000 compliant. Plan to complete testing by April.

Railroad Crossings Status: Compliant.

- ◆ Documentation from the Federal Railroad Administration states “grade crossing signals are event driven, rather than time or date driven” and are free of Year 2000 problems.

Lift Bridges Status: Non-Compliant. Correction Phase.

- ◆ Two lift bridges operated by the department:
- ◆ Sarah Long Bridge - Contract underway to enhance safety. Year 2000 compliance specification written in contract. The department has obtained verbal confirmation of Year 2000 compliance from contractor; awaiting written confirmation.
- ◆ The Memorial Bridge is manual.

Air Navigation Safety: No Status - Manual System.

- ◆ Department maintains five aeronautical navigational aid sites. Not considered critical by the department.
Agency Response: They have no dates or chips in them, therefore there is no Y2K problem.

Highway Maintenance Status: Non-Compliant. Correction Phase.

- ◆ Vehicles (250 snowplow trucks and 250 private snowplow contractors) - Year 2000 certifications obtained from vehicle vendors.
- ◆ Salt spreaders - New units are Year 2000 compliant. Some old units are not Year 2000 compliant but there is a manual override.
Agency Response: A Year 2000 fix will be applied after the winter by the vendor.
- ◆ Automated Fuel Distribution System:
 - Compliance based on vendor certifications of Year 2000 compliance. The new system is not installed yet, therefore the department has not tested for Year 2000 compliance.
 - Department operates approximately 90 fueling sites. Approximately 30 sites are automated and 60 are manual.
 - Some of the fuel sites have generators.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Department of Transportation (Continued)

Turnpike Toll Collection System Status: Non-Compliant. Correction Phase.

- ◆ Collects approximately \$50 million a year.
- ◆ Vendor (Transcore) has provided documentation that the software from the lanes to the plaza is Year 2000 compliant.
- ◆ Testing planned to begin in April to test data processing from toll plazas to the John Morton Building. Parallel testing planned to last three months.
- ◆ No formal written test plan has been developed as of February 9, 1999.
Agency Response: The Department has identified minimal issues regarding compliancy.

Other Issues

- ◆ Telecommunications (telephones and pagers) - No vendor certification has been sought or obtained for Year 2000 compliance.
- ◆ Heating in Dispatch Centers and Morton Building - No vendor certification has been sought or obtained for Year 2000 compliance.
- ◆ Generators - No vendor certification has been sought or obtained for Year 2000 compliance.
- ◆ *Agency Response: Most have no date calculation. Currently checking large generators to ascertain if they have dates in them.*
- ◆ Critical date expected to be 1/1/2000.
- ◆ No formal written disaster recovery plan. Consultant prepared disaster recovery assessment. Results and recommendations to be presented to management soon.
- ◆ No formal written contingency plan.
Agency Response: Information Technology Services reported “We do have a contingency plan. Our internal customer services area and maintenance agreements, in conjunction with the availability of our staff, who wrote most of our programs, will give us the ability to respond to any problems which may occur.”
- ◆ New radio system from Ericsson. Approximately 95% done. Expected to be completed in the next several months. There are two dispatch centers: Hooksett and Lancaster. Have vendor certification stating the Ericsson radios are Year 2000 compliant.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Treasury

Investment and Debt Management **Status:** Non-Compliant. Assessment Phase.

- ◆ Application is processing dates beyond January 1, 2000 and is believed to be compliant.
- ◆ Application resides on a non-compliant operating system and must be migrated to a compliant operating system.

Cash Management **Status:** Non-Compliant. Assessment Phase.

- ◆ Application has not been fully assessed for compliance.
- ◆ Application currently processes dates beyond January 1, 2000.
- ◆ Application resides on an operating system that is not Year 2000 compliant but can be made compliant.

General Fund Distribution **Status:** Non-Complaint. Assessment Phase.

- ◆ Application remains in assessment.
- ◆ Application resides on a non-complaint operating system and must be migrated to a compliant operating system.

Contingency and Business Continuity Plans

- ◆ Agency has not formalized contingency plans for critical systems.
- ◆ Agency has not formalized plans for business continuity.
- ◆ Agency does not have disaster recovery plans and is exposed to substantial risk by not having adequate procedures for recovery of critical functions.
- ◆ Agency has no business continuity or contingency planning body that involves all stakeholders to include executive management, business managers, information technology staff, and others.

Agency Response: Executive management and information technology staffs have discussed the issues of Year 2000 compliance.

External Interfaces and Data Exchanges

- ◆ Agency has not formally contacted its exchange partners including, but not limited to, other State agencies and banks.
- ◆ Agency has not fully assessed potential July 1, 1999, (State fiscal year) impact on its systems and applications.

Embedded Systems

- ◆ Agency has not fully assessed its embedded systems formally.
Agency Response: Agency is currently assessing its embedded systems.

Appendix D – Detailed Status Report Of Year 2000 Readiness (Continued)

Treasury (Continued)

- ◆ Agency relies on limited telecommunications for its critical functions. Loss of telecommunications would be inconvenient but it may be possible to work around such loss. No alternatives have been formalized.

Building Infrastructure

- ◆ Agency has not assessed building infrastructure and has not contacted agency responsible for building infrastructure.
- ◆ Agency can not operate without power as the uninterruptable power supply serves the agency's server only and not desktops or other needed services.
Agency Response: Agency has contacted the agency responsible for building infrastructure and has verbal confirmation that security and telephone systems are Year 2000 compliant. Written confirmation is being mailed to the agency.

Other Issues

- ◆ Agency lacks comprehensive, detailed plan that assesses its current status and delineates a reasonable plan to be compliant in a timely manner.
- ◆ No prioritization of agency effort has been documented but exists.
- ◆ Agency server is Year 2000 compliant but independent testing can not be verified.
- ◆ Agency lacks adequate test plans and has not adequately documented tests conducted to date.
Agency Response: Agency's plans are to have formalized planning documents complete by March 1999, testing completed by May 1999, and full compliance by June 30, 1999.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E

CONTINGENCY PLANNING COMPLIANCE CHECKLIST

INITIATION		
1.1 Develop and document a high-level business continuity planning strategy	Response (Y or N)	Remarks
Does a high-level business continuity planning strategy provide the agency's executive management with a high-level overview of the Year 2000 business risks and solutions?		
1.2 Identify core business processes		
Have business owners and Y2K staff identified core business processes?		
Have business owners and Y2K staff identified supporting mission critical systems for each business area?		
Are all key business dependencies (infrastructure, external interfaces, embedded systems, etc.) clearly identified?		
1.3 Define roles and assign responsibilities		
Are responsibilities for leading the planning effort assigned?		
Are individuals appointed to lead the development of contingency plans for each of the core business processes?		
Are responsibilities for documenting the business continuity plan defined?		
Are individuals responsible for the various business continuity and contingency planning activities held responsible?		
1.4 Develop a master schedule and milestones		
Has a schedule for the planning effort and the delivery of interim and final products been developed?		
Is the schedule linked to critical stages in the Year 2000 program effort?		
Does it include a drop dead remediation/replacement or compliance milestones?		
1.5 Implement a risk management process and establish reporting system		
Has a deliberate risk management process been applied to each risk?		
Does the plan assess the impact of each potential failure...		
...in terms of business operations and functions?		
...in terms of the probability of failure?		
...in terms of expected loss?		
Are alternative business processes to each identified risk areas developed?		
For each contingency, does the plan estimate:		
...cost of hardware?		
...cost of software?		
...cost of services?		
...FTE staff?		
...cost of FTE staff?		
...time required?		
...resource availability?		
Does the plan:		
...compare expected loss with expected cost for each proposal?		
...eliminate proposals where cost is greater than expected loss?		
...eliminate proposals with early decision date?		
...evaluate remaining proposals based on cost, resource, and lead-time?		

Appendix E - Contingency Planning Compliance Checklist (Continued)

...select one or more proposal?		
...define trigger points for each proposal?		
...include a risk reduction strategy?		
...relate infrastructure loss to business function impact?		
...consider alternative equipment and location use?		
Have business risks been ranked?		
Do ranked risks focus the planning effort on the greatest risk to critical core business processes?		
Have a reporting system, reporting requirements, and formats been established?		
Has risk been estimated and assigned to each mission critical system undergoing renovation or replacement?		
Are resources allocated based on risk rankings?		
Are resources linked to risk functions?		
Are actual costs tracked and compared against estimates?		
1.6 Assess existing business continuity, contingency, and disaster recovery plans and capabilities		
Have existing business continuity, contingency, and disaster recovery plans been assessed for applicability?		
1.7 Implement quality assurance reviews		
Have any internal and/or external quality assurance staff reviewed and commented on the business continuity planning process?		
Have quality assurance reviews examined worst case scenarios?		
Does the back-up strategy appear reasonable?		
Can back-up strategies be successfully implemented in a national emergency?		

BUSINESS IMPACT ANALYSIS		
2.1 Define and document information requirements, methods, and techniques to be used in developing the business continuity plan	Response (Y or N)	Remarks
Do they include:		
...operational priorities, service levels, dependencies, and relationships?		
...the primary and collateral Year 2000 business risks and the business scope of their impact?		
...the costs and benefits of business continuity strategies and alternatives?		
When collected, analyzed, and synthesized, does the information define a model of critical processes and risks to the business?		
2.2 Define and document Year 2000 failure scenarios		
Are business vulnerabilities and their impacts assessed?		
Is the loss of all mission critical information systems due to post-implementation failures or delays in renovation and testing assumed?		
Is the possibility that Year 2000 date problems may be encountered earlier than expected considered?		
Are the following potential disruptions assessed:		
...electric power?		
...telecommunications?		
...transportation?		
...loss of environmental control?		

Appendix E - Contingency Planning Compliance Checklist (Continued)

...system shutdown?		
...degraded performance?		
...irrational data generation, corrupted files, lost files, or unpredictable or unreliable results?		
...failure of renovation and testing timelines?		
...failure of security and safety systems?		
...failure of other physical plant functions?		
Are agency business continuity and contingency planning efforts focused on likely failure scenarios?		
2.3 Perform risk and impact analyses of each core business process		
Is the status and progress of the Y2K program monitored?		
Are Y2K-related risks posed by customers, suppliers, information technology vendors, and business partners considered?		
Is the impact of internal and external information system failures on each core business process determined?		
Is the impact of failure of infrastructure services on each core business process determined?		
Have manual and automated system support requirements been considered?		
Have infrastructure support requirements, suppliers, customers, service levels, processing cycles, and the external and internal business drivers been considered?		
Are the following identified:		
...critical functions?		
...recovery priorities and timing?		
...dependencies on other systems and processes?		
Has each data or information exchange partner been contacted and was the entity's Y2K status obtained?		
Are concerns regarding external data partners addressed in contingency plans?		
Are the potential costs of service disruptions estimated?		
Is the duration of each disruption addressed in these estimates?		
2.4 Assess and document infrastructure risks		
Is the Y2K readiness of public infrastructure, including power and telecommunications services monitored?		
Is the risk of service outages assessed?		
Is the potential impact of outages on the core business processes assessed?		
2.5 Define the minimum acceptable level of outputs and services for each core business process		
Has the minimum acceptable level of output and the recovery time objective been defined for each business process?		

CONTINGENCY PLANNING		
3.1 Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core business process	Response (Y or N)	Remarks
Are benefits, costs, and risks of alternative contingency strategies considered?		
Is a strategy that is practical, cost-effective, appropriate to the organization, and provides a high level of confidence in recovery selected?		

Appendix E - Contingency Planning Compliance Checklist (Continued)

Are three important factors in the selection process considered:		
...functionality? (the degree to which the replacement functionality supports the production of a minimum acceptable level of output for a given core business process)		
...deployment schedule? (the time needed to acquire, test, and implement)		
...cost? (life-cycle cost, including acquisition, testing, training, and maintenance)		
Is a contingency plan including strategies capable of meeting minimum acceptable output requirements for each core business process developed?		
Are the following implementation modes considered:		
...automated replacement?		
...semi-automated replacement?		
...manual replacement?		
Do manual alternatives require hiring and training additional staff?		
Are redundant business services provided through outsourcing contracts?		
Do triggers include:		
...early arrival system failure?		
...partial to total renovated/replaced system failure?		
...compliant system failure?		
...vendor certified system failure?		
...interface failure?		
...implementation failure?		
...infrastructure failure?		
...mechanisms to filter out non-Y2K failures due to hackers, sabotage, etc.?		
Have agency executives established business resumption teams?		
Have agency executives established business resumption priorities?		
Has a risk-reduction strategy and procedures for the period between Thursday, December 30, 1999, and Monday, January 3, 2000 been developed and documented?		
Does this strategy include an agency-wide shutdown of all of its information systems on Friday, December 31, 1999, and a phased power-up on Saturday, January 1, 2000?		
Has the agency considered extending the shutdown to infrastructure systems, including local area networks, elevators, and building management systems?		
Are:		
...events that may trigger the plan qualified?(What constitutes an event? How severe an event is it?)		
...trigger dates and times identified?		
...procedures to verify event in place?		
...procedures to verify event is Y2K related and not the result of other problems, hackers, sabotage, etc.?		
...plan implementation approval mechanisms in place?		
...procedures to notify key staff, including name, phone numbers, alternate means of contact, in place?		
...alternative modes of staff getting to work detailed?		
...alternative communications modes identified?		
...functional transfers to another agency, system, or contractor considered?		
...alternative power modes, including how long the generator must run, defined?		
Are procedures for operating in contingency mode defined to include:		
...safety?		

Appendix E - Contingency Planning Compliance Checklist (Continued)

...maintenance of essential information security?		
...maintenance of essential physical security, even in a complete failure?		
...documenting events?		
...criteria for resumption of normal operation?		
...procedures to restore or restart system?		
...procedures to check and verify results?		
...procedures to correct and restore corrupt or lost data?		
...provide for the preservation of data through database backups or printouts?		

TESTING	Response (Y or N)	Remarks
4.1 Validate business continuity strategy		
Is a strategy for validating the business continuity plan developed and implemented within the time that remains?		
Does the strategy define a minimum number of individual and joint exercises that combine training with testing?		
4.2 Develop and document contingency test plans		
Are contingency test plans defined?		
Are contingency test plans documented?		
Are the test plans reviewed?		
Are needed changes made?		
Has the agency executive signed the plan?		
Are documents disseminated?		
4.3 Establish test teams and acquire contingency resources		
Are test teams responsible for preparing and executing the contingency plan tests established?		
Has training been scheduled?		
4.4 Prepare for and execute tests		
Have tests been prepared for?		
Have tests been conducted?		
4.5 Validate the capability of contingency plans		
Is the functional capability of each contingency plan validated?		
Are test results examined for accuracy and consistency?		
Does each contingency plan adequately support a core business function?		
Have adequate capability to manage, record, and track the contingency transactions through the alternative business process?		
Do manual activities meet an acceptable level of performance?		
Does the alternative business process in general meet an acceptable level of performance?		
Is acceptable level of quality control provided to critical parts of the alternative business process?		
Is an acceptable level of security provided to the data captured by an alternative mechanism?		
4.6 Rehearse business resumption teams		
Are business resumption teams rehearsed to ensure that each team and team member is familiar with business resumption procedures and their roles?		
4.7 Update the business continuity plan based upon lessons learned and re-test if necessary		

Appendix E - Contingency Planning Compliance Checklist (Continued)

Is the plan updated?		
Is a re-test required to ensure that the problems do not recur?		
4.8 Update disaster recovery plans and procedures		
Are contingency and disaster recovery plans updated?		