



# Executive Briefing

## Year 2000 Embedded Systems



*Prepared for André Pettigrew*

### **Task Force Members:**

Audrey Aultman, General Support Services/Department of Personnel

David Kaye, Attorney General's Office

Jane Lopez, General Support Services/Department of Personnel

Brian Mouty, General Support Services/Department of Personnel

Susana Villescas, General Support Services/Department of Personnel



# Table of Contents

I. PREFACE.....	3
II. IDENTIFICATION OF EMBEDDED SYSTEMS.....	4
III. THE NATURE OF THE PROBLEM.....	5
IV. LEGAL ISSUES ASSOCIATED WITH FAILURE OF YEAR 2000 EMBEDDED SYSTEMS.....	6
V. RISK MANAGEMENT.....	9
VI. PROJECTED COSTS.....	10
VII. RECOMMENDED ACTIONS.....	10
VIII. CONCLUSION.....	13
IX. STRATEGIC PLAN OF ACTION.....	14



# YEAR 2000 EMBEDDED SYSTEMS

## *I. PREFACE*

Embedded systems are those electronic chips that are in just about everything. These chips programmed at the factory are in your car, your VCR, the fax machine, the microwave, cellular phone and automated systems such as elevators and security systems. Their responsibility is to regulate the basic functioning of these machines or systems such as making sure that pacemakers keep on ticking or controlling when security alarms go off. “*Embedded*” reflects the fact that they are an integral part of a system. In many cases the degree to which they are embedded may be such that their presence is far from obvious to the observer.

All embedded systems are computers. Some of them are however, very simple devices as compared with a PC. The simplest devices consist of a single microprocessor (often called a chip) which may itself be packaged with other chips in a hybrid or Application Specific Integrated Circuit (ASIC). Its input comes from a detector or sensor whose output goes to a switch or activator which for example, may start or stop the operation of a machine. In more complex systems, the functioning of the embedded system is determined by an application program, which enables the embedded system to do things for a specific application. While many of these systems are not date intensive and therefore will not create significant problems in the Year 2000, many others will present significant problems, or at least an inconvenience if not corrected prior to January 1, 2000!

The year 2000 problem arises because many of these embedded systems contain date references to help them perform certain basic tasks essential to their proper functioning. For example, a pacemaker would likely have an internal computerized device that records, monitors and then logs heart activity. While the monitoring and recording parts are not time sensitive, the logging part would be done using a date field that calculates year related information in a two digit format.<sup>1</sup> Typically, the systems are written in low-level code, then burned into the chip’s ROM memory, so the chip cannot be altered. This means that in order to fix the problem, somebody with expertise in the product (the vendor or manufacturer), must get at the system to test

---

<sup>1</sup> Two digits were used by programmers in the past instead of four to save (then expensive) memory and disk storage.

and fix Year 2000 problems. Each embedded system must be treated as if it were a different programming language that only a few people know. Without one of these experts to help, a system may be at risk! And, unless the problem is fixed, most systems with time-sensitive tasks will recognize the year 2000 as “00,” and may assume that the year is “1900” rather than 2000. This could either force a system to shut down or lead to malfunctions.

## ***II. IDENTIFICATION OF EMBEDDED SYSTEMS***

Following is a sample of State agency systems that might have embedded systems.

### **Office Systems and Mobile Equipment**

- Answering Machines
- Copiers
- Desktop Computers
- Fax Machines
- Laptops and Notebooks
- Mobile Telephones
- Personal Organizers
- Still and Video Cameras
- Telephone Systems
- Time Recording Systems
- Voice Mail

### **Building Systems**

- Air Conditioning
- Backup Lighting and Generators
- Building Management Systems
- Burglar and Fire Alarms
- CCTV Systems
- Door Locks
- Fire Control Systems
- Heating and Ventilating Systems
- Lifts, Elevators, Escalators
- Lighting Systems
- Safes and Vaults
- Security Access Control Systems
- Security Systems
- Security Cameras
- Sprinkler Systems
- Switching Systems

### **Transport**

- Automobiles
- Ticketing Machines
- Command and Control Systems
- Speed Cameras, Radar Speed Detectors
- Photo Surveillance Systems

### **Communications**

- Telephone Exchanges

Cable Systems  
Telephone Switches  
Satellites

**Medical**

Imaging Equipment

**Domestic Equipment**

Central Heating Control  
Catering Equipment  
VCR's  
Microwaves

### ***III. THE NATURE OF THE PROBLEM***

Most attention on addressing the problems and challenges surrounding the year 2000 has been focused on Information Technology (IT) systems. However, another dimension to the Year 2000 challenge involves those automated functions that involve embedded chips. While many of the systems that use embedded chips do not use dates and most of them aren't in places that will cause life or budget threatening problems, we do have systems within State agencies, that if they were to fail, could present the threat of real harm in the year 2000. Following are some of the more prevalent issues associated with embedded systems and the Year 2000.

- ***Lack of identification, assessment and testing of systems with embedded chips:*** Within State agencies, there are quantities of unknown machines/systems that have embedded chips. At this point in time, it is unlikely that anyone can accurately say where these embedded systems are, what they do and how such systems will be affected by the Year 2000. Therefore, assessment and testing of such systems for Year 2000 compliance cannot occur until such systems have been identified.
- ***There are various chip manufacturers:*** Because there are no standards for manufacturing something like a motherboard, manufacturers can use any chip in any way they want to. Since it is so easy to make systems different, each one of the embedded systems in use must be individually checked and tested to see if that system has a Year 2000 (Y2K) problem. In other words, one cannot test one "typical" system and then extrapolate the results to all others from that manufacturer. This involves resources to actually look at systems and the technical knowledge of what to look for.
- ***Time is critical:*** Although the State is aware of the seriousness of the Y2K problem, it has not yet factored in the potential Y2K effects upon State systems and operations. It has been stated that those companies that have begun to address the issue, have never overestimated the amount of time required to solve the problem. *"The problem has always proven to be larger, uglier and more costly than anyone imagined!"* Most analysts recommend deciding on a course of action by the first quarter of 1998, and allowing the remainder of the year and 1999 for

implementation and testing. Organizations that have approached the problem early have demonstrated that their time advantage has enabled them to devise strategies to reduce costs and incorporate benefits within chosen solutions. The key to that flexibility is the availability of time.

- ***Technical expertise/resources in this area is becoming increasingly scarce.*** As resources become scarce, the cost of available resources will rise. It has been reported that salaries of COBOL programmers have risen by over 100 percent. Similarly, salaries for relevant expertise continue to rise at a rate of 20 to 50 percent on a yearly basis. It will become more difficult to retain good technical expertise and/or compete for scarce resources. In order to retain and contract technical resources, the State must consider initiating measures such as bonus incentives, salary augmentation and competitive short term contracts that will attract technical resources to the State and retain those technical resources already within State agencies.
- ***Lack of state coordination:*** It is not enough to solve problems in isolation from other State agencies. We need to, as a State, address the Year 2000 problems of our customers, our suppliers and our State agencies. Everyone is in the same boat on the Year 2000 problem. If we fix everything in one agency, we are still at risk as a State from other State systems and anyone else with whom we share data and resources. Again, the overriding message is clear. We are in this together and the more we help each other and coordinate such efforts, the more we help ourselves.

#### ***IV. LEGAL ISSUES ASSOCIATED WITH FAILURE OF YEAR 2000 EMBEDDED SYSTEMS***

The most useful way to begin analyzing legal issues and risks associated with Year 2000 embedded systems is to first distinguish between the State's exposure to lawsuits for systems failures and the State's remedies against the product vendors or manufacturers. In the first instance, the State should be enforcing its rights against vendors simply to ensure value to tax payers. In the context of Year 2000 system failure, there is the additional consideration of pursuing available remedies as part of an overall risk management strategy against potential State liability to its employees and the public. Another area of focus in this regard is what the State should be including in its future contracts in order to address the Year 2000 problem.

##### **1. State Liability to Others**

With respect to Year 2000 Embedded Systems, the State is exposed to potential financial liability in three areas: (1) tort; (2) workers' compensation; and (3) contract.

- ***Tort Exposure:*** Tort Liability, that is damages for death or injury to people or property, is governed by the ***Colorado Governmental Immunity Act***. The State is not liable in tort unless immunity has been

waived by statute. Immunity has been waived in the Act for the following of actions:

- ⇒ The operation of a motor vehicle within the course and scope of employment, except for emergency vehicles engaged in responding to an emergency;
- ⇒ The operation of a public hospital, correctional facility or jail;
- ⇒ A dangerous condition of the following public facilities; hospital, jail, water, gas, sanitation, electrical, power, swimming, or any facility in a public recreation area or park if the public entity has assumed responsibility to maintain it;
- ⇒ A dangerous condition of any public building; and,
- ⇒ A dangerous condition of a public highway, road or street that physically interferes with the movement of traffic.

If immunity is waived, State liability is determined as it would be in the private sector, that is, was the State negligent in some manner. According to one legal commentator, *“attempting in earnest to address problems and failing through some unforeseen or uncontrollable cause is better than ignoring the problem or undertaking an unreasonably weak effort.”*

Where the State has waived governmental immunity, the Risk Management Fund may be required to pay up to \$150,000 per person for each occurrence, but not more than \$600,000 total for any single occurrence. A review of the sample list of products with embedded systems (see pages 3 & 4), reveals a rather large percentage of items impacting the safe condition and operation of public buildings and facilities.

The State may also be exposed to Federal civil rights violations for malfunctions resulting in injury to a legally protected interest (i.e., property interests). These injuries are different from bodily injury, death or damage to tangible property. For example, in the criminal justice context, improper issuance of warrants or improper calculation of prison sentences and earned good time may result in liability. There is no State law governmental immunity and the potential damages are not capped by statute.

- **Workers’ Compensation:** Dangerous conditions of public buildings and facilities, as well as malfunctioning equipment, also present increased workers’ compensation exposure for bodily injury or death of State employees. The State is self-insured through the Risk Management Fund for workers’ compensation claims. Therefore, the State will be directly and immediately impacted through claim payouts, rather than having the benefit of a year’s time lag for the claims experience to cause increased premiums under a commercial insurance policy.

Although there are some defenses available to the employer and its insurer, workers’ compensation claims are generally in the nature of strict liability, that

is, the injured employee need not prove negligence. A workplace injury is sufficient to trigger liability. The State would, however, have rights of subrogation to pursue recovery against anyone who is wholly or partly responsible for the injury. In the Year 2000 context, the list of potentially responsible parties may include vendors.

The *Workers' Compensation Act of Colorado* controls and limits the amount of financial recovery against the State as a self-insured employer. Currently, a single claimant's recovery for permanent total disability is unlimited except by how long the claimant lives. The claimant could receive 66.6% of his or her average weekly wage for the remainder of his or her working life. Benefits for permanent partial and temporary total disabilities combined may not exceed \$125,000 for those more than 25% impaired, and \$60,000 for those impaired 25% or less. Severely injured State employees may also be entitled to PERA disability benefits.

- **Contract:** The State may be liable for breach of contract in any case where the State's performance fails as a result of Year 2000 embedded systems failure. In many contracts, the State is obligated to provide some in-kind performance in addition to money. Where system failures render the State unable to deliver its in-kind performance and the vendor in turn is unable to perform in return, the vendor may sue the State for the benefit of the bargain. This measure of contract breach damages seeks to force the State to pay the profit the vendor would have earned on the contract if the State's breach had not prevented the vendor from performing its obligation and earning the entire fee. The magnitude of this problem will only be known after all affected systems and their functions are identified.

In pursuing corrections to identified systems, the State must exercise caution to ensure that copyrights are not violated and that systems which interface use compatible methodologies for resolving the Year 2000 glitch. If systems are repaired by someone other than the original owner of any proprietary rights, the State must ensure that the party undertaking the fix is properly licensed to do so. Further, Year 2000 calculations do not present a uniform problem. Software may require different remedies depending upon the problem and the available solutions. Where systems interface, the remedial methodologies must be compatible, so that systems may continue to work together.

## **2. State Remedies Under Existing Contracts:**

The State may have remedies against the product vendors (seller's manufacturers, or both) to correct systems incapable of properly functioning beyond 1999. Until recently, agreements have been silent as to the Year 2000 problem. Any existing State contracts, State purchases, or purchase orders, which do not expressly provide for Year 2000 compliance, may be the subject of dispute as to the vendor's responsibility to correct the problem.

There are a variety of legal theories under which the State may pursue corrective action at vendor expense. Vendors may also be liable directly to the injured parties. When sued, the State may make third party claims against vendors alleging their

ultimate liability to the injured person(s). A complete discussion of these causes of action is beyond the scope of this report.

The State must quickly identify the subject systems, locate the relevant agreements, and attempt to timely exercise whatever remedies may be available according to a priority list. This will be an enormous task involving thousands of agreements. It is important to point out, that this is a critical piece of any comprehensive Year 2000 plan, and the reasonableness of the State's attempts to deal with Year 2000 failures may be a central issue in tort and contract suits against the State.

### **3. Future State Contract Provisions**

The State must decide what new language to include in its prospective agreement in order to ensure the State is adequately protected in future acquisitions. This may include a general warranty boilerplate for all State contracts, specific performance standards as to each acquisition, or some combination of both.

It is important to note, that many contracts contain a "force majeure" clause that protects a contract party for a claim of default when it fails to perform due to an Act of God, or other event beyond the party's reasonable control. It is unlikely that the Year 2000 problem would be viewed as an Act of God, since it is a known problem, which can be corrected with enough planning and resources. Depending on the particular language used in each "force majeure" clause and the facts and circumstances surrounding the failure to perform, the Year 2000 problem may be claimed to constitute an event of "force majeure" in some contract disputes. The State may wish to alter their standard "force majeure" language to rule out the Year 2000 problem specifically.

## ***V. RISK MANAGEMENT***

Every State agency is at risk of widespread system failures and potential legal liabilities resulting from system failures. Unless corrected, the impact of such failures could be costly. For example:

- ⇒ The Year 2000 problem may present the biggest litigation wave our country has ever seen. Organizations that do not solve this problem in time are certain targets of suits. Moreover, many analysts believe that if litigation hits because of Year 2000 failures, it will hit like a fireball— fast and pervasive. Doing nothing is not an option!
- ⇒ Several companies manufacture varieties of programmable thermostats. If not designed to recognize the change in century, it is possible that we could awake on January 1, 2000 to a very cold environment. If pipes freeze and burst, the resulting damage both inside and outside could be immense.
- ⇒ Telephone systems may not be able to recognize the century change resulting in incorrectly time stamped voice mail messages and incorrectly routed calls.

- ⇒ Most elevators have embedded systems that monitor the amount of time between maintenance checks. If these automated devices calculate that the allowable time between maintenance checks has been exceeded, most elevators will go to the bottom floor in the elevator shaft, take themselves out of service and remain at the bottom of the shaft until maintenance is performed and the clock is reset. If embedded systems are not designed to identify the change from 1999 to 2000 and it interprets the “00” as 1900, making the time between maintenance checks exceed the limit, it will send the elevator to the bottom floor making it inoperable. This could be annoying in one building and potentially life threatening in another, where for some individuals, using the stairs is not always a viable alternative.
- ⇒ Defibrulators use an embedded device that calculates the time since the last maintenance similar to elevators. Like the elevator, if the time since the last maintenance check surpasses a certain time frame, the defibrillator will not operate.
- ⇒ Lawn sprinkler systems may spurt into action overnight.
- ⇒ Building security systems may not recognize ID badges.

## ***VI. PROJECTED COSTS***

Analyst projections and reports written on the subject, estimate the costs of Embedded Systems projects to be 50-100% of Year 2000 Information Technology (IT) program budget. Therefore, costs associated with a Year 2000 — Embedded System Project could potentially range from 20m to 40m, depending on the time and complexity of the project.

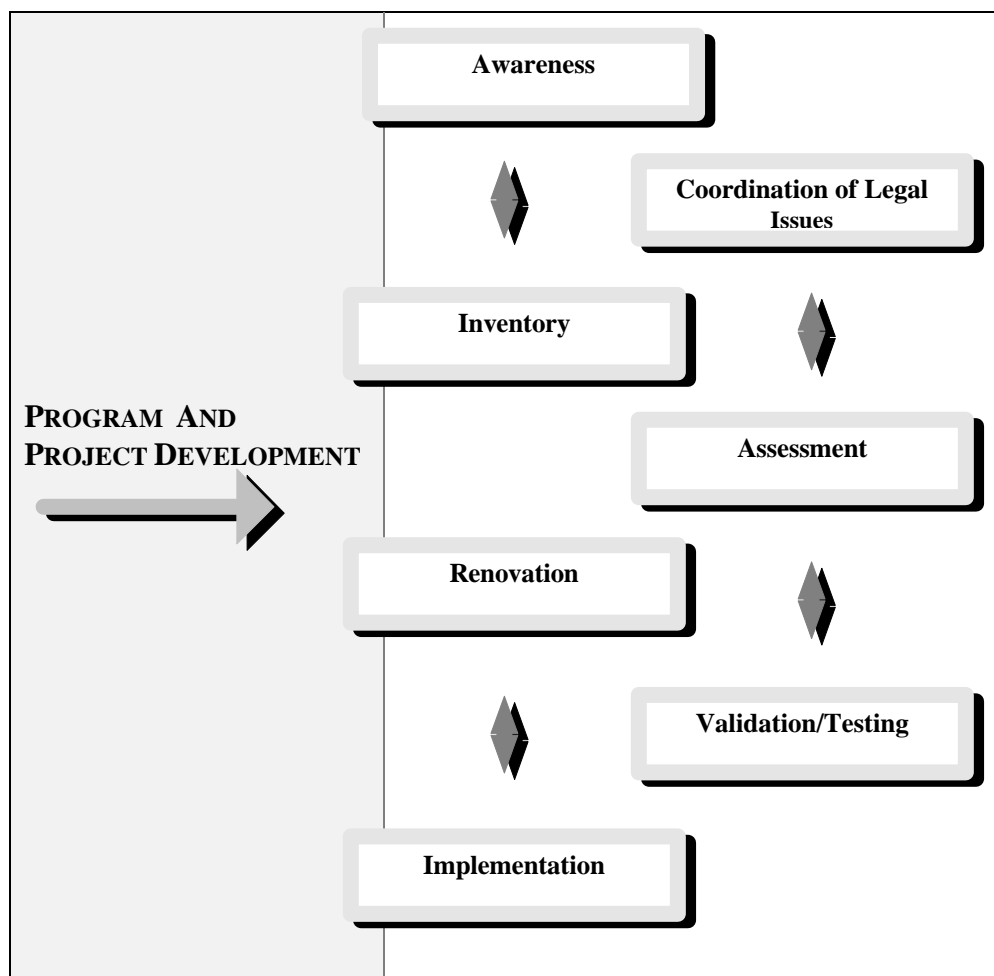
## ***VII. RECOMMENDED ACTIONS***

We cannot stress enough the critical importance of immediate action to address the problems associated with embedded systems. Although it appears that any organization can become Year 2000 compliant if it starts corrective action soon enough and devotes sufficient resources to the effort, it is important to underscore that time is running out! Year 2000 experts recommend that corrective action begin as soon as possible and not be delayed until there may not be enough time left to complete the requisite fixing and testing. Because identifying, fixing, and testing systems will be a massive and complex undertaking, agencies must act quickly to complete all of the required phases to complete the project. In order to succeed, the State must formulate a structured approach and rigorous project management to decrease our risks. Specifically, we recommend the establishment of a Year 2000 Embedded Systems program management structure that identifies the following elements: (See Appendix 1 to this Report).

- ❑ **Development of a Year 2000 Embedded Systems Project Task Force:** The Embedded Systems Year 2000 project will require input and cooperation of all organizational units and concerns. Thus, it is important that the technical and management staff of the core business areas work closely with the Year 2000 Embedded Systems project teams in the assessment and testing processes. Additionally, this task force can be instrumental in not only launching the Year 2000 Embedded Systems project during the interim period in which a Project Manager is appointed, but also in ensuring the smooth transition of project tasks from the task force to the Year 2000 Embedded Systems Program Staff. At a minimum we require that this task force consist of the following representation and expertise:

  - Attorney's General's Office
  - General Support Services/Department of Personnel
    - Division of Purchasing
    - Information Management Commission (IMC) (Adhoc member)
    - Administrative Services
    - Capitol Complex Facilities
    - Risk Management
    - State Controller's Office
    - Executive Director's Office (Project Coordination)
    - Division of Telecommunication
  - Office of State Planning and Budget (OSPB)
- ❑ **Development of a boilerplate for all State contracts and specific performance standards as to each acquisition that addresses Year 2000 compliance.** The State Controller's Office and the Division of Purchasing, should be jointly involved in developing the standards and communicating the standards to agencies through existing fiscal and procurement networks in the State system.
- ❑ **Each agency must designate a Year 2000 Embedded Systems project coordinator.** The coordinators shall be responsible for organizing department level activities and serve as the primary point of contact for the Year 2000 Embedded Systems Program Manager.
- ❑ **Develop a Year 2000 Embedded Systems Strategic Plan** that identifies at a minimum the following phases of program development and implementation:

## PROGRAM PHASES



- **Awareness:** It is essential that executive management be fully aware of the Year 2000 Embedded Systems problems and the potential impact on the business of the agency and its customers. We believe that it will be the responsibility of each Executive Director to provide the leadership in defining and explaining the importance of achieving Year 2000 compliance, selecting the overall approach for structuring the agency's Year 2000 Embedded Systems program, and mobilizing needed resources. The management support for the agency's Year 2000 strategy should be formalized by the issuance of a Year 2000 policy directive and/or Year 2000 program charter. Without such support, appointed staff or committees may not be able to mobilize adequate resources to implement the strategy and to interact with other organizations and data sources.
- **Coordination of legal issues:** The State Risk Manager and the tort defense lawyers in the Attorney General's Office should be consulted regarding any legal issues or concerns pertaining to Year 2000.
- **Inventory:** Agencies must determine the size and scope of the Year 2000 Embedded Systems problem by conducting a detailed system inventory of

embedded systems. This must include their functionality and interfaces with other systems.

- **Assessment:** Once systems are inventoried, the agreements for these products must be located and reviewed for remedies. The State Controller's Office and the contract review attorneys in the Attorney General's Office should be involved in coordinating the identification of the State's remedies. Agencies should then implement their remedies through their designated assistant attorney general.

Systems must be prioritized for action based on: (1) Criticality of function performed—does system support a function **critical** to the operation or mission of the agency that must be converted and/or replaced (first level priority) — does system support an important function of the agency that should be converted or replaced (second level priority)— or does system support a marginal function that may be converted or later replaced (third priority). (2) Risk of State tort or contract liability for system failure; and, (3) Time limits on the exercise of the State's contract or other remedies.

- **Renovation:** The renovation —conversion, replacement or retirement— phase involves identifying the manufacturer of the system and contacting the manufacturer to ascertain whether or not the embedded system is Year 2000 compliant and if not, if the system can be converted or replaced.
- **Validation/Testing:** The length of the validation and test phase and costs are driven by the complexity inherent in the Year 2000 problem. All converted or replaced embedded systems must be thoroughly validated and tested to: (1) uncover errors introduced during the renovation phase, (2) validate Year 2000 compliance and (3) verify operational readiness.
- **Implementation:** Once converted or replaced and subsequently tested, systems must be reintegrated into the production environment.

## ***VIII. CONCLUSION***

The coming of the millennium and issues associated with embedded systems presents significant problems for all of us. The problems are solvable if agencies take quick and effective action. Every aspect of this response must be carefully planned, including an assessment of the legal issues. Agencies that recognize the potential impact of the Year 2000 problems and take action to address them now, will have a distinct advantage over those who do little or nothing. In the final analysis, the best proactive action is to plan now to solve the problem. If we as a State collectively move forward in addressing the issues suggested by Embedded Systems in the Year 2000, the State will be fairly safe from the problems identified in this executive briefing.

## IX. STRATEGIC PLAN OF ACTION

NOTE DATES ASSIGNED PENDING APPROVAL OF CORE TASK FORCE

PHASE OF PROGRAM IMPLEMENTATION	ACTION ITEM	REQUIRED RESOURCES AND EXPERTISE	RESPONSIBLE OFFICIAL	START DATE	END DATE
<b>1. PRE-PHASE IMPLEMENTATION</b>	1.1. Complete identification and appointment of Y2K-Embedded Systems Project Task Force	N/A	Susana Villescas	12/9/97	12/10/97
	1.2. Establish Meeting Dates: (At the beginning of the program implementation phase, Task Force will meet every two weeks)	N/A	Susana Villescas	12/17/97	12/17/97
<b>2. AWARENESS</b>	2.1 Research existing methodologies and design of tools to inventory and record embedded systems	N/A	Susana Villescas	12/9/97	12/11/97
	2.2 Conduct presentation of the Y2K Embedded Systems Project throughout State agencies	Must be knowledgeable of the Y2K Embedded Systems Project and/or be a member of the Y2K Embedded Systems Steering Committee	Susana Villescas		
	2.3. Publicize: Write Technical Bulletin regarding Y2K - Embedded Systems for Stateline January 1998 issue	Writing skills and some knowledge of Embedded Systems	Susana Villescas	12/17/97	1/6/98
	2.4. Notify all Executive Directors and Presidents through letter format, the requirement to identify an agency representative who will represent their agency on Y2K issues. Agency representative will be part of an expanded task force and will be the point of contact for the Y2K Embedded Systems Project Task Force	Some knowledge of Y2K embedded Systems within the respective agency and knowledge for solving interface problems.	Susana Villescas	2/17/97	4/98
	2.5 Rewrite Y2K Embedded Systems Contract Language to comply with Year 2000 requirements	Legal Contract Knowledge and knowledge of State contracts and procurement	Richard Pennington & Jane Lopez		
	2.5. Identify the network of Y2K Embedded Systems Program Coordinators and publicize to all agencies.		Susana Villescas	3/98	4/98
<b>3. INVENTORY</b>	3.1. Design and Develop tool (assessment guide) for the inventory of embedded systems.	Some knowledge of inventory of systems and gathering and sorting of information		1/98	4/98

PHASE OF PROGRAM IMPLEMENTATION	ACTION ITEM	REQUIRED RESOURCES AND EXPERTISE	RESPONSIBLE OFFICIAL	START DATE	END DATE
	3.2 Design and Develop a data base to store and track inventory	*		3/98	4/98
	3.3. Identify, prioritize and mobilize needed resources to conduct inventory.	*		3/98	4/98
	3.4. Conduct inventory of Embedded Systems	*		4/98	5/98
	3.5. Locate relevant agreements and work with agency counsel in attempting to timely exercise whatever remedies may be available according to a priority list.	*		4/98	5/98
	3.6. Contact manufacturers in writing as to whether or not embedded system (s) is Y2K compliant	*		4/98	6/98
<b>4. ASSESSMENT</b>	4.1 Analyze embedded systems portfolio	*		1998	1998
	4.2. Prioritize systems and components to be converted or replaced.	*		1998	1998
	4.3. Establish project teams for business areas and major systems	*		1998	1998
	4.4. Identify, prioritize and mobilize needed resources	*		1998	1998
	4.5. Develop validation strategies, and testing plans	*		1998	1998
	4.6. Address implementation schedule issues	*		1998	1998
	4.7. Address interface issues	*		1998	1998
	4.8. Initiate the development of contingency plans for mission-critical systems.	*		1998	1998
<b>5. RENOVATION</b>	5.1. Convert selected systems and related system component.	*		1999	1999
	5.2. Replace selected system components	*		1999	1999
	5.3. Retire selected systems.	*		1999	1999
	5.4. Track conversion and replacement process	*		1999	1999
	5.5. Share information among Expanded Y2K Embedded Systems Committee	*		1999	1999

PHASE OF PROGRAM IMPLEMENTATION	ACTION ITEM	REQUIRED RESOURCES AND EXPERTISE	RESPONSIBLE OFFICIAL	START DATE	END DATE
	(State Coordinators)				
<b>6. VALIDATION AND TESTING</b>	6.1 Schedule system tests	*		1999	1999
	6.2. Develop and document test and compliance plans and schedules	*		1999	1999
	6.3. Perform system testing to ensure that the converted or replaced system and accompanying components are functionally correct and Year 2000 compliant.	*		1999	1999
	6.4. Define, collect and use test metrics to manage the testing and validation process.	*		1999	1999
	6.5. Initiate acceptance testing	*		1999	1999
<b>7.IMPLEMENTATION</b>	7.1. Develop implementation schedule	*			
	7.2. Resolve interface issues.	*		1999	1999
	7.3. Complete acceptance testing	*		1999	1999
	7.4. Implement contingency plans to ensure support for business systems that may be interrupted by the failure to achieve Year 2000 compliance of a specific mission-critical system.	*		1999	1999
	7.5. Reintegrate the converted and replaced systems into the environment.	*		1999	1999

\* To be identified by Core Task Force