Contingency and Consequence Management Planning for Year 2000 Conversion

A Guide for State and Local Emergency Managers

February 1999

TABLE OF CONTENTS

LIST OF TABLES

The Federal Emergency Management Agency (FEMA) has produced this guide to help State and local emergency managers meet the Year 2000 (Y2K) challenge by developing effective contingency plans. The National Emergency Management Association and the International Association of Emergency Managers provided helpful advice in the development of this guide.

Other information sources used include:

American Red Cross

Chief Information Officers Council Committee on Year 2000

Commonwealth of Pennsylvania and the Government of Canada

Environmental Systems Research Institute, Inc.

Gartner Group

General Accounting Office

League of Minnesota Cities

Metropolitan Washington Council of Governments

President's Council on Year 2000 Conversion

State of Florida Year 2000 Project Office

State of Kansas, Department of Administration, Division of Information Systems and Communications

State of Minnesota, Department of Public Safety, Division of Emergency Management

State of New Hampshire, Office of Emergency Management

State of Texas, Department of Information Resources

Many other States, municipalities, Federal agencies, and private organizations have developed helpful Y2K publications or web sites. The web sites listed in this guide will link you to basic information that is currently available. New sites are constantly appearing and old sites are sometimes changed, so be sure to keep checking for useful information. You can also call **1-888-USA-4-Y2K** for information on a range of topics.

The approaches described in this guide are recommendations, not regulations. Following them will not, in itself, ensure compliance with any applicable Federal, State, or local regulations. Nor will it ensure that you will not experience Y2K disruptions.

If you are just starting to address the Y2K problem in your State or communities, *Section 1, Getting Started,* provides a brief overview of:

- the Y2K problem
- who and what it could affect
- the basics of checking systems
- the actions being taken by the Federal government
- the actions that you should take now

Sections 2–5 provide more detailed information on:

- assessing risks
- testing systems
- developing consequence management plans

1. GETTING STARTED

These days, almost every newspaper and magazine has printed articles about the Year 2000 or "Y2K" problem. Some of these stories are downright scary. They predict massive failures of power systems, transportation networks, communications, and other systems at the stroke of midnight, December 31, 1999.

Are they right about what will happen? And if the stories are true, or even partly true, is there anything you can do about it?

The message of this guide is simple:

> **You CAN get control of the problem through planning and preparation — the same kind of planning and preparation you do regularly in your work as an emergency manager.**

As an emergency manager, your primary focus should be on protecting public safety and health if Y2K-related incidents occur. This guide will help you in the process. It describes the nature of the Y2K problem and explains what you can do to prepare for it. In a nutshell, you need to take the following steps:

- **Assess risk** – Get a handle on the size of the problem, both in your communities and in your emergency response agencies.
- **Keep your own agency running** – Make sure your own systems are prepared for the transition to the new century, and be sure to plan how you will operate if some of your systems do have problems.
- **Develop a consequence management plan** – Prepare a plan for protecting public safety and health if systems in your community have problems and you must respond.

What Is the Y2K Problem?

The Y2K technology problem, also called the "millennium bug," is something we have inherited from the early days of computers. Back then, computer memory was scarce and expensive, so programmers used a 2-digit entry to designate each year instead of a 4-digit entry. For example, 1999 was entered as 99.

Unfortunately, the 2-digit date format cannot process dates in two different centuries. So when the year 2000 arrives, systems that have the 2-digit year codes may interpret the year "00" to be "1900." These systems simply cannot tell the difference between the years 2000 and 1900 unless they have been fixed ahead of time.

However, 1/1/2000 is not the only critical date! In fact, some experts believe that as few as 8% of Y2K problems will occur on 1/1/2000; the rest will occur at another time. See *Section 2* for other dates of concern.

Who Could Be Affected?

Any person using or communicating with a computer or computer-driven product or system could be affected. Remember that the systems that could be affected are not just the actual "computers" or computer software. Any equipment with "embedded" computer chips could be affected.

Table 1. Some Infrastructure Systems at Risk

Building and Security	Elevators, electronic locks, burglar and fire alarms, sprinklers, photo surveillance equipment, HVAC equipment, parking lot barriers, equipment maintenance scheduling services, and card lock systems
Communications	Radios, mobile phones, fax and telex machines, telephones and switches, pagers, closed-circuit TV cameras/monitors, intranets, and internets
Emergency Services	911 (dispatch and public warning), weather warning devices
Finance	Banks, cash machines, and credit cards
Food Service	Refrigeration, freezing, ice-making, and distribution
Health	Hospitals, pharmacies, nursing homes, emergency medical services and equipment
Office	Time clocks and stamps
Public Response	Police, fire, and emergency medical services and public works
Transportation	Roads (traffic light controllers and vehicle operations), air, and railroads
Utility Power	Electric (generation and distribution), gas and oil (pipelines and distribution)
Water and Sewage	Distribution and wastewater treatment

What Infrastructure Systems Could Be Affected?

Progress is being made daily in ensuring that systems are Y2K compliant. Still, failures could occur in many kinds of systems that matter to emergency managers. Table 1 shows some of the systems and associated devices that could be affected.

The interconnectedness of many of these systems creates part of the risk associated with the Year 2000. As a result, you need to evaluate all systems, not just your own computer systems, for Y2K compliance. *Section 2* contains more information on these at-risk systems.

Why Should I Be Concerned about the Year 2000 Problem?

The computerized systems that may fail as a result of the bug could have an impact on your community — the same kind of impact as a natural or man-made disaster. For example, if electrical systems fail, people may need shelter, food, water, information, transportation assistance, financial help, etc.

Progress is being made daily to minimize the public safety and health impacts of potential Y2K disruptions. The all-hazards practices and techniques you routinely use for other disasters and emergencies should well serve our nation in planning for the potential consequences of Y2K conversion.

As an emergency manager, you need to understand the problem, be prepared, and be ready to provide help. You need to protect systems within your own organization, so it remains operational. Also, you should promote action on the Y2K issue in your communities. Include action by all of your communities' critical service providers.

How Can I Verify That All My Systems Are OK?

Start by checking all levels of computer technology in your systems and organizations. Begin with the systems that are most critical to your agencies' ability to function. Problems can occur in any of the levels shown in Table 2, even though the other levels are OK.

See *Section 3* for more information on these levels of technology and what to do about them.

Table 2. Levels of Computer Technology

Hardware	The chip architecture and the machine's internal clock
Operating Systems	Even some recent operating systems require upgrades
Databases	All of the files and data used by your applications
Applications	Software and word processors, spreadsheets, geographic information systems, and hazard models
Custom Code	The code built on top of applications
Embedded Systems	Many devices contain computer chips. Get information from suppliers. If you cannot, you might implement planned replacement/upgrades or devise a way to work around the failed device.

What Kinds of Plans Do I Need?

This guide promotes "Contingency and Consequence Management Planning." The Y2K community uses the term "contingency planning" to reflect the uncertainty regarding Y2K disruptions. "Consequence management planning" for specific hazards is a more familiar term to the emergency management community.

If you have an all-hazards emergency operations plan, you can use this guide to develop a hazard-specific Y2K attachment to it. If not, you can use this guide to develop a stand-alone Y2K plan.

Which Functional Areas Need Plans?

Your job will be to help maintain public safety and health. To do that, you must maintain normal operations as much as possible. To respond to disruptions, you may need to activate plans for operational continuity or consequence management.

Be sure you have plans to deal with disruptions in the following areas. Some mainly affect your own operations or the public. Others affect both. But all are important.

- Emergency services
- Emergency Operations Centers (EOCs)
- 911 systems
- Public warning and information
- Health services
- Communications
- Utility power
- Water and sewage
- Public works and facilities
- Transportation

How Do I Develop a Contingency Plan?

Planning for either continuity of operations or consequence management has four basic steps:

- ❑ Identify the problem areas
- ❑ Develop the plan
- ❑ Test it
- ❑ Implement the plan

These steps will help you deal with potential Y2K problems and help you find a stable, workable solution. In *Sections 3 and 4*, you will be guided through this important process.

When Should I Plan?

Start now! Just as when you develop plans for other hazards, you must allow enough time to test your plan before you need to activate it. We can't tell you which time frames to use, because communities vary widely in size and complexity. States and many local governments have already begun this process.

If you are just beginning, here are some possible time frames for phases of the planning process:

Identify the problem areas	February – March 1999
Develop the plan	March – May 1999
Test the plan	
Train response personnel	June – July 1999
Conduct drills and exercises	July – November 1999
Revise the plan as needed	Up to November 1999
Implement the plan	
Inform the public	February 1999 – January 2000
Acquire resources	May – June 1999
Activate the plan	December 1999 – January 2000

How Can I Promote Community-Wide Readiness?

Some of the most important work in emergency response takes place at the State and local levels. You have a key role in assuring preparedness — right now!

As you assess the possible consequences of Y2K conversion, you should work with critical service providers in your area — both public and private. Encourage them to take steps to ensure that their systems are Y2K compliant. State officials should reach out to local governments to determine their progress. Encourage them to inform the public about the status of key services — like power and water — and about how local officials are preparing to respond to any disruptions.

How Can I Help the Public Prepare?

To relieve anxieties and help people prepare for Y2K, you should conduct public outreach. Tell people that government at all levels, as well as business and industry, are working together to solve the problem and ensure that public health and safety services won't be disrupted when the new millennium starts.

Distribute brochures on Y2K through schools, local employers, public meetings, and community groups. Encourage people to get more involved in all-hazards emergency planning and help them understand the emergency procedures that are already in place. See *Section 4* for a list of helpful brochures.

In addition, you may want to suggest to the public these preparations for Y2K:

- Checking with manufacturers of any essential computer-controlled equipment in the home
- Preparing basic emergency supply kits
- Checking home smoke alarms and buying extra batteries
- Keeping a battery-operated radio or television available to be able to receive emergency information

Tell the public that they should prepare for Y2K disruptions in the same way they prepare for other problems, such as winter storms or tornadoes. For more information, see *Section 4.* FEMA's Community and Family Preparedness Program offers resources to help individuals and communities in emergency preparedness.

What Else Can I Do?

Work with your communities to develop Y2K awareness. Be sure that you are included in local planning groups; or volunteer to lead these groups if necessary. Develop a common message for public dissemination on local Y2K preparedness.

Once you have developed a contingency plan, you should develop an incident management plan in case failures do occur. Within your own organization, make sure that you have protocol information for contacting local or state emergency management officials if communication systems are affected. Decide whether you should activate your EOCs during the transition.

What Is FEMA Doing to Prepare for Nationwide Response?

FEMA is involved in several activities to prepare for Y2K. These include:

- Chairing the Emergency Services Sector Working Group of the President's Council on Year 2000 Conversion
- Conducting Regional Interagency Steering Committee Y2K workshops in all ten Regions: February – March 1999, August – September 1999, and December 1999
- Developing a short course on Y2K for State and local emergency managers
- Conducting Emergency Educational Network broadcasts on Y2K, March 1999 through January 2000
- Establishing a Y2K information clearinghouse
- Conducting Federal monitoring operations December 29, 1999 – January 4, 2000

Because of the potential for numerous, small-scale emergencies across the country, State and local response teams may be overwhelmed in their efforts to save lives and protect property, public health, and safety. Consequently, FEMA is currently developing an Operations Supplement to the Federal Response Plan (FRP) that describes the federal actions and operations that are needed to respond to the possible consequences of Y2K.

This supplement will address federal response operations beyond the current scope of the FRP — operations necessary to deal with the unique circumstances presented by Y2K problems. It will also cover the monitoring actions that FEMA will take prior to the millennium. The Operations Supplement is scheduled to be published by July 1, 1999.

However, FEMA assistance cannot substitute for personal responsibility taken by individuals and organizations to address their own situations. FEMA cannot prevent computer disruption beyond its own agency, nor can it respond to the underlying technical causes of computer disruption. In addition, there may be competing demands for resources if Y2K problems arise simultaneously across the nation. So States and local communities must be prepared to be self-sufficient for a period of time if Y2K disruptions are serious.

How Are State and Local Governments Addressing the Problem?

State, county, and local governments are working hard to address potential Y2K problems. Along with checking that their own computer systems are Y2K compliant, they are developing contingency plans to address potential failures in public and private services. Organizations with successful Y2K programs have:

- Gained the interest and support of high-level management
- Established and used commissions and planning or working groups to coordinate efforts
- Developed Y2K guidebooks or manuals to help government, business, industry, and individuals understand and deal with Y2K problems
- Examined and strengthened mutual aid agreements
- Initiated public outreach programs

Where Can I Find Useful Information about the Y2K Problem?

A lot of information has been generated about this problem. It is available from agencies and organizations, is located in books and magazines, and can be found on the World Wide Web. Finding information about relevant emergency management concepts and practices, however, can be both time-consuming and frustrating, since so much information is available. *Section 5* contains an annotated list of some information sources that can be useful to emergency managers.

2. GETTING CONTROL OF THE PROBLEM — ASSESSING RISK

The first step in preparing for Y2K emergencies is to assess the threat. What is the nature of the hazard? What systems are at risk? How vulnerable are your communities and your emergency response agencies?

The planning process is similar to the one you use for other technological emergencies, but Y2K problems do have some unique features. They may affect:

- Many kinds of systems at the same time
- Many geographical areas — your jurisdiction and others — at the same time

And though the time of impact is predictable to a certain extent, it won't necessarily be at midnight on December 31, 1999.

How Widespread Is the Problem?

To be blunt, the problem is pervasive. Just think of all the things we do every day that are now affected by computer systems.

These systems can be divided into two types: (1) *information technology (IT) systems* and (2) *systems that contain embedded chips*. IT systems include computer hardware and software — from the large computer systems that support large government agencies to the personal computers on people's desks. A wide variety of other devices and products contain embedded microprocessors (computer chips).

Some examples of IT systems are:

- Payroll systems
- Accounting and receivable systems
- Inventory systems
- Local or area-wide networks
- Management information systems
- Geographic information systems

Some examples of systems containing embedded chips are:

- Communications systems
- Traffic control and street light systems
- Building security and fire systems
- Elevators
- Automated heating and cooling systems
- Basic office equipment
- Electrical monitoring and distribution devices used by utility companies
- Biomedical equipment used in hospitals and nursing homes

These systems expand the scope of the Y2K problem. These devices and products have become essential, affecting nearly everything we do. Thousands of electrical and mechanical devices that we use in our private lives and during normal, day-to-day business are controlled by microprocessors. If these "invisible computers" fail, the effects could range from annoyance to disaster.

Many computers also are interconnected. A system may work fine by itself; but when it communicates with another system, it may experience Y2K problems.

Your best defense is to become aware of what can happen and prepare for it. Check the list of *Equipment and Systems to Check for Y2K Problems* on the next pages; it will help you start thinking about your communities' potential risk.

Table 3. Equipment and Systems to Check for Y2K Problems

Note: Read the list in its entirety because some equipment is multidepartmental. The list is not necessarily comprehensive; jurisdictions may find additional suspect equipment.

Office Equipment

_____ telephone systems
_____ voice mail/answering machines
_____ facsimile (fax) machines
_____ photocopiers
_____ printers
_____ scanners
_____ equipment w/ date stamps (video equipment, scales, time clocks)
_____ personal computers
_____ laptop computers
_____ personal digital assistants (PDAs)/handheld computers
_____ wireless communication systems (pagers, cellular phones)
_____ mailroom equipment
_____ other

Emergency Response: Police and Fire Operations

_____ emergency response phone and dispatch systems
_____ global positioning systems (GPS) used to track vehicles
_____ EMT medical equipment (defibrillator, monitoring devices, blood analyzer)
_____ breathalyzer
_____ criminal records systems
_____ response vehicles, fire trucks, ambulances
_____ two-way radio systems
_____ wireless communication systems (cellular phones, pagers)
_____ radar systems
_____ security systems (door locks, safes, vaults)
_____ motion detectors
_____ parking ticket handheld devices
_____ police and fire computer-aided dispatch systems
_____ surveillance cameras
_____ air traffic control systems
_____ fuel dispensing systems (gas pumps)
_____ contingent systems (systems or functions that are operated by others, but on which the jurisdiction depends for its emergency response operations)
_____ 911 systems
_____ public warning systems
_____ other

Public Works

_____ traffic control systems
_____ flood/storm water control systems
_____ electronic scales
_____ meters
_____ handheld water meter readers
_____ street maintenance systems
_____ geographic information systems
_____ street lighting
_____ sprinkler/fountain systems
_____ fuel dispensing systems (gas pumps)
_____ maintenance vehicles
_____ other

Water and Wastewater Systems

_____ pump controller systems
_____ chlorine injection or other effluent disinfecting systems (ultraviolet lights)
_____ lift station pump controllers
_____ telemetry systems
_____ vehicle computer systems
_____ equipment computer systems (mobile generators, mobile pumping equipment, construction equipment, maintenance and line cleaning equipment)
_____ wastewater line televising equipment
_____ contingent systems or functions (systems or functions operated by others but on which the jurisdiction depends for its sewer/wastewater operations)
_____ other

Building Inspections

_____ electrical generation and distribution
_____ gas distribution
_____ elevators, escalators, lifts
_____ building and premises security systems

_____ badge access systems
_____ emergency systems (power generators, lights, HVAC systems)
_____ engineering permits
_____ engineering assessments reporting
_____ fire control systems (alarms, sprinkler systems)
_____ other

Administration/Finance
_____ utility billing systems
_____ revenue systems (tracking of parking tickets, invoices, assessments, business licenses)
_____ financial accounting systems
_____ purchasing systems
_____ payroll
_____ tax collections
_____ credit cards

Computer Network Resources
_____ routers
_____ modems
_____ switches
_____ file servers
_____ disk controllers and drivers
_____ backup hardware and software
_____ print servers
_____ repeaters
_____ uninterruptible power supplies and software
_____ hubs
_____ CD-ROM towers

Software
_____ operating system software
_____ desktop publishing software
_____ graphics software
_____ desktop applications
_____ optical character reading (OCR) software
_____ virus scanning software
_____ desktop utility software
_____ custom software (desktop and network-based)
_____ network operating software
_____ network management software
_____ client/server software
_____ imaging software
_____ other

Nursing Homes and Hospitals
_____ medical equipment
_____ clinical records/patient information
_____ accounts payable/ receivable systems
_____ HVAC systems
_____ electronic billing system for Medicare and Medicaid
_____ food suppliers
_____ pharmaceutical suppliers
_____ medical supply vendors
_____ housekeeping supply vendors
_____ other

Utilities
_____ energy control systems
_____ power grid systems
_____ power plants/stations
_____ other

Interfaces
_____ banks
_____ other governmental entities
_____ automatic payroll
_____ billing
_____ dispatch
_____ other

Service Providers
_____ banks
_____ ATM machines
_____ bonding firms
_____ legal firms
_____ appraisal companies
_____ landfills
_____ maintenance companies
_____ trash collection companies
_____ electric utilities
_____ insurance providers
_____ telecommunications companies
_____ other

Food Storage and Distribution
_____ refrigerators
_____ freezers
_____ ice makers

Other
_____ railroad switching systems
_____ robots
_____ satellites
_____ library cards
_____ other

Source: Adapted from A Year 2000 Action Guide, League of Minnesota Cities, 1998.

How Can I Tell If I Have an Embedded Chip Product?

Check to see if it:

- Has an LED (light-emitting diode) maintenance or operations panel with menu options
- Stores data for further use
- Has an internal clock
- Has controls for changing functions on the basis of times or dates
- Communicates with the user or operator, either visually or with sound
- Displays a time/date

What Can I Do About These Devices?

Conduct an internal inventory to identify all items that may contain chip technology and all services that depend on them. Then try to check whether each product is Y2K compliant.

You should request letters certifying Y2K compliance from all of the applicable vendors. Be sure to insist that they describe the methods they used to determine compliance. If a vendor/supplier says its product is not compliant, develop a contingency plan to either replace the product or to deal with its failure.

When Will the Problem Strike?

Most of the publicity about Y2K points to problems on January 1, 2000. But that is not the only critical date. Some experts predict a string of malfunctions throughout 1999 and 2000, rather than a single calamity. Why is this the case? Because programmers enter dates differently in different systems and products. Table 4 lists some of the dates that could cause problems and explains why.

Table 4. Important Dates for Y2K

December 31, 1999 – January 1, 2000	Last day of 1999, first day of 2000
Throughout 1999	One-year look-ahead date
April 9, 1999	May be mistaken for "end of file" code
September 9, 1999	May be mistaken for "end of file" code
February 29, 2000 – March 1, 2000	Uncommon leap year
December 31, 2000	366th day of uncommon leap year
August 22, 1999	Rollover date for GPS systems
July 1, 1999 to October 1, 1999 (various months)	Start of government fiscal year 2000
January 10, 2000	First date in the year 2000 with 7 digits
October 10, 2000	First date in the year 2000 with 8 digits

As an emergency manager, you also must monitor and respond to Y2K problems that could occur days or weeks after January 1, 2000. Some incidents might initially seem unimportant, but they could turn into threats to public safety and health. For example, a medical facility's treatment equipment might be working; but if its payroll system were to be disrupted for very long, the facility might have to close. Or a power plant in one location might be operational but have to shut down after a few weeks if Y2K disruptions elsewhere were to stop fuel shipments.

Publications and web sites devoted to testing systems for Y2K compliance list other dates that should be included in a complete system test. See the references listed under "Resources for Testing Your Systems" in *Section 3*.

Vulnerability Analysis

Potential disruptions caused by Y2K problems are similar to other technological emergencies, so you can apply FEMA's all-hazards planning guidance (State and Local Guide 101, *Guide for All-Hazard Emergency Operations Planning*, September, 1996) to Y2K problems as well.

In addition, FEMA 141, *Emergency Management Guide for Business and Industry* (October 1993) includes a section on planning for technological emergencies. You may want to consult the whole guide. See *Section 5* for information about getting a copy.

The initial focus of contingency planning should be on those systems that you identify as most critical to your agencies' operations and to your communities. Vulnerability analysis will help you identify these systems. Here are some excerpts on vulnerability analysis from FEMA 141 to help you prepare.

Use the *Vulnerability Analysis Chart* (Table 5) to assess the probability and potential impact of Y2K emergencies. The process entails identifying potential problems, assigning probabilities, estimating impacts, and assessing resources, using a numerical system. The lower the score, the better.

Directions for Using the Vulnerability Analysis Chart

❑ List Potential System Failures

In the first column of the chart, list the Y2K failures that could affect you, such as:

- Safety system failure
- Telecommunications failure
- Computer system failure
- Power failure
- Heating/cooling system failure
- Emergency notification system failure

❑ Estimate Probability

In the Probability column, rate the likelihood of each emergency's occurrence. Judging the likelihood of Y2K failures is difficult in large systems like communications or transportation. Even the experts disagree. But you don't have to be highly precise. Use a simple scale of 1 to 5, with 1 as the lowest probability and 5 as the highest. This is a subjective consideration, but it is still useful.

❑ Assess the Potential Human Impact

In your work as an emergency manager, this step is critical. Analyze the potential impact that each emergency could have on people, such as the possibility of death or injury. Assign a rating in the Human Impact column of the Vulnerability Analysis Chart. Use a 1 to 5 scale, with 1 as the lowest impact and 5 as the highest. In this area, for example, 1 might equal discomfort, and 5 a loss of life or limb.

❑ Assess the Potential Property Impact

Consider the potential for property losses and damage. Again, assign a rating in the Property Impact column, 1 being the lowest and 5 being the highest. Consider:

- Cost to replace
- Cost for temporary replacement
- Cost to repair

❑ Assess the Potential Business Impact

Assign a rating in the Business Impact column. Again, 1 is the lowest, and 5 is the highest. Assess the impact of:

- Business interruption
- Employees unable to report to work
- Imposition of penalties or legal costs
- Interruption of critical supplies or services

❑ Assess Internal and External Resources

Next assess your resources and ability to respond. Consider each potential emergency from beginning to end and each resource that would be needed to respond. Assign a number to your internal and external resources. The lower the number, the better. Ask yourself:

- Do we have the needed resources and capabilities to respond?
- Will external resources be able to respond to us for this emergency as quickly as we may need them. Or will they have other higher priority areas to serve?

If the answers to these two questions are yes, move to the next assessment. If the answers are no, identify what can be done to correct the problem. For example, you may need to:

- Develop additional emergency procedures
- Conduct additional training
- Acquire additional equipment
- Establish or modify mutual aid agreements
- Establish agreements with specialized contractors

❑ Add the Columns

Add the numbers for each emergency. The lower the number, the better. While this is a subjective rating, comparing the numbers will help you determine planning and resource priorities.

Table 5. Vulnerability Analysis Chart

Type of System Failure	Probability	Human Impact	Property Impact	Business Impact	Internal Resources	External Resources	Total
	High (5) ↔ Low (1)	High Impact (5) ↔ Low Impact (1)			Weak Resources (5) ↔ Strong Resources (1)		

Source: FEMA 141

The lower the score the better

3. GETTING CONTROL OF THE PROBLEM — KEEPING YOUR OWN AGENCY RUNNING

If your emergency response agencies are at risk from Y2K problems, you need to plan ahead in order to keep operating if they strike. That's the only way you'll be able to help your communities.

Keep in mind that the Y2K problem could affect both computers and computer-driven products or systems. It could also affect many electronic devices that are common in emergency management. Remember — check all devices and systems that could be affected by the Y2K problem.

How Will I Know If My Own Systems Are Y2K Compliant?

NOTE: This guide does not give detailed instructions for testing systems for Y2K compliance. Instructions and tools are available on many State and commercial web sites. A partial list appears later in this section.

You cannot test your systems by just setting your computer's clock to 11:59 PM, December 31, 1999, and waiting 1 minute to see what happens. Problems may exist on many different levels, so you must ensure that all technology levels of your systems are Y2K compliant. Check with vendors and other experts to ensure Y2K compliance.

❑ Check Your Hardware

This task should cover both the specific chip architecture and the machine's internal clock. Check the web sites or user support lines of your hardware vendor and your operating system vendor for Y2K issues. Use either firmware changes from the hardware vendor or operating system patches.

❑ Check Your Operating System

Even some recent operating systems require upgrades to be fully Y2K compliant. Check your vendor's web site or user support line for Y2K issues.

❑ Check Your Databases and Files

These include all of the files and data used by your applications. Dates can be stored in any of your databases. Check to ensure their data management system is Y2K compliant. Also ensure that any custom date usage is based on 4-digit years or that you have a clear method for processing 2-digit years stored in custom date fields.

❑ Check Your Applications and Run-Time Libraries

Applications software runs on your operating system and works with various databases. Ensure that all applications you use and their run-time libraries are Y2K compliant. Check your application vendor's web site or user support line for Y2K issues.

❑ Check Your Custom Code

Custom applications are either built on top of application software or use application software components. Even though the underlying applications are Y2K compliant, the custom code may not be. Establish guidelines for testing your code to ensure that it is Y2K compliant. Accept only Y2K-certified applications from third-party developers.

Resources for Testing Your Systems

Many web sites list testing procedures and have software tools available for testing your systems. For example, see the following:

http://y2k.state.wi.us/
http://www.usfa.fema.gov/
http://www.nist.gov/

The web sites of many States also provide information, tools, and links to other web sites. The information on these sites and elsewhere is highly technical because the problem is complicated. You may need the help of an IT expert to solve it.

Where Can I Get Help in Fixing My Systems?

Many of the same sources listed for testing your systems also have software available for repairing some problems. Hardware and software vendors' web sites may have updates that you can use to fix their particular products.

Many service providers can help fix your systems, but FEMA cannot endorse specific private firms. You may be able to get help or advice on private firms from your State's information technology staff.

You can also locate resource lists of service providers on the World Wide Web by doing a keyword search. Try using search terms such as "Year 2000" or "Y2K."

Planning for Continuity of Operations

Even if you've tried to ensure that all your systems are Y2K compliant, you may suffer some unexpected failures. So plan ahead to keep your agency running and able to provide service in case of system failures.

In this regard, you're like any other agency or commercial business. So the guidance that has been written for them is good for you, too. There's extensive guidance on operations continuity planning in the web sites and publications listed in *Section 5*. To get you started, here's a step-by-step process taken from the General Accounting Office, *Year 2000 Computing Crisis: Business Continuity and Contingency Planning*, GAO/AIMD-10.1.19, August 1998. For a complete copy, see http://www.gao.gov/special.pubs/bcpguide.pdf

The following steps will help you plan for continuity of operations.

Steps for Continuity Planning

Step 1. Initiation

- ❑ Establish an operations continuity project work group
- ❑ Develop and document a high-level operations continuity planning strategy
- ❑ Identify core processes for operations
- ❑ Define roles and assign responsibilities
- ❑ Develop a master schedule and milestones
- ❑ Implement a risk management process and establish a reporting system
- ❑ Assess existing continuity, contingency, and disaster recovery plans and capabilities for core operations
- ❑ Implement quality assurance reviews

Step 2. Operations Impact Analysis

- ❑ Define and document information requirements, methods, and techniques to be used in developing the operations continuity plan
- ❑ Define and document Year 2000 failure scenarios
- ❑ Perform risk and impact analyses of each core operations process
- ❑ Assess and document infrastructure risks
- ❑ Define the minimum acceptable level of outputs and services for each core operations process

Step 3. Contingency Planning

- ❑ Assess the cost and benefits of identified alternatives and select the best contingency strategy for each core operations process
- ❑ Identify and document contingency plans and implementation modes
- ❑ Define and document triggers for activating contingency plans
- ❑ Establish a resumption team for each core operations process
- ❑ Develop and document a zero day strategy and procedures

Step 4. Testing

- ❑ Validate your operations continuity strategy
- ❑ Develop and document contingency test plans
- ❑ Establish test teams and acquire contingency resources
- ❑ Prepare for and execute tests
- ❑ Validate the capability of contingency plans
- ❑ Rehearse operations resumption teams
- ❑ Update the continuity plan based on lessons learned and re-test if necessary
- ❑ Update disaster recovery plans and procedures

4. GETTING CONTROL OF THE PROBLEM — YOUR CONSEQUENCE MANAGEMENT PLAN

No matter how well you have assessed the risk of Y2K problems and addressed them in your own jurisdiction, you need to have a Y2K Consequence Management Plan. That way, you will be prepared for what might happen if Year 2000-related problems actually occur despite efforts to avoid or prevent them. Such a plan, which deals with the consequences rather than the causes of a failure, will help you to:

- Reduce the number of decisions to be made during response and recovery operations
- Provide and restore critical services quickly
- Minimize the impact on public safety and health
- Restore all your jurisdiction's services in a timely and cost-effective manner

Where to begin? Often the first step is the most difficult. Here is a suggested approach. Fill in the blanks with the organizations, facilities, and resources that apply to you. You probably have done some of these things already and can fill in many blanks without doing further research.

As you follow these steps, remember to work with all of your communities' critical service providers. Encourage them to take steps to ensure that all of their critical systems are Y2K compliant.

Gathering Information for Your Plan

Step 1. Identify the Potential Impact on Your Jurisdiction

Imagining the results of these outages can help you start planning for them. (Also see the Vulnerability Analysis in *Section 2*.)

Power

Loss of electrical power

_____

_____

Loss of natural gas

_____

_____

Communications

Loss of telephones/pagers/radios

_____

_____

Loss of sirens/EAS

_____

_____

Water and Sewage

Interruption in water supply

_____

_____

Problems with sewage service

_____

_____

Emergency Services

911 service

Fire service vehicles and equipment

Law enforcement vehicles and equipment

Mutual aid resources

Emergency Operations Center

Medical

Ambulance vehicles and equipment

Hospital systems and equipment

Nursing homes

_____

_____

Public Works and Facilities

Street and traffic lights

_____

_____

Vehicles and equipment

_____

_____

Airports

_____

_____

Government buildings

_____

_____

Correctional facilities

_____

_____

Schools

_____

_____

Step 2. Identify Potential Community Resources

Identify and designate backup resources in the event that primary systems fail.

Generators for backup power for critical facilities

_____

_____

_____

Alternate methods of communications

_____

_____

_____

Food supplies

_____

_____

_____

Shelters that have backup power

_____

_____

_____

Transportation services (and fuel for them)

_____

_____

_____

Step 3. Promote Interdepartmental Teamwork

Creating a Y2K Consequence Management Plan for a jurisdiction will require working with a number of departments and agencies. They will each need their own plans and will need to be aware of the overall, coordinated jurisdictional plan.

Police Department

_____

_____

Fire Department

_____

_____

Emergency Medical Services

_____

_____

Public Works Department

_____

_____

Building Inspection Department

_____

_____

Social Services Department

_____

_____

Step 4. Work with Other Governmental Units

Infrastructure problems caused by Y2K will cross jurisdictional lines. Emergency managers will need to coordinate their planning with:

State-level departments

_____

_____

_____

County offices

_____

_____

_____

City and town offices

_____

_____

_____

School district officials

_____

_____

_____

Red Cross and other non-government organizations

_____

_____

_____

Step 5. Coordinate with Utilities and Other Businesses to Prepare

Gather information on preparedness and backup plans from:

Utility companies (including suppliers of electricity, natural gas, water, telephone, and other services)

_____

_____

_____

_____

Manufacturers and vendors of equipment you depend on

_____

_____

_____

_____

Landlords of buildings that you lease

_____

_____

_____

_____

Local businesses

_____

_____

_____

_____

Step 6. Establish Communication with the Public about Y2K

Emergency managers and other local leaders should establish themselves as reliable sources of information about Y2K and communicate what they are doing to prepare for Y2K via:

Local newspapers

_____

_____

_____

Local television stations

_____

_____

_____

Local radio stations

_____

_____

_____

Local Chambers of Commerce

_____

_____

_____

Community clubs and associations (League of Women Voters, etc.)

_____

_____

_____

Organizing the Y2K Effort

Each jurisdiction should designate a person as the Y2K Coordinator to lead all efforts. In addition, each jurisdictional department should appoint someone to assess the Y2K problem for its area. These individuals will work together to create the overall Y2K consequence management plan.

To create this plan for your jurisdiction, the Emergency Management Director or Coordinator (or his/her designated Y2K Coordinator) must obtain information from all departments within the jurisdiction. First focus on those systems identified as critical in the risk assessment process. For each critical system, evaluate the likelihood of Y2K failure or malfunction and the types of problems that could result. (See *Section 2* for a listing of *Equipment and Systems to Check for Y2K Problems*). Once the potential problem areas have been identified for your jurisdiction, the departments can develop their own plans.

In addition, members of each organization should also have a personal contingency plan, so they will be available and ready to respond if there is an emergency and will not be concerned about personal matters.

The jurisdiction's overall Y2K Consequence Management Plan should cover the following elements:

- Designation of leaders and their responsibilities, including a Recovery Team Director, a Command Center (or EOC) Coordinator, and the members of the Recovery Team
- Procedures for activating plans
- Allocation of resources, including personnel, funding, and equipment
- A Communications Plan for contacting key staff (other than by telephone)
- Documentation of procedures and instructions
- Designation of a Command Center and alternate facilities

We Already Have a Comprehensive All-Hazards Plan. Can't We Just Use It for Y2K?

You probably know that FEMA advocates a comprehensive approach to emergency planning in State and Local Guide (SLG) 101, *Guide for All-Hazard Emergency Operations Planning*. This approach is still valid for the Y2K problem; but remember that there are differences between the Y2K problem and other hazards.

What are they?

- The Y2K problem could affect many local, State, and even international jurisdictions at the same time, instead of being confined to one locale or region.
- It could affect many different systems at the same time (power, transportation, communication, finance, etc.), instead of just one or two (like a power outage).
- The size of the problem could overtax local resources, and mutual aid might not be available if neighboring jurisdictions are also affected.
- In addition, State and Federal resources may be overtaxed.
- Some of the resources you usually use could be affected by the Y2K problem. For example, emergency communication systems could be inoperable, or school shelters could be without power or heat. Any resources that depend, directly or indirectly, on computer chip electronics might be unusable.

Because of these unique features of the problem, you should at least develop a Y2K hazard-specific attachment to your emergency plan. Consider what resources might be unavailable, and what alternative provisions you could make to protect public safety and health for such critical functions as these:

- Emergency services
- Emergency Operations Centers (EOCs)
- 911 systems
- Public warning and information
- Health services
- Communications
- Utility power
- Water and sewage
- Public works and facilities
- Transportation

All plans should contain the information in the checklist below.

❑ Objective of the Plan

Each plan should specify its own objective for responding to potential problems, maintaining an acceptable level of service, and minimizing the threat to public safety, health, and critical infrastructure.

❑ Criteria and Procedures for Activating the Plan

The plan should include the criteria for activating the plan, such as a predetermined length for downtime or procedures for handling a problem in a specific area of responsibility. Describe the steps for activating the plan, such as how to contact needed employees (including alternate methods to using the commercial telephone in case service is disrupted). Many emergency management and other designated jurisdiction personnel are preparing to be on stand-by or activated in the days leading up to and following December 31, 1999.

❑ Roles, Responsibilities and Authority

Designate team leaders and members and identify their responsibilities. Provide alternates for each position in case the primary designee is unavailable. These should be consistent with your general emergency response procedures.

❑ Procedures for Operating during or after System Failures

List detailed procedures for operating if systems fail (i.e., who is to do what and by when). Explain ways to operate equipment manually or to get around the problem. For several examples of such procedures, see Table 6.

❑ Resources Available to Support Emergency Operations

List resources needed and available to implement the plan. Resources can include personnel, materials, supplies, communications, and other equipment. They may be different from those needed during normal operations.

❑ Criteria and Procedures for Returning to Normal Operations

List the steps for standing down.

❑ Estimated Cost of the Plan

Document the estimated cost of activating and implementing the plan, keeping in mind that the length and severity of the problem will affect the final costs.

❑ Testing the Plan

Conduct a hands-on run-through of the plan before it is needed to see if it works. Refine the plan by incorporating lessons learned from the drill. Many communities have held such drills and exercises already. See the web sites listed in *Section 5* for examples. Test, and test again!

❑ Post-Emergency Plan

Schedule a staff debriefing after the plan has been implemented. Any lessons learned during the response phase should be noted, and changes to the jurisdiction's plans should be made accordingly.

After Table 6, you will find an example of a Y2K Consequence Management Plan, which was prepared by a local Public Works department.

Table 6. Example Procedures for Operating during or after System Failures

Services	Areas of Concern/Impact	Backup Systems/ Contingency Plans
Emergency Services		
911	Emergency response may be delayed or prevented	Use alternate phone numbers, cell phone, radio.
Weather warning and tornado warning sirens	The system may not activate when needed or could produce false alarms	Manually activate, if possible.
Security		
Street lights	Parking lot and street security jeopardized; increased risk of crime and driving hazards	Manually activate, if possible. Secure additional security personnel available for escort service.
Lockups	Prison escapes	Perform lockdowns manually. Disable any computerized lockdown controls.
Automated door locks	Entrance/exit from offices, etc.	Distribute keys to responsible personnel. Develop plans for manual entrance/exit.
Video surveillance	Tape dating: wrong dates may be recorded	Implement manual record maintenance by security personnel.
Alarm systems	Unnecessary false alarms	Disable all but the most critical systems. Issue memos to security personnel regarding potential problems and appropriate procedures.
Power		
Municipal and public utilities and the power grid	Loss of heating/air conditioning, lighting, communications, and other amenities of daily life	Secure standby generators.
Standby generators	Loss of power with the same results as above	Manually activate standby generator. Obtain additional generators and fuel as necessary.

Services	Areas of Concern/Impact	Backup Systems/ Contingency Plans
	Communication	
PBX	Loss of internal and external communication lines	Use radios, pagers, cell phones, or couriers.
Radio	Loss of police patrol communication	Use cell phones if possible.
Pagers	Missed and erroneous pages	Use cell phones, if possible; otherwise, use periodic call-ins or face-to-face communications.
Cell phones	Missed and erroneous calls	Use radios or face-to-face communication.
Written (copiers, fax machines)	These machines may stop working	Postpone or use carbon copies if available.
	Commerce	
EDI (electronic data interchange)	Electronic supplier payments disrupted, resulting in shortages of goods and services	Write checks manually or otherwise implement pre-electronic procedures.
Electronic payroll deposit	Employee payments made through direct deposit may be late or could fail entirely	Write checks manually or pay in cash.
Credit card purchases	Purchase approval may be denied; cards could become unusable	Use manual purchase orders. Institute blank purchase orders with local merchants

Services	Areas of Concern/Impact	Backup Systems/ Contingency Plans
Transportation		
Traffic control	Traffic lights malfunction	Use police overtime, or auxiliary police force if available, to manually direct traffic.
Freeway management systems	Highway congestion	Use police overtime, send letters to the public, or place newspaper ads stressing the need for greater safety consciousness.
Trains	Railroad crossing warnings fail (warnings are controlled by microcomputer)	Send letters to the public or place newspaper articles alerting the public to the danger.
Drawbridges	Bridge crossing warnings fail or bridges fail to open and close	Warn land and water traffic; use police who are working overtime or auxiliary police to reroute traffic.
Airports	Air traffic control systems disrupted	Increase traffic intervals; require use of visual flight rules.
Airports	Timed runway lighting systems disrupted	Disable computer controls; activate manually if possible.

Services	Areas of Concern/Impact	Backup Systems/ Contingency Plans
Basic Necessities		
Water – Pumping	Pumps stop working and soon distribution pipes are empty	Prepare water trucks for emergency distribution. Encourage citizens to have bottled water handy.
Water – Cleaning	Sanitary systems quit	Use water trucks.
Water – Well management	Not available when needed	Use alternate sources of supply.
Emergency food distribution	Supermarkets closed because of power outages, etc.	List locations for assistance. Prestock essential supplies.
Health Care		
Medical devices and equipment, operating rooms	Pacemakers, lighting, etc.	Probably the best measure is to ensure that standby generators are ready. Medical triage rules should be applied.

Source: Adapted from Keane, Inc.

SAMPLE PLAN

Contingency Plan for Wastewater Collection System

The jurisdiction's Wastewater Collection System consists of 3 lift stations, light alarm systems, and gravity sewer lines.

1. Objective of the plan

To provide normal level of service.

2. Criteria and procedures for activating the plan

To ensure that electricity flows out to one or more lift stations, the Public Works Director will assign employees to monitor the system beginning on December 31, 1999, through a night shift into January 1, 2000, on an emergency basis until it is clear that there are no problems with the operation of the system. If an employee discovers a problem, then he or she will notify the Public Works Director (or designee) via (describe primary and backup communication methods for contacting the Director) and describe the nature of the problem. If needed, the Director will notify other employees to report for duty and will assign them emergency responsibilities.

3. Roles, responsibilities, and authority

The Public Works Director will be in charge of activating and implementing this contingency plan. The Director will assign workers in the department as needed. If additional personnel are needed, the Director will have the authority to use personnel from the Parks Maintenance Dept. If the Public Works Director is unavailable, the Sewer Lead Worker will assume the responsibilities of the Director as outlined in this plan.

4. Procedures for operating during or after system failures

- Portable Generators — The jurisdiction has two portable generators that can operate the lift station, and all three lift stations have a generator receptacle so that they can be run by a portable generator. Based on the amount of storage in the lines and the wetwell in the vicinity of the lift stations, the Public Works Director will assign employees to transport and hook up the portable generators to the lift stations. If all three lift stations are not working, the Director will establish a schedule to rotate the two generators among the three lift stations. If necessary, the Public Works Director will try to obtain an additional generator through mutual aid agreement or rental.

- Vacuum Truck — If the generators are not able to handle the flow, the jurisdiction can pump sewage out of the lift stations with the vacuum truck. The Public Works Director will assign employees to use this truck to pump sewage.

- Tanker Truck — The jurisdiction also may be able to pump the sewage into its tanker truck. The Public Works Director will assign employees to pump sewage using this truck.

- Lift Station Bypass — Because of the topography in the vicinity of lift station #1, we would be able to establish a line to bypass that lift station. If needed, the Public Works Director will contact a contractor to construct this line. This is not an option for lift stations #2 and #3 because the distance to a manhole, which discharges into a gravity line, is too great.

- Temporary Overflows — To avoid sewer backups in citizens' houses if the above options do not handle overflow, the jurisdiction may have to establish temporary overflows from the lift stations. The jurisdiction will work with the State Environmental Protection Agency to try to minimize the use and impact of this option.

- Water restrictions — If a jurisdiction-wide or regional power outage lasts more than 24 hours, the jurisdiction will consider restricting community water usage to reduce flow of wastewater through the system.

5. Resources available to support emergency operations

- Personnel — 3 Public Works employees for most operations. If necessary, an additional 3 employees from the Parks Maintenance Department.

- Equipment — 2 portable generators and trucks to transport them; 1 vacuum truck; 1 tanker truck with pump; pipe or hose for lift station bypasses.

6. Criteria and procedures for returning to normal operations

- Restore electricity to all three lift stations.
- Disconnect any portable generators that have been connected to the lift stations.
- Remove bypass for lift station if that was constructed.
- Clean up any temporary overflows.

7. Estimated cost of the plan

- Personnel including regular, overtime, and holiday pay for three workers for a five-day period: $2,000–$3,000.
- Generator rental at $100/day, 5 days: $500. (Purchase of generator–$30,000)
- Construction of bypass–$500.

8. Testing the plan

Prior to December 31, 1999, the Public Works Department will provide training to its employees and the Parks Department employees on how to implement this plan.

9. Post-emergency plan

The Public Works Director will meet with the personnel who assisted in implementing the plan to determine how it worked. If necessary, changes will be made to the plan for future emergencies.

Prepared by: _____ Date: _____
PRINT

Department/Agency Head: _____ Date: _____
SIGNATURE

Resources for Helping the Public Prepare for Y2K

The general public has understandable concerns regarding Y2K. You can help them prepare for Y2K by being a credible source of information. Tell them about the potential effects of Y2K in their area, and about prudent actions they can take to be prepared.

The President's Council on Year 2000 Conversion has expanded its web site http://www.y2k.gov/, creating a separate area devoted to consumer issues and the Y2K problem. The information in this part of the site is similar to that described in the next paragraph, but users can also link directly to the agencies, companies, and industry groups that are the primary sources for much of the existing information on Y2K efforts.

Individuals can also call the number **1-888-USA-4-Y2K** to get information about power, telephones, banking, government programs, household products, and other common topics. This information comes from primary sources — government agencies, companies, or industry groups. Information specialists, supported by researchers, are available to provide additional information to callers. Pre-recorded information is available seven days a week, 24 hours a day. Information specialists staff the line from 9 AM to 8PM (EST), Monday through Friday. The service also has "FAX-back" capability.

The Federal Trade Commission (FTC) also has Y2K publications for consumers on consumer electronic products, home office equipment, and personal finances. These publications are available on-line at http://www.ftc.gov and through FTC's Consumer Response Center at 202-FTC-HELP. It also has a Business Fact Sheet urging businesses to disclose the Y2K status of their products to their consumers.

Assistance is also available for small businesses and service providers. The Small Business Administration (SBA), the National Institute for Standards and Technology's Manufacturing Extension Program, and the President's Council on Year 2000 Conversion have compiled many Y2K tools for small businesses and critical service providers. Information about these tools can be found on their web sites: http://www.sba.gov/, http://www.mep.nist.gov/, and http://www.Y2K.gov/. Small- and medium-sized businesses can also call 1-800-U-ASK-SBA for information on Y2K.

In addition, almost every State has several web pages devoted to the Y2K problem. These pages generally provide State-specific information, additional planning guidance, tools and procedures, and links to other Y2K-related web sites.

You probably will be asked how the public should prepare for the possible effects of Y2K. Advise them to prepare for limited interruptions in critical services, like those caused by winter storms. To help them prepare, you can distribute brochures with basic information. To get these camera-ready brochures free from FEMA and the American Red Cross, call 1-800-480-2520, or write to: *FEMA, PO Box 70274, Washington, D.C. 20024* for copies of the following documents:

- *Your Family Disaster Plan* —
  How to prepare for any type of disaster

- *Your Family Disaster Supplies Kit* —
  A checklist of emergency supplies

- *Emergency Preparedness Checklist* —
  An action checklist on disaster preparedness

- *Helping Children Cope with Disaster* —
  How to help children deal with the stress of disaster

All four documents are available in Spanish. You can find these helpful documents and others on-line (see *Section 5*). Also check the American Red Cross web site listed in *Section 5* for specific information about preparing for Y2K. These preparations should include:

- Checking with manufacturers of any essential computer-controlled equipment in the home
- Preparing supply kits for family disasters
- Checking home smoke alarms and buying extra batteries
- Keeping a battery-operated radio or television available to be able to receive emergency television

5. NEXT STEPS

If you follow the guidance in the preceding sections, you will make a good start on getting control of the Y2K problem. You will participate in:

- Awareness education
- Operations and consequence management planning for your agencies and communities
- Updating your emergency operations plan for Y2K actions
- Ensuring that a communications plan links local and State organizations
- Establishing operating guidance for your emergency operations centers before and after the transition date
- Coordinating between local and State public information offices on a media plan for your jurisdiction

Developing an Incident Management Plan

The preceding sections will help you to:

- Assess the risk of Y2K problems in your agencies and communities
- Plan for continuity of operations if Y2K problems occur
- Plan to manage the safety and health consequences of Y2K problems

One more planning step is left — developing an Incident Management Plan. This plan will help you respond effectively at the time of a Y2K disruption. Such planning is beyond the scope of this Guide, though portions of your Consequence Management Plan will carry over to an Incident Management Plan. If a system fails, you may be unable to determine immediately whether it is due to Y2K or another cause. You will need an IT professional either way, but should try to determine the cause as part of your Incident Management Plan.

The National Emergency Management Association (NEMA) is preparing more detailed guidance on incident management planning. Check the NEMA web site, listed later in this section, for more information.

Obtaining Additional Information

As discussed earlier, the first, best place to look is on your own State's web site. Virtually every State has several web pages devoted to the Y2K problem. They generally provide State-specific information, additional planning guidance, tools and procedures, and links to other Y2K-related web sites.

In addition, many of the FEMA documents cited in this guide are available in its on-line library. Go to http://www.fema.gov, follow the link to the Library, and then go to the Preparedness, Training, and Exercises Room. You can also order documents from FEMA's Printing and Publication Branch, PO Box 2012, Jessup, MD 20794-2012. Phone: 1-800-480-2520. Fax: 301-362-5335.

Types of Resources Available

A wealth of information is available from a variety of sources on the Y2K problem. These sources include:

- Newspaper articles
- Magazine articles
- Technical publications
- Computer manufacturers
- Software manufacturers
- Vendors
- Libraries
- Bookstores
- Consultants
- Private industry and businesses
- Television and radio features
- Federal, State, and local government agencies and departments

The easiest and quickest way to obtain a wide range of current Y2K information is by examining the many Internet web sites dedicated to this issue. By looking at the World Wide Web, you can discover the nature and magnitude of Y2K problems, see what others are doing to solve these problems, obtain contingency planning information from organizations and governments, and get examples of approaches you may wish to consider adopting.

The following list of representative web sites can help you get started. This list is a pathway to web sites that contain specific information and can lead you to other sources of useful information. The addresses of these sites have been reduced to the minimum number of characters needed to get you to the site. Once there, you can follow links to obtain more detailed information within and outside of the site.

Selected Web Site Listings

http://www.y2k.gov/
The President's Council on Year 2000 Conversion — provides status reports and information for consumers on how the Y2K problem may, or may not, affect their daily lives. For links to many sites dedicated to fixing systems, select "Text" or "Graphics," select "Becoming Y2K Compliant," then select "Tool Kit: Understanding Your Organization's Y2K Challenge."

http://www.fema.gov/
FEMA Year 2000 Issues — FEMA provides information and web links to additional information on emergency service, and emergency response, preparedness and contingency planning.

http://www.itpolicy.gsa.gov/
U.S. Government's Office of Information Technology — provides links to Y2K directories and is especially useful to municipalities that want to access a variety of State and local Y2K information sites.

http://www.usfa.fema.gov/
The National Fire Data Center — answers some frequently asked questions (FAQs) and lists Y2K web sites of importance to emergency managers.

http://www.nstl.com/
The National Software Testing Lab — provides shareware to test computers for Y2K compliance.

http://www.redcross.org/
The American Red Cross — answers some FAQs and provides individuals with a checklist of actions to follow for preparedness.

http://www.senate.gov/~y2k/
The U.S. Senate Special Committee on the Year 2000 Technology Problem — provides links to governmental agencies.

http://www.gao.gov/
The General Accounting Office's *Year 2000 Computing Crisis: An Assessment Guide* — provides help in developing a Y2K compliance project checklist. Check under "Special Publications."

http://www.year2000.com/
Year 2000 Information Center — provides a forum for exchanging information and possible solutions to Y2K problems.

http://www.dps.state.mn.us/
Minnesota's *Y2K and Emergency Management Information for Community Preparedness* — a guidebook that deals with the technical mitigation and consequence management aspects of the Y2K problem.

http://www.dir.state.tx.us/y2k/
Texas's *Guidebook 2000, About Time: Managing the Y2K Problem in Local Government* — a reference point for cities, counties, and other subdivisions to address Y2K problems.

http://www.irm.state.ny.us/
New York State's *Guide to Solving Year 2000 Problems in NYS Local Government* — helps local communities identify and develop plans to address the Y2K problem; can be downloaded.

http://www.co.mo.md.us/year2000/
Montgomery County, Maryland's *Contingency Plan Guidelines* — deals with continuing mission-critical government and business services that could be affected by the Y2K problem.

http://www.mspemd.org/
Michigan's *Maintaining Essential Services in the New Millennium* — an assessment tool with an extensive list of systems that could contain embedded chips.

http://nemaweb.media3.net/
National Emergency Management Association — contains position papers on Y2K for State and local emergency managers.

http://www.iaem.com/
International Association of Emergency Managers (IAEM) — January 1999 issue of *IAEM Bulletin* focusing on Y2K.

http://www.mitre.org/
Mitre Corporation — an extensive list of critical dates and information for Y2K testing.

http://www.pa2k.org/
The Commonwealth of Pennsylvania and Government of Canada — *Guidebook for Local Governments*.

http://www.lmnc.org/
League of Minnesota Cities — *A Year 2000 Action Guide*.

http://www.mwcog.org/
Metropolitan Washington Council of Governments — *Year 2000 Best Practices Manual*. Look under "Year 2000 Initiative."

http://y2k.state.fl.us/
State of Florida Year 2000 Task Force — *Year 2000 Remediation Checklist*. Look under "Tools & Training."

http://y2k.state.ks.us/
State of Kansas, Department of Administration, Division of Information Systems and Communications — *Outreach to the New Millennium*.

Additional Contacts

The following names and phone numbers are FEMA Regional Y2K points of contact for emergency managers.

Region I	Dan McElhinney	(617) 223-9567
Region II	Robert F. Jones	(212) 225-7018
Region III	Lora Werner	(215) 931-5724
Region IV	Shelley Boone	(912) 225-4572
Region V	Alyce O. Williams	(312) 408-5522
	Lawrence L. Bailey	(312) 408-5582
Region VI	Sherry Wainwright	(817) 898-5152
Region VII	Jim Donley	(816) 283-7010
Region VIII	J. Scott Logan	(303) 235-4864
Region IX	PT&E Division	(415) 923-7220
Region X	Kathy J. Burke	(425) 487-4603