IACP Project Response: Preparing Law Enforcement for Y2K

Introduction and Background

Much has been said, written and reported on the catastrophic impact that Y2K will have on the American public. Little has been reported on where we really stand with respect to Y2K and what steps law enforcement executives should be taking to prepare for this heavily publicized event.

The purpose of this report is to provide law enforcement executives with an objective orientation to the Y2K issue. This non-technical primer will provide police chiefs with the following:

• an orientation to the Y2K problem
• a global status report on critical systems
• an assessment of risks, including checklists
• contingency planning guidelines, including checklists
• a resource directory
• a layman’s Y2K glossary

It is important to note that at this late date, work on critical Y2K/date-sensitive components of national, state and local infrastructure should be in the final stages of completion and testing. At this point, agencies must focus on the emergency and critical incident management aspects of Y2K. Effective emergency management planning and training will provide a strong foundation from which to address the range of incidents the new millennium will present. This report contains such guidance, focusing on review and organization of emergency management resources on the local level to mitigate the impact of Y2K on organizations and communities.

In any problem-solving exercise, panic and pandemonium are detrimental, while leadership, planning and training are supportive. Fortunately, police departments and their chiefs have had plenty of practice in solving both major and minor problems in their communities. This report will help them serve their communities through this eventful—or perhaps “event-less”—period, providing the tools necessary to avoid the panic this topic can engender, and access the attention, experience and resources the issue demands.

Orientation to the Y2K Problem

The Year 2000 problem, also known as the millennium bug, is the result of computer programming decisions made as far back as 40 years ago. Early system programmers typically used two digits to represent the year in order to conserve scarce computer memory. As a result, when the year 2000 rolls around, many date-sensitive information technology systems will read it as 00 or 1900—or even 1980. This glitch could cause systems to malfunction or even shut down—a significant problem in our electronic information-dependent society. Other projected effects of the Y2K bug are discussed later.
This problem is not confined to computer programs, but includes embedded computer chips as well. Embedded chips figure prominently in our daily activities, operating everything from microwave ovens and coffeemakers to telephones and automobiles. Indeed, it’s difficult to list all the processes involving these chips, as their number has been estimated at 25 billion—and growing.

With such heavy reliance on computer chips, many early prognoses for Y2K included a loss of electrical and telecommunications capabilities, among other important functions. These concerns deserve serious attention in their own right, of course; even more importantly, however, they serve to illuminate the possible repercussions of not fully addressing the Y2K problem.

Nearly all governments and organizations, including private entities, have addressed this issue on some level. However, the Y2K problem is far from solved; indeed, even after the new century arrives, a number of problems will likely require attention. In the pages that follow, we will attempt to address the omnipresent problems, promote contingency plans and provide credible information sources your agency can use.

**Current Progress**

Although much of this report is directed to agencies in the United States, we want to emphasize that this is a global problem that requires immediate attention. System failures in the Far East, Europe and Africa could have an impact upon operations in the United States and vice versa.

According to the Senior Advisors Group to the President’s Council on Year 2000 Conversion, several priority issues remain. These include communications, information sharing, contingency planning/emergency response and assessing international readiness. (Memorandum to Members of the Senior Advisors Group, January 12, 1999.)

With respect to communications, one of the more serious domestic threats we face is the public’s overreaction to problems they anticipate. The President’s Council has been proactive in this area, issuing a quarterly summary of sector assessments conducted by national associations (addressed later in this report), and launching a toll-free consumer hotline.

While there is confidence that critical national infrastructures in the United States will operate without major disruptions, some areas may experience localized failures. Most organizations (including government and private entities) will use skilled teams during the New Year weekend to ensure that their systems have made the transition smoothly and to handle any problems that arise. These workers—a critical source of expertise—could assist others in similar organizations with difficulties that exceed their abilities. The challenge for government and industry will be how best to coordinate these resources.
For a smooth transition, we must do a better job of sharing the Y2K technical information that is so critical to organizations lagging behind in their preparations, both domestically and abroad. Toward this end, the “Year 2000 Information and Readiness Disclosure Act” was passed into law to promote the good-faith exchange of such data. Many states are also considering legislation that will reduce or provide caps on liability with Y2K issues.

The good news is that virtually all areas of industry reported a high awareness of the problem and its potential consequences. Several segments are mounting aggressive efforts to combat the problem and ensure that critical systems will be able to process the date change. Among the most notable in these efforts are financial organizations, including banks and security firms. Major disruptions in banking, power and telecommunications industries are increasingly seen as less likely.

Most large organizations have made significant progress, as compared to their smaller counterparts. Some of these smaller organizations, including smaller businesses, believe they will be unaffected or are delaying action until failures occur. This lack of preparedness increases the risk for localized Y2K disruptions.

Around the globe, levels of Y2K preparedness vary dramatically. The President’s Council has accessed many international associations to raise awareness and motivate action. Despite these increased efforts, international failures are likely, as a number of countries have done little to reprogram critical systems.

One aspect of the Y2K issue is actually helpful. The first day of 2000 begins at a spot in the middle of the Pacific Ocean 17 time zones earlier than Eastern Standard Time in the United States. Therefore, if the Y2K bug does cause immediate problems in information systems and embedded chips, the effect will ripple from time zone to time zone. For example, Y2K problems that occur at the stroke of midnight in Wellington, New Zealand, won’t hit the United States until 17 hours later, when clocks on the East Coast strike 12. We will thus have advance notice of potential problems-crucial information that the Federal Emergency Management Agency (FEMA) will disseminate through a “Y2K First Alert System.” This system is intended to provide information through normal emergency response channels, although other communication sources are being reviewed. (U.S. Senate, Special Committee on the Year 2000 Technology Problem, October 2, 1998.)

Risk Assessment

This document includes a checklist and glossary of common applications and concerns specific to law enforcement agencies. Though not all-encompassing, it is a starting point for agencies that have not yet adequately addressed the problem and its impact. For those that have, it may provide insights into areas that they may have overlooked.

Many entities have developed a rating system and sorted their Y2K problems into different priority levels. A typical system has four levels: Fatal, Critical, Important and Routine.
First Priority Level—Fatal: defined as a failure that could result in death, severe financial loss or legal liability to the department. It includes all essential (mission-critical) functions in the operation of information systems and delivery of services to community and department staff. Examples include E911 systems, telecommunications equipment, two-way radios, etc.

Second Priority Level—Critical: defined as a business function that is critical to departmental operations—difficult to do without for any length of time. Examples include PCs for data entry, security systems (badge readers), elevators, programmable thermostats, etc.

Third Priority Level—Important: defined as a business function that is important but not critical to the agency. Examples include copiers, fax machines, still and video cameras, pagers, etc.

Fourth Priority Level—Routine: defined as devices that are not strategically important to the department, whose failure would inconvenience individuals but not disrupt projects. Examples include automatic coffeepots, VCRs, microwaves, etc.

Once priorities have been established, it’s time to review the following risk factors:

• What police department functions would be affected if the system failed?
• What would be the consequences of the failure?
• Would system failure create legal liability?

This evaluation process may appear overwhelming, but smaller agencies can begin by doing a walk-through of their agency. Larger agencies can designate the evaluations to their subordinates and subordinate commands. The important thing to remember is that no one is in it alone: businesses, governments and even residences will be similarly affected. Billions of dollars spent on this problem have produced answers and resources, many of which are available on the Internet, and have been included in this report. If your agency doesn’t have Internet access, contact a local library, school or other resource that does.

Part of the reason the Y2K problem is so complex is that so many disciplines are intertwined. An agency review may provide insights into communications, utilities, etc., but does not typically address the public works department. This can have far-reaching implications. For example, localized power outages call for manual traffic direction in intersections controlled by electrical devices (or devices with embedded chips). If such events require increased staffing, there will be a corresponding increase in the need for food and fuel. Local food or gas suppliers could run short by the end of December, requiring alternative sources. And if problems begin before year’s end, will you have sufficient personnel and resources to ensure continuity of your operations? All these external considerations should be factored into your contingency planning.
Assessment/Planning Checklist

The following questions are designed to assist you in assessing and planning for any Y2K corrections:

- Has an individual been designated to assess Y2K problems?
- Have all business processes been examined to identify dependencies on systems that are vulnerable to Y2K problems?
- Has a Year 2000 data standard been defined, i.e., have you decided how you will record the date in numeric form on forms, in computer systems, etc.?
- Have budget estimates for testing, fixing and/or replacing systems been prepared and authorized?
- Has a plan identifying milestone dates been prepared?
- Is progress being monitored?

Obviously, law enforcement agencies cannot provide answers to all Y2K problems, but they will be a primary point of contact for many people. To meet the additional workload, the Royal Canadian Mounted Police (RCMP) has taken a prudent approach to staffing, ensuring that 100 percent of its workforce is available during the critical transition period of December 27, 1999, to March 15, 2000, by canceling annual leave for all RCMP members and all public servants who perform “essential service” duties.

Computer Systems and Embedded Chips

The degree to which law enforcement agencies have addressed internal Y2K problems associated with computer systems and embedded chips varies widely. Some larger departments have worked on the problem for years, while many smaller agencies—which often rely on relatively few electronic devices—may have only a few systems or devices that may or may not be vulnerable to problems.

The following information will help determine if your computer is Y2K compliant.

The date on a computer results from the interaction of the real-time clock (RTC) and the Basic Input/Output System (BIOS). The RTC is an incremental counter, battery-powered to continue functioning after the power is turned off, that counts in increments of 1 from 00 to 99. The century indicator is hard-coded in read-only memory (ROM) to indicate 19. As the RTC counter goes from 99 to 00, it will pair up with the century indicator and display the year 1900 unless the computer has a Y2K-compliant BIOS. (The Resource Directory includes additional information on BIOS.)
The BIOS, which is stored in ROM (or flash ROM on newer systems), is the application that allows the operating system to communicate with the computer’s hardware, recognizing and controlling the hard drive and disk drives, and interfacing with the CPU and other motherboard components. The BIOS takes the date and time from the RTC, and delivers it and other information about the computer to the operating system during the boot process. The BIOS is responsible for changing the “century byte” of the RTC from 19 to 20. A Y2K-compliant BIOS will read the 00 value and the 19 value on the century counter and reinterpret it as the year 2000. If the BIOS doesn’t make this change when the year rolls over from 1999 to 2000, the RTC will read 1900, rather than 2000.

The best way to ensure that the BIOS is compliant is to physically replace it or flash upgrade it. Once, upgrading the BIOS meant prying off the old chip and replacing it with a new chip. Newer computers store the BIOS in flash memory, meaning it is not hard-coded and can be easily updated by downloading the utility via the Internet. Several software products are available to check BIOS compliance and provide third-party fixes for the hardware problem. If you are unable to physically replace or upgrade the BIOS, and no software patch is available, the computer is probably too old and should be replaced.

Community Risk Assessment

The following list is designed to help your department assess risks in your community and anticipate possible scenarios:

- Public utilities (electric, water, natural gas, waste treatment): Have systems been tested? Are they ready? Is there a contingency plan?

- Fire departments: Do they have contingency plans? Have they considered the possibility of more fires if citizens use alternative sources of heat? Are alternative sources of water available?

- Vehicle fuel: Will sufficient fuel be available? Are gas pumps compliant? Are generators available?

- Grocery stores: Are cash registers and inventory control systems ready? If not, will stores be open? How will they operate?

- Banks: Have all PCs and security systems within the bank been tested? Are banks ready with extra cash?

- Health services (hospitals and ambulance services): Have all systems and devices been checked? Are contingency plans in place?

- Legal issues: Is your department obligated to provide any services that may be impossible to provide during major disruptions? Do you have assurance letters from major suppliers and vendors guaranteeing the flow of supplies and operation of all
systems?

- Jails and prisons: Have jails and prisons at the local, state and federal levels developed and implemented contingency plans?

- Civil unrest: Do you have good intelligence to determine if any groups may attempt to incite panic in the community?

**Contingency Planning Guidelines and Plan**

The President’s Council has emphasized that all organizations should develop contingency plans to address internal and external Y2K-related failures and thus minimize Year 2000 disruptions. Indeed, contingency planning is probably the most critical issue law enforcement executives should consider when preparing their agencies’ Y2K response. A strong contingency plan, clearly understood by internal and external emergency management personnel, will serve as a map to follow through the critical incident maze that Y2K may present.

If your agency has not yet developed a Y2K contingency plan, take heart. Remember that police agencies, by their very nature, rely on contingency plans to help them navigate natural disasters. Many of these plans are Emergency Operations Plans (EOPs) that have been in place for many years. Your agency may not have its own EOP, but your city, county or state probably does, and it is a good beginning. By building on existing plans, you can avoid reinventing the wheel and save valuable time.

These plans anticipate the loss of electricity, telecommunications, utilities, etc., and provide guidelines for coordinating multi-jurisdictional responses to these and other emergencies. It is crucial that you review and update your contingency plans now to minimize time lost due to confusion and disorientation. To the extent possible, try to coordinate with other agencies and train on these plans.

Following are outlines for contingency planning and an Incident Command System (ICS). The contingency plan (which may be adapted to suit a particular situation) is generally agency-specific, while the ICS module is geared toward a multi-agency, multi-jurisdictional response. A checklist is included to facilitate this process.

**Contingency Plan**

1. **Definition**

A contingency plan is a complete, consistent statement of all actions to be taken before, during and after a disaster. The plan must include documented test procedures that, if followed, will ensure the availability of critical resources and facilitate the continuity of operations.
A. Facts

• There is no standard contingency plan; each must be developed to meet individual needs or requirements.

• Although a contingency plan can be quite simple, it may be more complex if you rely heavily on technology.

• The main objective of a contingency plan is to promote a continuity of operation—even at a degraded level.

• The main benefit of a contingency plan is the reduction of future losses in the performance of essential services.

• The cost of the plan should not be more than the savings the plan is expected to yield.

B. Elements

A good contingency plan consists of well-defined requirements, definitions of responsibility, statements of critical resources needed to implement the plan, definitive plans to ensure critical resource availability, and detailed procedures to accomplish necessary functions/activities.

The following elements should be considered in developing a contingency plan:

• Trained personnel to carry out the functions
• Hardware and office equipment
• Software and data files
• Preprinted forms and other supplies
• Communication facilities
• Detailed operating instructions

II. Criteria for Critical Applications

Usually, less than 20 percent of all applications are critical. However, this small percentage cannot be neglected if disruption is to be avoided. The following guidelines can help you decide which of your applications are critical.

• The law or a contractual agreement period requires performance within a given time.
• Performance is required to maintain either cash flow or operations.
• Performance is required to maintain records for legal, accounting or tax purposes.
• Performance is desired to support long-range planning or development.
III. Phases

A good plan has three phases:

- Emergency response—actions that must be taken during an emergency to lessen its impact
- Back-up operations—alternative processing until normal service is restored
- Recovery actions—actions to be taken to restore normal service

**Contingency Planning Checklist**

Have the lines of communication been established with:

- FEMA?
- the state emergency coordinator?
- the city/county emergency coordinator?
- emergency coordinators in neighboring jurisdictions?
- the Red Cross?
- Have Memoranda of Understanding (MOUs) been established with neighboring jurisdictions for the purpose of sharing information and resources?
- In the event of power outages and/or loss of heat, have shelters been designated?
- Is there a plan for heating the shelters?
- Is there a plan for directing traffic?
- Is there a plan for food and water distribution?
- Is there a plan for crowd control and/or civil unrest?
- Is there a contingency plan for problems affecting transit?
- Does the public know and understand what to do in cases of emergencies?
- Has your department prepared a consistent message to be delivered to the community?
• Will there be enough dispatchers and police personnel to meet additional needs?

**Incident Command System**

Once contingency plans are completed, agencies should turn their attention to the Incident Command System (ICS), which has proven effective in numerous emergency situations and is applicable for long periods of time. The ICS, which is taught by the IACP, is used by many jurisdictions—as well as such organizations as FEMA and the National Fire Academy—to manage emergency management resources during critical incidents. The ICS organizational structure develops in a modular fashion based upon the type and magnitude of an incident.2

**Six-Step Incident Response Process**

Step 1: Size up the Situation.

Begin by answering the following questions:

- What is the nature of the incident?
- What hazards are present?
- How large an area is affected?
- How can the area be isolated?
- What location would make for a good staging area?
- What entrance/exit /safe routes would be good for the flow of response personnel and equipment?

Include the following information in size-up reports:

- The unit designation
- A description of the situation
- Obvious conditions (e.g. hazards)
- Initial actions taken
- Obvious safety concerns
- Assumption, identification and location of command post
- Request or release of resources

Step 2: Identify Contingencies.

Remember that Murphy’s law—and its corollaries—apply to incident management:

- If anything can go wrong, it will.
- Nothing is as easy as it looks.
- Everything takes longer than you think it will.

Step 3: Determine Objectives.

Meaningful objectives are:

- measurable
• used to monitor incident progress and establish priorities
• based on size-up reports and identified contingencies

Step 4: Identify Needed Resources.

Start by determining:
• what resources are necessary
• whether they are on hand
• where you might get them
• how long it will take
• what is available from other agencies
• whether there are any special requirements

Step 5: Build an Incident Action Plan and Management Structure.

Identify:
• responsibilities
• chain of command
• coordination

Step 6: Take Action.

Incident stabilization involves the following steps:
• Establishing command
• Mobilizing resources
• Setting up a staging area
• Isolating the area
• Treating/assisting the injured
• Setting up entrance/exit/safe routes
• Issuing warnings
• Initiating evacuation
• Establishing liaison

Conclusion

January 1, 2000, is an immovable deadline; there will be no second chances to complete preparedness measures. You can, however, mitigate the impact Y2K may have upon your department and your jurisdiction. Go over the checklists in this booklet carefully and see whether you have missed any details while you still have time to make necessary preparations.

If you feel well prepared, reach out to agencies in your area that need assistance and share the lessons your agency has learned. Finally, don’t forget to communicate with your community. Provide your constituents with an educated and objective voice of reason. Your citizens need to know what to do and where to go in an emergency. Your leadership and that of your agency can have a tremendous impact on your communities’
Critical Services Progress Overview

The following is a brief overview of the progress of critical services as reported on January 7, 1999, to the President’s Council on Year 2000. The information was compiled by federal agencies, government organizations, trade associations and other groups in cooperation with the Year 2000 effort. (Memorandum to Members of the Senior Advisors Group, January 12, 1999; noted in their Web site—www.y2k.gov.)

Here, by category, are some possible contacts for more information on specific Y2K problems. This list is not exhaustive, so we recommend that you contact your local and state governments for more extensive Y2K program objectives.

Communications/Power

Wireline (e.g. conventional telephones, etc.). Based upon information to date, the most likely Y2K difficulties would be small, localized problems in the network. Estimates vary, but the average target date for complete implementation is June 30, 1999.

Cable. Current data is unavailable; however, the set-top boxes found in the common household will not be affected. Other services report that compliance will be achieved before the end of the century.

Wireless (e.g. cellular, PCS, CDPD, and land mobile radio, etc.). The majority of cellular and PCS phones are not date-sensitive. However, there could be problems in trunked systems or in other systems that integrate the cellular system into a larger network, such as public service answering points operated by local emergency response providers. More information will be available in the first quarter of 1999 through www.fcc.gov/year2000.

Mass media. According to the industry, Y2K problems should not cause a loss of essential services due to multiple broadcast systems; further most susceptible equipment can be manually overridden.

International. Telecommunications companies engaged in trans-border services indicate that neither dial tone nor data transmission are likely to experience significant difficulties, though billing and maintenance systems are cause for concern.

Electric power. The remediation/testing phase of Y2K preparations is expected to be completed in May 1999. Mission-critical systems and components (e.g. power production, energy management systems, telecommunications, substation controls and system protection, and distribution systems) are to be Y2K-ready by June 30. This industry is strongly emphasizing contingency planning for the transition.
Emergency Services

Emergency management directors. Early responses indicate that all state level agencies have resolved, or plan to resolve, the vast number of Y2K-related issues involving critical emergency preparedness facilities, systems, and services. Limited contingency planning is complete at state and local levels.

Fire service. Working with several associations to assess the problem.

“911” centers. The FCC is working with the National Emergency Number Association to assess Y2K readiness; an initial report is expected in early 1999.

Emergency medical services. An assessment is ongoing; however, 75 percent of state EMS directors report that their systems will be 100 percent compliant by January 1.

Federal response planning. Virtually all Federal Response Plan primary agencies—the departments of Transportation, Defense, Agriculture, Energy, and Health and Human Services, as well as FEMA, NCS, GSA and the EPA-state that they expect their mission-critical systems used for emergency response under the FRP to meet the March 31 government-wide goal for Y2K compliance. See www.fema.gov/y2k/ for current updates.

Immediate Concerns

Financial services. According to the latest data from federal supervisory agencies, financial institutions are well ahead of most organizations in preparing systems. Banks, credit unions, and the futures and securities industries are far into the Y2K remediation process and expect system-readiness before the new millennium.

Oil and gas. Industry officials are cautiously optimistic that the U.S. oil and gas sector will be ready for the transition. Survey results indicate that progress is good but not fast enough.

Solid waste. Waste industry organizations—waste haulers, handlers and disposers—use a relatively low level of automation in their operations; consequently, the industry reports its exposure to Y2K-related difficulties will be minimal. See www.epa.gov/year2000 for current updates.

Transportation. Air carriers and large airports and transit providers are making significant progress. Concern focuses on the potential readiness of airports and transit services in small communities and rural areas. More data are needed for fuller understanding of the readiness level throughout this industry. Information on other industry components is expected. For more information, consult www.y2ktransport.dot.gov or www.dot.gov

Water supply. The most recent survey data indicate a majority of public water system representatives do not expect Y2K interruption of services. Most public water systems
can be manually operated, maintaining sufficient environmental protections.

**Benefits payments** (e.g. SSA, SSI, VA benefits, etc.). Work remains to ensure complete readiness of all systems responsible for making federal benefit payments, but agencies expect to perform that duty without disruption in January 2000.

**Postal Service.** The USPS has renovated 78 percent of its mission-critical systems; the remaining renovation and implementation will be completed in the first half of 1999.

**Devices That May Contain Embedded Systems**

The following list of computer systems and devices is provided to assist agencies in their assessments. While it may seem overwhelming at first, bear in mind that not all items pertain to every department and that, in most cases, these devices will not be affected. Unfortunately, no comprehensive database shows which years, makes and models will be vulnerable to problems. Check with suppliers and sales representatives regarding vulnerability of their devices.

**Arrest and Property Processing Equipment**

- Evidence processing equipment—labeling, bar coding, stamping equipment
- Fingerprint processing equipment—photographic lasers, special lighting or digitizing equipment, data transfer equipment
- Audio/Video Equipment
- CCTV cameras/monitors
- Digital cameras
- Listening devices
- Photo/surveillance equipment
- Recording devices, both video and audio
- Remote control devices for security cameras or projectors
- Security cameras

**Aviation**

- Aircraft systems (Avionics)
- Helicopter systems, including infrared sensors, night vision, sirens, public address systems, television networks or cameras

**Communications**

- Intercom systems
- Mobile phones
- Pagers and alerting devices, systems or networks
- Radios
- Radio systems
• Software programs that schedule training or certification
• Telephones and switches
• Telephone recording systems or devices
• Voicemail/message systems
• Computer and Information Systems
• Computer-aided dispatch (CAD)
• Connections to city, county, state and federal online databases
• Electronic pens; laptop and palm-top computers
• Global positioning systems (GPS)
• Geographic information systems (GIS)
• Mobile data terminals and computers
• Records management systems (RMS)

General Building and Office-Related Systems

• Building maintenance systems, especially those that control access, lighting or power
• Burglar and fire alarms (public/private; business/residential)
• Electronic locks
• Elevators
• Heating and ventilation systems
• Remotely operated doors
• Security systems
• Sprinkler systems
• Office Equipment
• Faxes
• Photocopiers
• Postal meters
• Telex machines
• Time-stamping devices for legal documents or time cards

Other Equipment

• Breathalyzer instruments
• Car park barriers
• Crime lab equipment that may be date-dependent
• Electronic equipment for crime scene investigation
• Electronic firearms trigger guards or safety locks
• Electronic laser sighting devices
• Electronic prisoner tracking devices; ankle-mounted electronic devices
• Equipment that may alert the operator to battery service
• Equipment that may do its own maintenance scheduling
• Explosive and drug detectors
• Hazardous materials detection equipment
• Laboratory instruments
• Metal detectors
• Night vision devices
• SCUBA equipment
• Traffic lights

**Vehicle-Related Systems**

• Automatic vehicle locating systems
• Breath-analysis instruments
• In-car cameras
• Speed-measuring devices (Radar/LIDAR)
• Vehicle management systems
• Vehicle systems, including infrared or night vision, sirens, public address systems, audio and video recording devices
Resource Directory

Law Enforcement-Specific

This section, which lists police departments that have been successful in assessing and correcting their Y2K problems, includes both internal and external problem areas and the processes involved in their resolution.

Colorado Springs Police Department
Colorado Springs, CO
*Includes a PowerPoint presentation on strategy planning for Y2K from assessment to reparations of problems with computers.

Denton Police Department
Denton, TX
www.ci.denton.tx.us/y2k/index.html
*Includes meeting notes from Y2K Challenge committee with a breakdown of possible problem areas and specific agency affected.

Royal Canadian Mounted Police
www.rcmp-grc.gc.ca/html.rcmp2.htm
*Includes status of systems and general Y2K information.

City and State Governments
This section includes general resources and plans for addressing Y2K problems and emergency management. Most have links to their state and local law enforcement agencies.

City of Albuquerque
Information Systems Officer, Y2K Program
www.cabq.gov/y2k
*Provides templates for Y2K project management, including an in-depth review of how to develop Y2K-specific contingency plans.

City of Austin, TX
Austin 2000 Project
www.ci.austin.tx.us/y2k
*Explains the coordination of city government departments and services to create an emergency preparedness plan and to educate the community about Y2K effects.

Montgomery County, Maryland
Year 2000 Project Office
www.co.mo.md.us/Year2000/index.html
*Provides a section on lessons learned while testing systems, complete with successes and failures of components.
State of Alaska
Y2K Project Office
www.ak-prepared.com/y2k.htm
*Provides efforts by the government, community and law enforcement on Y2K issues and emergency preparedness. Includes a PowerPoint presentation.

State of California
Department of Information Technology
916-445-4900
*Gives compliance assessments for systems, identifies special issues and provides contingency plans for them.

State of Connecticut, DOIT
Year 2000 Program Office
www.doit.state.ct.us/y2k
*Provides information about the state’s completed and continuing efforts to become Y2K-compliant. Includes a list of certified Y2K vendors and their links.

State of Ohio
Y2K Administrator
Ohio Data Network
www.oy2k.state.oh.us/
*Provides guidelines and information about Y2K compliance and its impact public agencies and their abilities to perform their duties properly.

State of Maryland
Y2K Program Management Office
www.mec.state.md.us/
*Great source of information technology and century compliance efforts. Provides examples of letters to vendors and warranties to estimate systems’ needs.

State of Michigan
Emergency Management Division
Michigan Department of State Police
www.mspemd.org/y2klinks.htm
*Provides general information about contingency planning and emergency preparedness. Gives links to other general Y2K sites.

State of Minnesota
Minnesota Department of Public Safety
www.dps.state.mn.us/emermgt/index/html
*Provides an information packet for local emergency managers to assist in Y2K contingency planning. Also includes information for family preparedness.
State of Texas
Year 2000 Project Office
Texas Department of Information Resources
www.yeeha.net/y2k/
*Gives links to Texas Y2K project office, FEMA and information on embedded chips and other technology.

Commonwealth of Virginia
Century Date Change Initiative Project Office
www.cdci.state.va.us/
*Provides a Y2K checklist used by the Virginia State Government to review the completion of Y2K efforts in phases.

**Community-Based Programs**
This section contains information for individuals to prepare themselves and their communities for possible Y2K problems.

Napa Valley Citizens for Year 2000 Preparedness
PO Box 2254
Napa Valley, CA 94558
707-226-6221
www.y2knapa.com
*Gives a detailed list of how to prepare your family and community for any possible Y2K problems. Includes information on contingency planning.

**Computer and Information Systems**
This section contains relevant general and technological information related to Y2K issues and steps to becoming compliant.

The Correction Connection Network
159 Burgin Parkway
Quincy, MA 02169
617-471-4445
*Has a Y2K help center and lists government articles addressing Y2K and related vendors.

Department of the Interior
Office of Managing Risk and Public Safety
Mailstop 7356
1849 C Street, NW
Washington, DC 20240
202-208-7702
www.mrps.doi.gov/le1.htm
*Gives links to other sites dealing with Y2K and embedded-chip problems, along with
contacts.

FCW Government Technology Group
3141 Fairview Park Drive
Suite 777
Falls Church, VA 22042
703-876-5100
www.fcw.com
*Includes articles from the federal government on Y2K correction operations from the military to general technology information.

IACP Technology Clearinghouse
515 N. Washington Street
Alexandria, VA 22314-2357
703-836-6767; 1-800-THE IACP
fax: 703-836-4543
www.IACPtechnology.org
*Established to collect and disseminate information on promising law enforcement information management technologies; provides agencies with constant and impartial information through a peer-to-peer exchange.

National Law Enforcement and Corrections Technology Center
PO Box 1160
Rockville, MD 20849
1-800-248-2742
www.nclectc.org
*Includes the Justice Technology Information Network.

9-1-1 Magazine
PO Box 11788
Santa Ana, CA 92711
800-231-8911
www.9-1-1magazine.com
*Serves the public safety communications and response industry and provides good emergency preparedness information.

President’s Council on Year 2000 Conversion
1-888-USA-4-Y2K
www.y2k.gov
*Provides information on becoming Y2K compliant, as well as contingency planning and tips for computer consumers.

Y2K States List
www.y2k.com/non-us-fedgov.htm
*Provides links to other state Y2K sites, NASIRE state search and Information
Technology Association of America (ITAA).

Y2K and You
http://pti.nw.dc.us/y2k/index.html
*Includes information to help local governments with Y2K problems, contingency planning and emergency preparedness.

Emergency Planning and Management
This section contains resources for emergency preparedness and management.

American Red Cross
2025 E Street, NW
Washington, DC 20006-5009
202-728-640
www.redcross.org
*Includes a checklist for individual emergency preparedness and other general information on the subject.

Federal Emergency Management Agency
500 C Street, SW
Washington, DC 20472
1-888-USA-4-Y2K
www.fema.gov
*Includes Y2K Initiative and compliance update of FEMA’s systems. Also gives basic emergency management information such as preparedness and consequences.

International Association of Emergency Managers
111 Park Place
Falls Church, VA 22046-4513
703-538-1795
www.emassociation.org
*Includes an on-line Y2K discussion group for emergency managers and other basic emergency management information.

International
This section contains sites with general information on Y2K and each countries’ operations to correct systems and prepare for the millennium.

www.itaa.org/intlink.htm
www.ccep.ca/tool_kit.html

Canada

Canada
www.ispo.cec.be/y2keuro/year2000.htm
Europe

Hong Kong (in Chinese)
www.y2k.gov.in/

India
www.y2k.gov.my/

Malaysia
www.y2k.gov.au/

New South Wales, Australia
www.y2k.govt.nz/

New Zealand
www.ncb.gov.sg/ncb/yr2000/

Singapore
www.y2k.org.za/

South Africa
www.bug2000.co.uk/

United Kingdom
www.unorg/members/yr2000/

United Nations

**BIOS Resources**
The BIOS Survival Guide Co-edited by Jean-Paul Rodrigue and Phil Croucher
http://www.lemig.umontreal.ca/bios/bios_sg.htm

BIOS Setup Information Guide
http://www.sysopt.com/bios.html

Basic Input/Output System—Surviving The BIOS Nightmare
http://www.smartcomputing.com/articles/archive/r0202/26t2/26t2.asp?guid=i2fsf8mk
A Layman's Y2K Glossary

The following information has been obtained from various sources to give the reader a better understanding of Y2K.

BIOS (Basic Input/Output System)—controls the startup of the machines or computers and other functions such as the keyboard, display, and disk drive. The BIOS is stored on read-only memory (ROM), and is not erased when the computer is turned off. The BIOS on newer machines is stored on flash read-only memory, allowing it to be erased and rewritten to update the BIOS.

Bridge—Temporary program translating dates between formats. A forward bridge converts an old file format into a changed file format. A backward bridge converts a changed file format into an old file format. Bridges are required to allow interfaces to open partition boundaries. Early partitions access dates in a different format than newer partitions.

Client/Server Architecture—A network model in which a computer (server) provides services to the workstations (clients) connected to that computer (server). This architecture allows the client to share valuable resources with other clients.

Code conversion—Repairing of the computer code making it Year 2000 compliant.

Compliant—The ability of hardware and software to satisfy a particular requirement such as manipulation of four-digit dates.

Compression—Converting four-digit years into hexadecimal or unsigned packed decimal to fit into two-digit year fields.

Contingency plan—A plan for responding to the loss or degradation of essential services due to the Year 2000 technology issue. Describes the steps and processes to ensure the continuity of these essential services.

Conversion—Translating valid values into another format on a permanent basis; for example, translating two digit years to four-digit year values.

Data simulation—Temporarily changing the date and/or time of system clock by intercepting the date from the system clock, entering in a different date, then sending it back to the program using it.

DDE (Dynamic Data Exchange)—Two-way connection among multiple programs allowing them to exchange data while the programs are running.

Device driver—Program allowing the computer to communicate with a hardware peripheral (i.e. printer).
Diagnostic program—A program that collects information from the computer hardware and peripheral and produces a report used to diagnose technical programs.

DLL (Dynamic Link Library)—Executable subroutine stored separately from the programs using it, allowing for efficient use of memory because they are loaded into memory as needed. The DLL file name extensions are .DLL, .DRV, and .FON.

Embedded system—A singular functioning device containing a microprocessor, whose inability to handle two-digit dates or leap days can cause the device and the system that uses it to shut down.

LOC (Lines of Code)—Measures size of an application program, indicating the amount of code to be analyzed and/or converted.

Mission-Imperative/Critical System—System or element whose dysfunction would immediately or eventually create a critical situation. Mission-critical systems are those for which no workarounds have been devised.

Motherboard—Circuit board containing the computer’s CPU, RAM chips and expansion slots; also known as the system board or mainboard.

Network—Two or more computers joined by some type of transmission media (i.e. cable, telephone lines or satellite) to share storage devices and peripherals.

ODBC (Open Database Connectivity)—Standard used to transfer data between two databases written with two different programs (e.g., Microsoft Excel and Microsoft Access). However, the two programs must support this standard.

Partitions—Set of applications and data dividing the overall work effort into separate manageable data.

Performance test—Testing an application that has been modified to ensure it meets its throughput, response time and availability criteria.

Peripheral—Any device connected to a computer to perform a specific function.

Regression test—Test performed before production to identify and prevent errors and verify that unchanged software will continue to function as designed.

Risk analysis—Combination of risk assessment and risk evaluation performed at a specific time.

Risk assessment—Activity performed to identify and estimate probability and impact of risks to assess damage or loss from system failures.
Risk evaluation—Process used to determine the acceptability of risks.

Risk management—Management approach to prevent and reduce risks and their impact.

Risk mitigation—Procedure to eliminate or reduce the impact or likelihood of a risk.

Risk/threat—Negative event or occurrence that could endanger a function or subsystem of an organization.

Server—Program in the client/server architecture that answers client’s requests. The server is also the computer that makes resources available to the workstations (clients) on the network.

Shareware—Copyrighted software distributed on a free-will donation basis through the Internet.

Short date format—Using two digits to specify a year. Computers not yet Y2K-compliant can interpret “00” as the year 1900 or 2000.

Source code—Formal program language in which a computer program is written.

SQL (Structured Query Language)—Database language used by a relational database to query, modify and manage information.

Standardization—Enforcement of standard date formats, names and routines.

Strategic plan—Long-term, high-level plan identifying goals and steps to achieve goals.

System infrastructure—Information management functions supported by computer and communication hardware, software, database, people and policies.

Terminate and stay resident program (TSR)—Program remaining in memory, showing no sign of existence until it is needed to perform a particular function (e.g., screen savers are activated only after a predetermined length of inactivity).

Validation—Evaluating a system during or at development completion to determine if it satisfies all the requirements.

Y2K compliant—System capable of accurately and efficiently processing date and time data, including but not limited to calculating, comparing and sequencing date and time data from into and between the years 1999 and 2000. Also applies to systems used in combination with other technologies.
Possible Problem Dates

- September 9, 1999: general testing date
- January 1, 2000: the new year
- January 3, 2000: first full work day of the new year
- January 10, 2000: first nine-character date
- February 29, 2000: first nine-character leap year
- October 10, 2000: first 10-character date
- December 31, 2000: 366th day of the year
- January 1, 2001: first day of the 21st century
Endnotes

1 Based on material supplied by Chief Jim Brown of the Hudson, Ohio, Police Department.

2 The coordination of multi-discipline and multi-jurisdictional resources in disasters cannot be left to voluntary cooperation along. The responsibility to efficiently direct and coordinate activities of all resources toward a common objective requires unity of command. This is best achieved by vesting a single person, called the Incident Commander, with the authority to take whatever actions are necessary to properly direct and control the resources under their command.
Professional Acknowledgements

This project has been supported by numerous IACP members who have worked diligently to prepare law enforcement for Y2K. The generous input and review these individuals have provided is indicative of the willingness of IACP's 17,000 members to support each other in the interest of their profession.

Philip A. Broadfoot, Chief of Police, Waynesboro, Virginia, Police Department
Jim Brown, Chief of Police, Hudson, Ohio, Police Department
Major Bernard H. Levin, Ed.D., Waynesboro, Virginia, Police Department
Lieutenant Donald McLellan, Ph.D., Oakland County, Michigan, Sheriff's Office
David Morreau, Royal Canadian Mounted Police
David J. Skaret, D.B.A., Y2K Coordinator, Virginia Department of State Police
Commander G. Thomas Steele, Alexandria, Virginia, Police Department

IACP Staff

Daniel N. Rosenblatt         Executive Director
Eugene R. Cromartie          Deputy Executive Director
Charles Higginbotham        Project Response Director
G. Matthew Snyder           Y2K Project Manager

Content

Brian Chodrow               Primary Author
Renee Cobb                  Contingency Planning Developer
Mark Henriquez              Content Reviewer
Thomas Robey                Glossary Developer
Jeff Stump                  Content Reviewer
Rebecca Waldroup            Resource Directory Developer

Production

Rebecca Hoeckele            Editor in Chief
David Paulson               Technical Support Specialist
Jennifer Wykoff             Designer

Marketing and Dissemination

Elisa Cohen                 Marketing Manager
Robert DelCore              Training Developer
Katherine Spivey            Web Publisher

This report was provided to you as a service of the IACP’s Project Response Activity.