

YEAR 2000 EMERGENCY MANAGEMENT

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY

OF THE

COMMITTEE ON
GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

FIRST SESSION

MARCH 22, 1999

Serial No. 106-59

Printed for the use of the Committee on Government Reform



Available via the World Wide Web: <http://www.house.gov/reform>

U.S. GOVERNMENT PRINTING OFFICE

61-297 CC

WASHINGTON : 1999

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington,
MARK E. SOUDER, Indiana	DC
JOE SCARBOROUGH, Florida	CHAKA FATTAH, Pennsylvania
STEVEN C. LATOURETTE, Ohio	ELIJAH E. CUMMINGS, Maryland
MARSHALL "MARK" SANFORD, South	DENNIS J. KUCINICH, Ohio
Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, Jr., Tennessee
GREG WALDEN, Oregon	JANICE D. SCHAKOWSKY, Illinois
DOUG OSE, California	-----
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont
JOHN T. DOOLITTLE, California	(Independent)
HELEN CHENOWETH, Idaho	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

CARLA J. MARTIN, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

BONNIE HEALD, *Communications Director/Professional Staff Member*

HARRISON FOX, *Professional Staff Member*

MASON ALINGER, *Clerk*

FAITH WEISS, *Minority Counsel*

CONTENTS

Hearing held on March 22, 1999	Page 1
Statement of:	
Heckler, Margaret, attorney at law, former Secretary, Department of Health and Human Services; Michael Humphrey, business director for telecommunications and information, Public Technology, Inc.; James Morentz, president, Essential Technologies, Inc.; Phyllis Mann, president-elect, International Association of Emergency Managers; and Lawrence Gerschel, Lawrence and Alberta Gerschel Foundation	77
Walker, Michael, Deputy Director, Federal Emergency Management Agency, accompanied by Lacy Suiter, Associate Director, Response and Recovery Directorate, Federal Emergency Management Agency	5
Letters, statements, etc., submitted for the record by:	
Heckler, Margaret, attorney at law, former Secretary, Department of Health and Human Services, prepared statement of	81
Humphrey, Michael, business director for telecommunications and information, Public Technology, Inc.: Guide to Y2K and You	157
Prepared statement of	90
Mann, Phyllis, president-elect, International Association of Emergency Managers, prepared statement of	115
Morentz, James, president, Essential Technologies, Inc., prepared statement of	101
Walker, Michael, Deputy Director, Federal Emergency Management Agency: Guide for State and local emergency managers	22
Prepared statement of	7

YEAR 2000 EMERGENCY MANAGEMENT

MONDAY, MARCH 22, 1999

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn, Biggert, and Turner.

Staff present: J. Russell George, staff director and chief counsel; Bonnie Heald, director of communications, professional staff member; Harrison Fox, professional staff member; Mason Alinger, clerk; Kacey Baker and Richard Lukas, interns; Faith Weiss, minority counsel; and Jean Gosa, minority staff assistant.

Mr. HORN. The Subcommittee on Government Management, Information, and Technology will come to order.

From hurricanes and earthquakes to nuclear accidents and Y2K computer meltdowns, disaster scenarios continue to provide a lucrative business for Hollywood movie makers. Most of us enjoy those disasters on the silver screen, but we don't expect them to occur in our backyard. When they do occur, the human tendency is to assume that they happen to someone else.

History is replete with examples of ill-equipped regimes, cities, and business and governments experiencing natural and man-made disasters. Such lessons should promote preparedness; but, distressingly, fear of unknown consequences places citizens at the risk of either overreacting or not reacting at all.

Fortunately, as we prepare to enter the new millennium, there is heightened awareness within the world, and specifically within Congress, of new man-made risks that must be considered in emergency planning. The possibility of widespread computer problems associated with the year 2000 is a concern. But it is only one concern among many.

As a Nation, we must prepare for disasters of all types, man-made and natural. Unlike hurricanes and earthquakes, we know when the year 2000 problem will occur. Since 1996, there has been diligent work to prevent widespread disruption in our national infrastructure; however, the Social Security Administration began its work in 1989. It is unfortunate that neither the legislative branch nor the executive branch understood the complexity of the management issues involved.

Since April 1996 when this Subcommittee on Government Management, Information, and Technology has held various investigations and been in the forefront of how those investigating citizens, private sector, and governments can best prepare for these emergencies, we have continued to prod Federal agencies to ready their computer systems for the year 2000.

As the most recent report card reflects, the Federal Government is working extremely hard to meet the unstoppable January 1st deadline. Some agencies have been highly successful. A few others lag behind. The year 2000 computer challenge, often called the millennium bug or Y2K, dates back to the 1960's and 1970's when computers were bulky in size but small in memory, and a few programmers had the bright idea, Why are we wasting all of this space by putting in "1967," why don't we just put in "67"; the first two digits are assumed to be 19.

Unless corrected, these date-sensitive computer systems and microchips embedded in countless mechanical devices may misinterpret the 00 in 2000 as 1900. The fear is that this confusion may cause the systems to generate erroneous information, corrupt other systems or possibly shut down.

While the Federal Government is moving ahead with its Y2K readiness, we remain concerned about State, local and international agencies, as well as businesses that exchange information with systems. Nearly all of us who have been closely monitoring this agree that the year 2000 won't cause a massive shutdown of the Nation's infrastructure, but there may be inconveniences, some of which could require an emergency response. Every citizen and resident of this Nation needs to know that if they need help, help will be available.

Today we will hear from both public and private sector emergency management experts. We have asked them to report on the preparations that are underway for managing emergencies, concentrating on the response to the year 2000 computer problem and other recent concerns, such as biological and chemical threats.

In addition to our distinguished panel of witnesses, immediately after today's hearing, four report groups will convene in workshops this afternoon and tomorrow morning.

The first group will explore the role of technology in emergency management.

A second group will identify the Y2K needs of citizens and emergency management response, specifically evaluating what needs to be in a year 2000 tool kit.

A third group will sketch out a strategic emergency management plan focusing on key emergency management policy issues involving both public and private sectors.

The fourth group will review the latest disaster information systems that could be used domestically and internationally.

The workshop groups will report their conclusions at 11:30 a.m. tomorrow morning in room 2203 of the Rayburn House Office building.

Before we introduce the panel of witnesses, I yield time to the ranking minority member, Mr. Turner of Texas. And we appreciate you coming.

Mr. TURNER. Thank you, Mr. Chairman. I appreciate the opportunity today to review the emergency management procedures with an emphasis, of course, on the Y2K problem. The hearing and the workshop format by which we are addressing these matters is unusual for the Congress, and I am interested in seeing how useful this approach will be for the participants as well as for the public.

The focus of the workshop will include the review of two areas: emergency management in general—ranking from man-made occurrences to national disasters such as flooding and hurricanes—and the specific emergency management preparation for Y2K. Y2K presents some serious and unique challenges for this country, because we are technologically dependent.

While there are those who will panic in reaction to potential Y2K problems, Americans generally are not prone to overreaction. And it is my hope that the mainstream media will maintain responsible journalism to avoid unnecessarily inciting panic or anxiety on the part of the American people.

It should be comforting to learn that the Federal Emergency Management Agency [FEMA], has been actively engaged in preparing for the date change. FEMA has reached out actively to, among others, the State and local emergency managers. FEMA is also holding Y2K workshops in each of its 10 regional offices, and these workshops bring Federal representatives, State and local emergency managers, State fire marshals, and State Y2K coordinators to the table to discuss the unique challenges presented by Y2K.

Governments are working hard to assure that they are prepared and there will be steps that individuals should take as well. People should check with the manufacturers of any essential computer-controlled equipment they use, prepare basic emergency supply kits and have a battery-operated radio and television available. This basic advice is not offered to scare people, but simply to ensure that they are prepared for any temporary problems which may occur. Some advice, though well-intended, may actually create significant problems that otherwise would not exist.

Unnecessary overreaction may well be our greatest potential obstacle on January 1, 2000. For example, advising people to fill their gas tanks on December 31st will cause a gas shortage on that day. Advising those who use prescription drugs to purchase a 3-month supply might also create artificial shortages, one which could most seriously harm those who are in need of prescription medications but are financially unable to purchase them in advance.

We must strive to assure that legitimate concerns are addressed without causing undue fear and anxiety when commenting on Y2K readiness. This hearing should be helpful for Americans to learn what the Federal, State and local governments are doing to minimize any inconveniences due to Y2K.

In closing, I would like to thank the witnesses and participants who have come here today. I look forward to hearing your opinions on emergency management, and I look forward to meeting the challenge of Y2K.

Thank you, Mr. Chairman.

Mr. HORN. I thank the gentleman for his excellent statement, and now yield to the vice chairman of the subcommittee, Mrs. Biggert of Illinois.

Mrs. BIGGERT. Thank you, Mr. Chairman. I too am pleased to participate in today's hearing on the emergency management challenge of the year 2000. As our witnesses I am sure know, today's hearing is one of a series of hearings on the Y2K issue. And the subcommittee has heard testimony from a variety of governmental departments and agencies as to their various level of preparedness for continued computer capacity in the new millennium.

As prepared as the United States may be, situations are likely to arise during the year 2000 date change that we have not anticipated. Emergency management may be an essential component of our ability to deal well with these unexpected aspects of the new millennium. I am interested to hear today's testimony on the emergency management and our readiness for the challenges that we face.

I will also be interested to review the results of the accompanying workshops related to today's hearings. Working groups will focus on the development of a Y2K tool kit for individuals and families, preparation for local governments and policy issues for both the public and private sector. I am pleased to see this emphasis on education and preparation for all sectors of our society. And I look forward to the testimony and accompanying materials to address each of these areas.

Thank you again, Mr. Chairman, for your work in preparing this hearing.

Mr. HORN. Thank you. I appreciate your thoughtful statement. Let me just note the procedure this morning. We have two panels. And we, by tradition of the full committee and the subcommittee, swear in all witnesses. And No. 3, the minute you are introduced, your statement is automatically made a part of the record, the full statement.

We would appreciate it if you could summarize in your own words the statements so we would have more time for dialog and questioning.

So with the first panel, we have Mr. Michael Walker, the Deputy Director, Federal Emergency Management Agency, otherwise known as FEMA, accompanied by Mr. Lacy Suiter, the Associate Director, Response and Recovery Directorate, Federal Emergency Management Agency.

If you gentlemen, plus any assistants that are behind you that might comment, please have them all stand. We will have a massive baptism and swearing in at the time.

Mr. WALKER. Mr. Chairman, also Kay Goss, who is our Associate Director for Preparedness; Clay Hollister, our Associate Director for Information Technology, and Carrie Brown, our Fire Administrator.

Mr. HORN. Thank you very much.

[Witnesses sworn.]

Mr. HORN. All five possible witnesses and actual ones have affirmed the oath.

And we know you have a time schedule, Mr. Walker, and we are going to try to accommodate you. So you have got a lot of traveling today.

Mr. WALKER. Yes, sir.

Mr. HORN. So please go ahead.

STATEMENT OF MICHAEL WALKER, DEPUTY DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY, ACCOMPANIED BY LACY SUITER, ASSOCIATE DIRECTOR, RESPONSE AND RECOVERY DIRECTORATE, FEDERAL EMERGENCY MANAGEMENT AGENCY

Mr. WALKER. Mr. Chairman, thank you very much. And on behalf of FEMA's Director, James Lee Witt, I want to thank you for inviting us to participate in these hearings.

Mr. Chairman, a great deal of progress has been made on Y2K and progress is being made every day. As Mr. Turner points out, we are holding 10 regional workshops around the country, in fact, we will be leaving here to fly to the West Coast for the last 3.

In those workshops, Mr. Chairman, we're finding that awareness is growing, and that more is being done to prepare for Y2K than frankly we had expected to find when the workshops began. So it is important to say the sky is not falling because of Y2K. We are in agreement with the assessment that Y2K should not result in major disruptions in America's basic infrastructure.

Of course, there is so much hype and misleading information on Y2K these days, it is very difficult for the American people to sort fact from fiction. There are those who seek to scare people or profiteer from Y2K; others who bury their heads and risk a "wait and see" attitude; and still others who fear panic and downplay the whole thing. All of those approaches are wrong. They mislead the American people.

To those who are afraid, let us assure them, there's no need for horror. There is no need to take money out of banks. There is no need to head for the hills. In fact, those kind of extreme reactions could actually cause a disaster that otherwise would not happen.

To those who would wait and see or those who are downplaying Y2K, let us say, Y2K does not fix itself. Let us remind them that fixing Y2K is about leadership. It is about taking responsibility. And it is not too late. The biggest challenges are in the small business sector and in smaller towns and counties.

I am from a small town, myself, in Tennessee, and I understand how difficult it is to scrape up the money to make infrastructure investments on the local level. But I also know that failure to fix Y2K will cost communities and businesses much more later on and, at the same time, endanger the well-being of American families. Of course, no one believes that every computer will be reprogrammed or every date-sensitive embedded computer chip found and replaced by the end of the year.

So while we do not now expect major dislocations, the emergency management community is preparing to deal with the potential consequences of localized disruptions. And I would emphasize that where those disruptions occur will depend entirely on where the Y2K problem has been fixed and where it has not. So local leaders must wait no longer to assess their communities' Y2K compliance and fix their critical systems.

The truth is, Mr. Chairman, the Y2K challenge pales besides the great challenges Americans have faced and conquered throughout our history. So I commend this committee for helping to get the word out that, while progress is being made, the job is not complete and that we must fix Y2K where it has not yet been fixed, and that

all of us share in the responsibility not to wring our hands, but to fix the problem and rise to the occasion as Americans have throughout our history.

Thank you, Mr. Chairman, we look forward to your questions.
[The prepared statement of Mr. Walker follows:]

STATEMENT FOR THE RECORD

MIKE WALKER

DEPUTY DIRECTOR
FEDERAL EMERGENCY MANAGEMENT AGENCY

BEFORE THE

COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND
TECHNOLOGY

UNITED STATES HOUSE OF REPRESENTATIVES

MARCH 22, 1999

Good morning Mr. Chairman and Members of the Committee. Thank you for the opportunity to appear before the committee on the Y2K issue.

My name is Mike Walker. I am the Deputy Director of the Federal Emergency Management Agency. Joining me here today is Lacy Suiter, who is our Executive Associate Director for Response and Recovery. Mr. Suiter and I are pleased to be appearing before you.

In the audience is Kay Goss, FEMA's Associate Director for Preparedness, Training, and Exercises and Clay Hollister, Executive Associate Director for Information Technology Services.

I would like to describe FEMA's efforts to address the potential threat posed by the Year 2000 (Y2K) technology problem for fire services and emergency management within the United States.

FEMA'S ROLE IN THE PRESIDENT'S COUNCIL ON Y2K CONVERSION

FEMA has a role as one of the approximately twenty-five sector coordinators supporting the President's Council on Y2K Conversion, chaired by John A. Koskinen, Assistant to the President. FEMA chairs and coordinates efforts of the Emergency Services Sector (ESS) working group. Primary member agencies include FEMA, the Departments of Agriculture, Commerce (mainly the National Oceanographic and Atmospheric Administration), Defense, Health and Human Services, Interior, and Transportation. The American Red Cross participates as an honorary member. FEMA and the other Emergency Services Sector members are responsible for increasing awareness of emergency services providers throughout the Nation and for encouraging them to assess the readiness of their technology-based systems to support operations before, during, and after the clock rolls over to the year 2000. It is important to clarify that FEMA does not have a role in repairing the billions of bytes of public and privately held computer code infected by the Y2K bug. FEMA does not have the regulatory authority, the technical expertise, or the resources - required to do so.

BRIEF ASSESSMENT OF GOVERNMENT PREPAREDNESS FOR THE YEAR 2000

We submitted our latest report on the ESS to the President's Council on Year 2000 Conversion on March 5, 1999. I will provide a full report for the record and summarize the most significant findings here.

There has been significant progress in assessment of the Emergency Services Sector (ESS) since publication of the initial report of the President's Council on Year 2000 Conversion, dated January 7, 1999. ESS organizations continue to obtain important information for areas such as the fire service and 911 centers, State and local emergency management organizations, emergency medical services, and other professional and private emergency management organizations. It should be recognized that this information is being provided to us on a voluntary basis and that

numerical values cited in this report may not be statistically representative of the populations sampled. ESS member agencies listed in the initial Council report contributed to this report through the period ending March 1, 1999.

At this point we can report that State-level emergency preparedness offices are making good progress but there continues to be a wide disparity of readiness, in general, in emergency service systems at the county and municipality level. Noting this, FEMA is increasing its outreach activities, and through its Regional offices is working with State and local emergency management and constituent organizations, as well as others, to broaden and accelerate Y2K emergency services preparedness at the local level.

Two areas, in particular, need increased attention: 911 and the fire services.

"911": To date, 584 9-1-1 centers in 35 States (13 percent of the 4,300 centers) have responded to a mailing conducted in partnership of USFA with the National Emergency Number Association (NENA). The results show 17 percent of the centers are now compliant, and an additional 69 percent, or 86 percent in all, expect to be ready by January 1, 2000. Forty (40) percent have contingency plans in place.

Fire Service: The United States Fire Administration (USFA) and its partners have obtained the following information regarding Y2K readiness: Surveys of more than 2300 students at the National Fire Academy (NFA), generally mid- to upper- level managers in fire departments, representing almost 1,300 departments and all 50 States, reveal that 98 percent of departments are aware of potential problems, 77 percent are actively working on solutions, and 35 percent already are fully Y2K compliant.

A survey of 10 representative fire departments in each State, conducted by the National Association of State Fire Marshals (NASFM), has produced 57 responses to date (11 percent of the 500 departments surveyed) in 14 States and shows that 95 percent have assessed their vulnerabilities, over 90 percent expect to be compliant by January 1, 2000, but less than 50 percent presently have back-up or contingency plans.

OUTREACH TO THE EMERGENCY SERVICES SECTOR ON Y2K

FEMA and the other Emergency Services Sector members are actively reaching out to their respective constituencies. For example, HHS is in contact with hospitals, clinics, and other health-related facilities across the country. DOD's Corps of Engineers is working with the private sector contractors who provide services such as debris removal. These Federal agencies are heightening awareness and will provide assessments in the fire services community, emergency medical services community, the National Guard, and, of course, emergency management services, including the volunteer agencies supporting disaster response.

FEMA's outreach to the fire services community and State and local emergency management is described in more detail below.

Fire Services

FEMA's United States Fire Administration (USFA) has initiated a multi-phased plan to raise awareness and assess readiness on the Y2K technology problem. This approach was selected to take greatest advantage of the decentralized and independent structure of the fire services community.

Fire Administration staff issued a suggested article for the fire and emergency services publications on Y2K preparedness. Staff have also been interviewed by a variety of fire and emergency services publications for articles on the Y2K issue.

In August 1998, FEMA developed a list of frequently asked questions regarding Y2K, along with answers, and formatted them into a Y2K brochure. The brochure is made available to students attending classes at the National Fire Academy. The brochure has been mailed to the major fire service organizations and the State Fire Marshals, along with a cover letter asking them to help get the word out to fire and emergency services nation-wide. The brochures are also available for local distribution. Approximately 33,000 individual fire departments across the country were sent copies of the brochure. FEMA also sent materials to associations of fire and emergency service equipment manufacturers and distributors, and asked them to share information on actions their members are taking to ensure that their products are Y2K compliant.

The Fire Administration has enlisted the aid of State Fire Marshals in determining local fire service readiness for the Year 2000. Throughout FY99, Y2K will be featured as an important topic in speeches and conference displays developed for the fire and emergency services community.

State and Local Emergency Management

FEMA's Preparedness, Training, and Exercises Directorate provides grants, guidance, training, and exercise assistance to State and local governments to help them to prepare for all types of emergencies. FEMA has initiated activities to address the Y2K problem and is aggressively pursuing outreach activities with its primary constituents, the State and local governments, through their national organizations, the National Emergency Management Association (NEMA) and the International Association of Emergency Managers (IAEM). A main emphasis of this outreach effort is to heighten awareness of State governments, and indirectly of local governments, on the criticality of this issue and to provide Y2K emergency preparedness guidance and information.

At the September 1998 NEMA Annual Conference in Charleston, South Carolina, the new NEMA President identified Y2K as a priority area for NEMA to address this year in full coordination with FEMA. NEMA and IAEM have discussed with FEMA's Associate Director for Preparedness, Training and Exercises the importance of and need to develop emergency preparedness measures and guidance to deal with potential Y2K issues. During the Fall, the States and territories were surveyed on their progress in

addressing Y2K and it became very apparent that guidance on contingency and consequence management planning was needed, especially at the local level. In response to this expressed need, we have published 75,000 copies of a planning guide, entitled "Contingency and Consequence Management Planning for Year 2000 Conversion: A Guide for State and Local Emergency Managers." Copies of the Guide are being distributed to the States, territories, local communities, and at regional Y2K workshops and various other conferences. The Guide was developed with assistance from NEMA, IAEM, and the President's Council on Year 2000 Conversion. While it is addressed to emergency managers, the guide can be useful for private organizations and the public as well.

In addition, we have published a Y2K Bulletin which is a consumer's guide to preparing for the Year 2000. FEMA has received numerous positive comments on both the planning guide and consumer bulletin, and we anticipate an increased demand for the documents, which are also available on the FEMA website homepage. Information on model State and local Y2K programs and practices is also being collected and will be posted on our website.

As part of FEMA's training activities, the Emergency Management Institute (EMI) has instituted a "Y2K Show-of-Hands Survey" at the beginning of every class, which includes the following questions:

- Are you aware of the potential problem facing all computer systems called "Y2K" that involves the computer's ability to accommodate the change to the year 2000?
- Is your organization actively working to ensure that its computer systems are able to deal with this potential problem?
- Are the computer systems in your organization currently fully prepared to successfully accommodate the change to the year 2000?

The survey provides immediate feedback on Y2K preparedness at all levels of government. More importantly, it raises the awareness of students at EMI and highlights the need for action. EMI is examining ways to insert Y2K considerations into the exercise scenarios for the Integrated Emergency Management Courses. Y2K considerations add value to an all-hazards curriculum by focusing attention on consequences and operational requirements that could also emerge during other types of technological emergencies.

To further the training outreach to our State and local emergency management partners, a new Y2K awareness course has been developed by FEMA's EMI for state and local emergency managers. The course will be launched in April and will be available in residence at EMI and through regional and state train-the-trainer sessions, Internet downloading and on CD-ROMs. We have also produced Y2K awareness training information for all FEMA employees. Our Emergency Education Network will be used to broadcast information on Y2K planning and preparedness activities as part of the monthly

National Alert Broadcasts. These updates will address Y2K efforts taken by FEMA and State governments and offer planning information for the general public. Three more detailed Emergency Education Network Broadcasts will cover the results of regional Y2K workshops and community and family preparedness.

To date, we have held seven of ten Federal regional "workshops" which we are conducting across the country to further increase awareness and encourage assessment of emergency managers' readiness. In fact, this morning Mr. Suiter and I will be heading directly to the airport to go and kick off the last three workshops in San Francisco, California; Vancouver, Washington; and Denver, Colorado. We are part of a national team comprised of senior leadership from FEMA and nine other Federal agencies, presenting the national Y2K overview, which is followed by breakout group discussions. The expected outcomes of the workshops are:

- (1) heightened awareness, promotion of functional continuity planning, and shared ideas;
- (2) identification and prioritization of categories of assistance that may be required;
- (3) identification of actions to be taken by States;
- (4) identification of Federal Government actions; and
- (5) input to help form a national integrated consequence management strategy.

Last month, Director Witt addressed the National Governor's Association on the status of several FEMA initiatives, including Year 2000 outreach, and offered suggestions on what the Governors can do to further the efforts to raise awareness, promote personal responsibility, and ensure operational readiness at all levels of government.

FEMA'S RESPONSIBILITY UNDER THE FEDERAL RESPONSE PLAN

The final element of our strategy, for which the Executive Associate Director for Response and Recovery is responsible, is to ensure that if preventive measures fail, the signatory agencies to the Federal Response Plan are primed and ready to assist State and local governments with response to consequences of a Y2K problem affecting lives, property, and public health and safety. It has been our experience that consequences of an order of magnitude to require assistance under the Federal Response Plan fall into a consistent set of functional areas, regardless of the type of hazard that caused the emergency. The Plan is organized to provide assistance to State and local governments in transportation, communications, public works and engineering, firefighting, information and planning, mass care, resource management, health and medical services, hazardous materials, food, and energy.

A Y2K technology problem will create two sets of needs. The first includes technological support to the owner/operator of the disrupted system, such as advice on technical work-around options, and repair or replacement of disrupted hardware, software, or networks. The Federal Response Plan is not designed to meet this need. This is the job of information technology professionals in each owner/operator

organization, public and private, to address through internal business continuity plans, with the on-going technical assistance from the Federal agencies represented on the President's Council on Y2K Conversion. The second set of needs includes emergency assistance to State and local governments, to enable them to continue to perform essential community services, such as issuing emergency warnings, disseminating public health and safety information, carrying out health and safety measures, reducing immediate threats to public health and safety, providing temporary housing assistance, and distributing medicine, food, and other goods to meet basic human needs.

It is difficult to determine the exact nature and extent of the threat posed by the Y2K problem. Reports in print and television media and on the Internet range from predictions of business-as-usual to some form of cyber winter. To identify and prioritize actions to take to ensure we are able to provide assistance to State and local governments, we need credible assessments from authoritative sources that describe specific vulnerabilities, areas at highest risk, and potential consequences that could lead to activation of the Federal Response Plan. We believe that the quarterly assessments published by the President's Council on Y2K Conversion are authoritative sources for information on this hazard.

The Council is scheduled to release its second quarterly assessment report in mid-April. John Koskinen, Chairman of the President's Council on Y2K Conversion, attended our January meeting of all Federal Response Plan agencies, and stated that, domestically, he is most concerned about small- and medium-sized organizations (public and private), and over-reaction by the public. He re-iterated that based upon current assessment data, the basic infrastructure will work through the Y2K transition, and that nationwide catastrophic disruptions are unlikely. However, he stated that there may be requirements for Federal response in some service sectors and in some geographic areas.

Our primary operational objective will be, in accordance with the Robert T. Stafford Disaster Relief and Emergency Assistance (Stafford) Act, to respond to physical consequences on lives, property, and public health and safety. It is difficult to imagine a Y2K scenario that would trigger widespread physical consequences that threaten lives and property. However, a Y2K scenario could cause scattered disruptions in critical systems such as traffic control, communications, or power, which would complicate local, State and Federal efforts to provide disaster response. I am particularly concerned about rural areas in northern and western states in December and January, which is severe winter storm season.

We are developing a Y2K Operations Supplement to the Federal Response Plan, which will be used in case there is a need for Federal assistance. Our operations concept will be to activate monitoring operations through the critical conversion period here in Washington and in our regional operations centers, and to request information technology liaisons with access to FEMA internal and interagency sources of technology support. We may not be able to respond to requests for technology support, but we can use the Federal response system to provide a backup network to ensure

that such requests from State and local governments are referred to the appropriate public/private coordination channels that have been established through the efforts of the President's Council on Y2K Conversion.

We continue to hold monthly meetings with officials of the primary agencies of the Federal Response Plan to focus attention on potential needs and options. Agencies have reported that the majority of mission-critical facilities and support systems necessary to conduct Federal Response Plan operations will be functional through the Y2K conversion period. Agencies are developing work-around options for those that will not be ready by March 31, 1999. FEMA is doing all that it can, as the lead agency for the Federal Response Plan, to encourage Federal Response Plan agencies to work with their partners in the State and local emergency management and fire service communities, to promote awareness and business continuity planning for Y2K.

The Y2K technology problem involves several dimensions and touches upon nearly every aspect of day-to-day business in the world. The efforts of emergency management and fire service organizations cannot be viewed as a substitute for personal responsibility and personal preparedness. Every organization and every individual, in public and private life, has an obligation to learn more about this problem and their vulnerability, so that they may take appropriate action to prevent a problem before it occurs. As elected leaders, you also play an important role in increasing public awareness and promoting personal initiative through a range of activities, such as this hearing. We in FEMA respect your concern and your commitment to this issue. At the same time, FEMA is working with the emergency management and fire services communities to raise awareness, to increase preparedness, and to stand ready to provide Federal response assistance to State and local governments, if required. We will keep you informed on our progress as the countdown to the new millenium continues.

Mr. HORN. Thank you. I will yield my time to Mrs. Biggert, the vice chairman of the subcommittee. Mrs. Biggert, the gentlewoman from Illinois.

Mrs. BIGGERT. Thank you, Mr. Chairman.

Mr. Walker, you said that there was a wide disparity of readiness in general. What about the emergency service systems at the county and municipality level; is this just indicative of the Y2K problem, or is this something that's indicative of just emergency readiness in general?

Mr. WALKER. Well, Congresswoman, the emergency management system at every level of the country has improved substantially in the past several years. Director Witt has made a great effort to work with the States, and the States working with local communities to improve emergency management.

I remember when I was first growing up in Tennessee, emergency management in the fifties during all the floods was essentially neighbor to neighbor.

Well now we have, thanks to this fellow next to me, Lacy Suiter—who was the emergency manager for many years in Tennessee before he came to Washington—a very professional emergency management system at every level. We're finding that every level of government is greatly improved from where it used to be, but, of course, just like any other institution, it differs from place to place.

Mrs. BIGGERT. Are there special—is there special attention to 911 or any of those emergency systems of what will happen?

Mr. WALKER. Well, with regard to 911 specifically, there are 4,300 911 systems in the country. Through the Fire Administration, we have conducted a survey of 911 systems participating with the National Emergency Number Association. What we're finding is we're beginning to get responses back from those requests, and we're finding that work still needs to be done in some of the areas. So we're going back out and resurveying the 911 systems, quite frankly, as an effort to remind them that they must get on with the job.

Mrs. BIGGERT. What then about the fire departments? Is this something—is there a way to communicate media crisis information to and from these fire departments?

Mr. WALKER. Oh, yes. We have already been in touch with 32,000 fire departments around the country, and they're hard at work at making their systems compliant. And we feel very confident that the vast majority of fire departments will be Y2K compliant.

Mrs. BIGGERT. Are there some that are holding out on this?

Mr. WALKER. It is like I said in my opening statement, it is a bigger challenge in smaller towns and communities, in large part because it costs money. And I found out over the weekend, for instance, that the neighboring town to mine in Tennessee just found out they're going to have to spend \$200,000. That is a lot of money for a small town.

Mrs. BIGGERT. All right. Then do you think that the established channels of the communication between the Federal Government, the State and the local government are sufficient?

Mr. WALKER. I do. And Lacy might want to comment on that.

Mr. SUITER. Certainly between the Federal Government and the State government, there are a number of independent systems which are not dependent upon the normal telephone switch networks to communicate with them. With the National Warning System, we can talk to every State all at the same time on one of the world's largest party lines, if you will, and get information back the other way. And that goes to about 2,000 different communities all across the country, also in the larger communities, as well as other warning points around the country.

And then there are the side band HF radios that are in place—there's any number of redundant communications to the States. Many States have far superior communications with their local governments than even the Federal Government does. Those are currently all going through an evaluation process, which we will have some information by the end of April, by April 26th actually.

Mrs. BIGGERT. Who really—who is responsible really for developing these communications, the Federal Government or the States or the locals?

Mr. SUITER. Between the Federal Government and the State government, obviously FEMA and the different Federal agencies that are involved have different communication systems. FEMA itself has the national emergency systems which connect the President with the Governors and the different State agencies that have emergency responsibilities in it. Between the State government and the local government, it is obviously up to the States to set up whatever type of system they have, and it is different all across the country.

If you go to the State of Arkansas, there's a rather major 800 megahertz system that connects all of the major services together. Different States have different systems. Some of them are satellite driven, such as in California and in Florida.

Mrs. BIGGERT. What would be FEMA's top priorities for ensuring maximum community and individual citizen awareness and readiness to cope with potential problems posed by the Y2K phenomenon?

Mr. WALKER. As we sit here today, our top priority is to get the word out in those communities and businesses that have not yet fixed the problem, to fix the problem. That is the No. 1 thing. We still have 9 months left in the year. Nothing about Y2K is pre-ordained except the date. We know what the problem is, we know how to fix it. It is a matter of leadership and taking the action to do so.

Mrs. BIGGERT. And how are we going to ensure that within 9 months—some of these people are going to have problems, aren't they?

Mr. WALKER. Well, as I said in my opening statement, we—everyone knows that every computer won't be reprogrammed and every embedded chip is not going to be found by the end of the year. So that's why we are preparing for what could be localized disruptions in various communities that frankly just don't make the investments in time.

Mrs. BIGGERT. As I was coming over here today, there was—just caught a snippet on the news—one of the schools had a fifth grader in their school that they wanted to hire to fix their Y2K problem,

because he was the genius of the school that was going to be able to do this. And it was a big thing with the school board about whether they should pay him those big bucks that some of these other people are getting.

Mr. WALKER. I have a nephew like that, I understand.

Mrs. BIGGERT. So I think sometimes people are waiting for that one person that's going to come up to be able to solve this whole problem. And I think we have found that probably isn't true.

Mr. WALKER. It just takes hard work. It is tedious work, but it is work that can be done.

Mrs. BIGGERT. Thank you. Thank you, Mr. Chairman.

Mr. HORN. You're welcome.

I now yield 6 minutes to the ranking member, Mr. Turner of Texas, for the purpose of questioning.

Mr. TURNER. Mr. Walker, what do we know about the status of our electrical power companies? I mean, it seems to me that could be the greatest problem if we have power failures. In my own State, I know Texas Utilities has been quite diligent to be sure they are ready for 2000. What's your impression of the state of readiness?

Mr. WALKER. In fact, with regard to Texas, I just read on the way over here a statement from the Texas Utility Board, I think they released over the weekend, saying they were confident that electric power and telecommunications, et cetera, would be in good shape in Texas. With regard to the electric power grids, we agree with the assessment that a great deal of work has been done, and that there is not an expectation at this point that there will be any kind of widespread electrical power problem.

As you know, the President's Council on Y2K is divided up into 25 major sectors. FEMA chairs the emergency services sector, the Department of Energy chairs the energy sector, and they've been doing a great deal of work through the North American Electrical Liability Council. And all of their findings, by the way, are posted on the web of the Council. So we believe that the national structures are in good shape.

I would note that the Senate committee pointed out that there could be problems in rural areas like rural electric cooperatives. I know in my home when there's an ice storm, they often go down, a little bit longer than others. NAERC has released a statement since that report came out saying that they are—they're staying in touch with their members, there are a thousand of them, and they're working hard to get compliance and they believe they're on track.

Mr. TURNER. Would you describe for me what the general—or generally describe the kind of problem that power companies are having to prepare for? Where is the weak link in the power grid that causes them to have a Y2K problem?

Mr. WALKER. Well, according to what the assessment is from NAERC, there appears to be no weak link in the national power grid at the present time. But I am not an expert on that. I would have to refer you to the Council for specifics.

Mr. TURNER. I have a great deal of concern. I would be interested in your assessment of what you have sensed the public reaction is to Y2K, because I fear—my greatest fear is that we will overreact.

Mr. WALKER. Yes, sir.

Mr. TURNER. I was at home this weekend. Visiting with my dad, and he just happened to mention that he checked into the price of generators and that the one with the electric starter was \$2,600, but you can get one for \$900 if you are willing to crank it. But at his age, he said, "I don't know if I can pull the cord on it to start it." And I was a little bit surprised, and I said, "Dad, I don't really think you need to be worrying about buying an electric generator. And, you know, from my perspective, I really feel that way," and yet my own dad was out there pricing generators.

So give me—you know, you have been traveling around, you have been to these workshops—do you sense a growing panic out there? Are we doing pretty good?

Mr. WALKER. The problem is there's so much misinformation and hype about Y2K. There are people who are really scaring people or trying to profiteer from it. There are people, on the other hand, who just wish it would go away, because they're afraid of panic. And then there are others who are saying, Well, you know, I don't know if it is going to affect me, so I am going to wait to see. All of those approaches miss the mark.

So I think it is very important that we continue the effort that we're engaged in and that this committee is engaged in, in getting the word out to the lowest level of government in the country and to every community that, No. 1, there's no need to head for the hills, that the national structures are in good shape, that most communities are doing what they need to do. But in those that are not, we would encourage citizens to begin asking the question of their local leaders, What are you doing, and are you going to be Y2K compliant? That will help immensely.

Mr. TURNER. I understand the problem you described, talk about embedded chips, and the problem that we may not find all of those problems, and they may be out there. But it just seems to me that the bigger problems, the problem of loss of electric power, that those seem to be becoming fairly remote as possibilities based upon what the power companies are doing.

Mr. WALKER. That's correct.

Mr. TURNER. I really have never had a discussion with anybody in that industry to know. But it would seem to me if there was even a disruption that it would be able to be remedied fairly quickly. In my hometown, I am from a rural area, as you are, we're accustomed to having occasional power disruptions, and you might lose the meat frozen in your freezer, but that's about the extent of it. It seems to me that most of those problems could be very well overstated.

Mr. WALKER. Yes, sir. I agree, Mr. Turner. I mean we have that happen every year. We just had an ice storm in Tennessee. We had ice storms all over the country and power has gone off for a few hours or a few days, and the companies have responded just like they would in any crisis, and got the power back on.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. I thank you. I also grew up in a rural area, and I agree on some of these things that we're talking about.

I think, Mr. Walker, when you and I chatted a week or so ago, I mentioned the problem of frequencies in Los Angeles County. We

have 81 cities there, a county of 10 million people, the largest city being the city of Los Angeles, 3 of the 10 million. I happen to live in the second largest city there, which is about 450,000, half a million. And when I was at the university, California State University at Long Beach, we had our own police force, all the rest. And when we engaged in these exercises, all the channels were jammed; when you have got 81 cities, the sheriff, all sorts of National Guard, Reserves, so forth.

What does FEMA know about our vast urban areas and the ability to communicate? Are they going to be jammed up again, be it riot, earthquake, in our case; fire, flood also in our case, and so forth; what can you tell us about that?

Mr. SUITER. Yes. First of all, Ellis Stanley, who is the director for the city of Los Angeles is with us today and could probably explain more to you about the details of how the city of Los Angeles operates, if anybody can.

Mr. HORN. OK. We will swear him in.

Mr. SUITER. And I would strongly suggest you seek his advice. Basically, since last July, we have been working with the different Federal agencies to make sure that the information that we were passing on to the Governors in this country was reasonably accurate. Information about such things as the power grids, the national communications structure, the fact that the Federal Government itself, in terms of its emergency systems, would be working and the problems we have would be corrected.

We have been spending a great deal of time getting that done. We have been convening all the Federal agencies in the Catastrophic Disaster Response Group, which is part the Federal Response Plan. And defines how the President will manage a potential disaster declaration. We're in the process right now of preparing an operations supplement to that response plan that will say what the Federal Government will do in response to specific requests from the Governors.

We're just about to the end of the 10 regional meetings. As Mr. Walker has indicated, he will be attending the last of these meetings this week. When we get to the end of that, our regions will be giving us a specific assessment, State by State, which is due in to the director by the end of about the 26th, I believe it is, of April. And from that, more information will be compiled and put together so that we will have better information, as an example, of what Mr. Stanley is doing in Los Angeles and the specifics of how all of this is working together.

We hope that as a result of all of this, we are planning for a non-event in the process that would come out, and if it is a non-event, at least it is an event that will have an appropriate reaction and not an overreaction on the part of the public to those things that are concerned.

In New England, last year where we had the major ice storms and we lost major transmission lines and people went without power for 2 or 3 days and it—most communities, I mean there's been a great deal of change in the United States since the turn of the century. Since the turn of the century, a hurricane came to shore in Galveston, TX and killed 6,000 people. It doesn't happen anymore.

That isn't necessarily because the Federal Government or the State government did anything; it happened because the local government communities and their acceptance of the responsibility of what they have to do to prepare their people. That's where all of this occurs first. And that's who owns the disaster.

I would suggest to you, sir, that local community acceptance and responsibility is going on in the country right now. I may not be as easily reportable at this stage as we would like, but in another 30 days we will have a better feel for that level of preparedness. And I think we're going to see a great deal of improvement over the next 30 to 45 days or at least in terms of identifying more specifically for us at the Federal Government what the requirements might be.

Mr. HORN. Does FEMA have a satellite at all that's dedicated to its ability to send messages throughout the United States?

Mr. SUITER. The answer is yes.

Mr. HORN. Is it strictly for the use of FEMA or is it shared? Just identify yourself. Sit down and make yourself at home. There's an extra chair. This is just family folks.

Mr. HOLLISTER. Yes, sir. Clay Hollister, FEMA Chief Information Officer. Yes, we do. We have what we call the FEMA switch network, which is a voice and a data network, which we manage, full period lease circuits, including one satellite transponder. And we manage all of our own switches, and that's our primary source of communications. And we do have that available. For disasters, we use it all the time.

Mr. HORN. Could that satellite be blocked by either a foreign power or somebody in the United States so the communications wouldn't reach the ground?

Mr. HOLLISTER. Congressman, I don't know whether that could be jammed. I really don't know the answer to that.

Mr. HORN. Could we get the answer and put it at this point in the record?

Mr. HOLLISTER. Yes, sir, I will get it for you.

Mr. HORN. Without objection, it will be put at this point in the record.

I think you ought to have a satellite. I think we ought to have a number of alternative means so the Federal Government can communicate, as well as some of the State governments, like California with 33 million people or so, would pay if they could communicate with the cities in California particularly, since we're so earthquake prone and not just not fire prone. We have got enough of those every year, and not just flood prone.

I've got the largest flood control problem in the country in the Los Angeles River alone, with 500,000 people affected in the floodplain, as FEMA knows. And FEMA has been very helpful to get us through this thing, slowly but surely. Two more years, we think the levies will be up, and you will release the insurance that we're going through right now and then that will make my constituents very happy. And five other members' constituents, I might add.

So what about other means of communication?

Mr. HOLLISTER. We also have the FTS system, Federal Telecommunications System. And we have the public switch network.

Mr. HORN. But that FTS system, does it have its own systems throughout the country?

Mr. HOLLISTER. Yes, they're managed by dedicated vendors who manage the switches, as well as the dedicated lines. So that's another fallback. And the third, at least in terms of voice, is the public switch network itself, which we can go out commercially and communicate. We also have HF radio, which communicates. We have a FEMA-HF system, which is there as well. And we have satellite phones which we use in disasters, which we are going to certainly place at each of other regional offices.

Beyond that, we had made—we are looking at the possibility of putting satellite phones in each State emergency operation center as another alternative. We proposed that, and we're waiting to see whether the requirement is still valid for that in the fall based on what we know.

And, finally, Mr. Suiter referred to it, we also have the National Warning System or NWS, which is a two-way 1,500 drop communication system between FEMA, the regions in each State, ERC, so we have a quite robust voice connectivity, sir.

Mr. HORN. Well, getting back to that satellite, and any satellite, what does the Defense Department tell you about the ability of other types of satellites to put a beam into that satellite and just mar it from ever transmitting messages?

Mr. HOLLISTER. Well, I would have to answer that for the record, sir.

I would have to go back to DOD on that. It is a commercial transponder. We lease it from a commercial vendor. It is one of the standard voice transponders up there.

Mr. HORN. Do you have full use of it?

Mr. HOLLISTER. Yes, sir, we do.

Mr. HORN. OK. That's good news.

Mr. HOLLISTER. Yes, sir.

Mr. HORN. Mr. Turner, do you have any other questions?

Mr. TURNER. No other questions, Mr. Chairman.

Mr. HORN. Mrs. Biggert, do you have any other questions?

Mrs. BIGGERT. First of all, just a comment. You might have floods and earthquakes, but in Illinois we have sometimes below-zero weather. And if we don't have the electricity and the heat, it will cause quite a problem, even without any of those national—or natural disasters. So I think in all parts of the country, it is certainly a problem.

Just one other. You have copies of a planning guide——

Mr. WALKER. Yes, we do.

Mrs. BIGGERT [continuing]. Entitled what, Contingency and Consequence Management Planning?

Mr. WALKER. Right. A Guide for State and Local Emergency Managers. We brought extra copies today for the committee.

[The information referred to follows:]

Contingency and Consequence Management Planning for Year 2000 Conversion

**A Guide for State and Local
Emergency Managers**



February 1999

Y2K

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.

Y2K

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.

Y2K

Table 2. Levels of Computer Technology

Hardware	Microprocessor, clock, and the machine's internal clock
Operating Systems	Windows, Unix, etc. (each system has its own upgrades)
Database	Microsoft Access, Oracle, etc. (each application has its own upgrades)
Application	Software, hardware, and the application itself (each application has its own upgrades)
Client/Server	Software, hardware, and the application itself (each application has its own upgrades)
Enterprise System	Software, hardware, and the application itself (each application has its own upgrades)

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.

Y2K

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	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	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.

Y2K

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.

Y2K

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

Y2K

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.

Y2K

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	<input type="checkbox"/> wireless communication systems (cellular phones, pagers)	<input type="checkbox"/> sprinkler/fountain systems
<input type="checkbox"/> telephone systems	<input type="checkbox"/> radar systems	<input type="checkbox"/> fuel dispensing systems (gas pumps)
<input type="checkbox"/> voice mail/answering machines	<input type="checkbox"/> security systems (door locks, safes, vaults)	<input type="checkbox"/> maintenance vehicles
<input type="checkbox"/> facsimile (fax) machines	<input type="checkbox"/> motion detectors	<input type="checkbox"/> other
<input type="checkbox"/> photocopiers	<input type="checkbox"/> parking ticket handheld devices	Water and Wastewater Systems
<input type="checkbox"/> printers	<input type="checkbox"/> police and fire computer-aided dispatch systems	<input type="checkbox"/> pump controller systems
<input type="checkbox"/> scanners	<input type="checkbox"/> surveillance cameras	<input type="checkbox"/> chlorine injection or other effluent disinfecting systems (ultraviolet lights)
<input type="checkbox"/> equipment w/ date stamps (video equipment, scales, time clocks)	<input type="checkbox"/> air traffic control systems	<input type="checkbox"/> lift station pump controllers
<input type="checkbox"/> personal computers	<input type="checkbox"/> fuel dispensing systems (gas pumps)	<input type="checkbox"/> telemetry systems
<input type="checkbox"/> laptop computers	<input type="checkbox"/> contingent systems (systems or functions that are operated by others, but on which the jurisdiction depends for its emergency response operations)	<input type="checkbox"/> vehicle computer systems
<input type="checkbox"/> personal digital assistants (PDAs)/handheld computers	<input type="checkbox"/> 911 systems	<input type="checkbox"/> equipment computer systems (mobile generators, mobile pumping equipment, construction equipment, maintenance and line cleaning equipment)
<input type="checkbox"/> wireless communication systems (pagers, cellular phones)	<input type="checkbox"/> public warning systems	<input type="checkbox"/> wastewater line televising equipment
<input type="checkbox"/> mailroom equipment	<input type="checkbox"/> other	<input type="checkbox"/> contingent systems or functions (systems or functions operated by others but on which the jurisdiction depends for its sewer/wastewater operations)
<input type="checkbox"/> other		<input type="checkbox"/> other
Emergency Response:		
Police and Fire Operations	Public Works	Building Inspections
<input type="checkbox"/> emergency response phone and dispatch systems	<input type="checkbox"/> traffic control systems	<input type="checkbox"/> electrical generation and distribution
<input type="checkbox"/> global positioning systems (GPS) used to track vehicles	<input type="checkbox"/> flood/storm water control systems	<input type="checkbox"/> gas distribution
<input type="checkbox"/> EMT medical equipment (defibrillator; monitoring devices, blood analyzer)	<input type="checkbox"/> electronic scales	<input type="checkbox"/> elevators, escalators, lifts
<input type="checkbox"/> breathalyzer	<input type="checkbox"/> meters	<input type="checkbox"/> building and premises security systems
<input type="checkbox"/> criminal records systems	<input type="checkbox"/> handheld water meter readers	
<input type="checkbox"/> response vehicles, fire trucks, ambulances	<input type="checkbox"/> street maintenance systems	
<input type="checkbox"/> two-way radio systems	<input type="checkbox"/> geographic information systems	
	<input type="checkbox"/> street lighting	

Y2K

- _____ 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.

Y2K

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.

Y2K

Table 4. Important Dates for Y2K

December 31, 1999	Last day of 1999
Throughout 1999	One-year look-ahead date
April 9, 1999	"Mayday" end of file code
September 9, 1999	"End of file" code
February 29, 2000 – March 1, 2000	
December 31, 2000	16th day of uncommon file
January 1, 2000	Rollover date for 2000
July 1, 1999 to October 1, 1999	Start of permanent fiscal year 2000
July 10, 2000	First date in the year 2000 with 7 digits
August 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

The lower the score the better

The lower the score the better

Contingency and Consequen Management Planning for Year 2000 Conversion



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.

Y2K

☐ 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://y2kstate.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

Y2K

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

Y2K

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

24

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.

Y2K

☐ **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

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.

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

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.

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.
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 8 PM (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.

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

Y2K

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, P.O. 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

Y2K

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.

Y2K

<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

Mrs. BIGGERT. Right. And this is for State and local emergency managers so that they can see how—kind of judge how far along they are in their planning?

Mr. WALKER. Yes, ma'am.

Mrs. BIGGERT. Here we have issued report cards to the Federal agencies. Is there anything that you might plan to do that with the State and local governments?

Mr. WALKER. Congresswoman, there are 87,000 units of local government in this country. On top of that, there are another 200,000 water districts. That might be a little more difficult than 37 departments and agencies.

Mrs. BIGGERT. Probably so. But I think, though, that knowing that somebody is kind of looking to see the progress helps to move people along.

Mr. WALKER. Yes. And the State emergency management officials are doing just that. They're working hard to stay in touch with their local communities.

Mrs. BIGGERT. OK. Thank you very much.

Mr. WALKER. Thank you.

Mr. HORN. Let me add to that. The problem of small cities that you and I grew up in, small towns—and we're trying to get at this, and if the other body will help us with it, it will be done—and that is provide some incentive from the Federal Government in either loans or grants, or a combination thereof, to get their water facilities up to speed both environmentally and simply for the basic case of emergencies.

Does FEMA have any input when the administration is circulating legislation like that around the executive branch?

Mr. WALKER. EPA is a member of the Federal response plan and they're responsible, of course, for the sector under the Y2K Council. It will be more appropriate for EPA. They would be doing it for the Federal response plan.

Mr. HORN. Well, what I am thinking of—terrorism. I am thinking of what can be put in the water supply. It seems to me FEMA has a major role that they're not going to look at the environment. That's fine.

Mr. WALKER. Yes, sir. FEMA coordinates 27 Federal departments and agencies under the Federal response plan, including EPA, but EPA is the lead agency for all of that, that you just referred.

Mr. HORN. Including environmental terrorism?

Mr. WALKER. Yes. Yes, sir.

Mr. HORN. OK. Well, we will deal with them in my other hat too, which is being on the Subcommittee on Environment and Water Resources.

Mr. WALKER. Yes, sir.

Mr. HORN. OK. Let's see here. On current research and development efforts related to emergency management, are there any programs you have with universities or other State emergency groups that might well have done some things maybe the Federal Government hasn't done, and it is a good idea and maybe we ought to do it? How is that working?

Mr. WALKER. I would like to refer you to Kay Goss, our Associate Director for Preparedness. Her office has responsibility for just that work you described.

Ms. GOSS. We have a higher education project in which we're making an effort to get a degree program or at least a certification program in emergency management offered in every State. And I am very happy to report that we have all but 18 States involved in that right now. Also Director Witt has a fairly elaborate program through our Project Impact, working with institutions of higher ed and their research centers in making them disaster resistant, to protect the resources that they have such as libraries or their research centers.

Mr. HORN. Are there curricula developed, and perhaps FEMA has help for this, in emergency management where you have pulled together the best examples nationwide; or are there books that professors and, say, public administration have written on their own? What can you tell us about that?

Mr. GOSS. Higher ed institutions have done that, as well as our Emergency Management Institute in Emmitsburg, MD. And I am really glad you asked about best practices, because the Preparedness Directorate now for the 4th year has published a volume of exemplary practices in emergency management. Mostly they are low-cost or no-cost programs at the local level that can be replicated nationwide.

Mr. HORN. Is that printed through the Government Printing Office?

Mr. WALKER. Yes, it is.

Mr. HORN. So it is available to the public?

Mr. GOSS. Yes, it is.

Mr. HORN. Can it be downloaded from any computer system?

Mr. GOSS. Yes, it is on our website as well. Yes, sir.

Mr. HORN. So if they punch the right button, they can find all of your wisdom on emergency management?

Mr. GOSS. Yes, right.

Mr. HORN. Good, I think that's great.

Mr. GOSS. Thank you.

Mr. HORN. Well, that's all the questions I have. And we thank you and your team for coming up here. And we wish you well in these regional meetings.

Mr. WALKER. Mr. Chairman, thank you very much. If I might add something to Congresswoman Biggert, you point out very well that you know you can have a flood or a hurricane or an ice storm any day of the week. What we hope is that the American people take to heart that they need to be prepared for everything. They need to be prepared for that ice storm or whatever and to take care of their families on a daily basis. So thank you for mentioning that.

Thank you, Mr. Chairman.

Mr. HORN. All right. With that, we wish you well and we will call the next panel. Thank you for coming.

Mr. WALKER. Thank you.

Mr. HORN. Panel two has the Honorable Margaret Heckler, now attorney at law, former Secretary of the Department of Health and Human Services; Mr. Michael Humphrey, the business director for Telecommunications and Information of Public Technology, Inc.;

Dr. James Morentz, the president of Essential Technologies, Inc.; and Ms. Phyllis Mann, the president-elect, International Association of Emergency Managers.

Are there any assistants or anything that you might be calling on, because we will get them all. It is like the Pentagon. When they show up, there's usually a battalion. So I just want to get them all sworn in at once. So you're it, right? Lawrence Gerschel, and you're with the Lawrence and Alberta Gerschel Foundation. Why don't you just join Ms. Heckler there? If you will stand and raise your right hands.

[Witnesses sworn.]

Mr. HORN. The clerk will note that all five witnesses have affirmed that oath and we will begin with Ms. Heckler. We thank you for coming and sharing your ideas with us.

STATEMENTS OF MARGARET HECKLER, ATTORNEY AT LAW, FORMER SECRETARY, DEPARTMENT OF HEALTH AND HUMAN SERVICES; MICHAEL HUMPHREY, BUSINESS DIRECTOR FOR TELECOMMUNICATIONS AND INFORMATION, PUBLIC TECHNOLOGY, INC.; JAMES MORENTZ, PRESIDENT, ESSENTIAL TECHNOLOGIES, INC.; PHYLLIS MANN, PRESIDENT-ELECT, INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS; AND LAWRENCE GERSCHEL, LAWRENCE AND ALBERTA GERSHCEL FOUNDATION

Ms. HECKLER. Thank you so very much, Mr. Chairman and members of the committee. I have a sense of *deja vu* sitting here, because as a new member of the House of Representatives in 1967, under Chairman Jack Brooks, this was my first committee assignment. Many years have passed; hopefully some knowledge has been gained.

Mr. Chairman, I want to thank you so much for sponsoring this hearing, for holding this the hearing. I want to express my own appreciation to FEMA for the leadership that they are providing to the problems that we are dealing with today. And I am here today particularly because of my former service as Secretary of Health and Human Services, because I think that the millennium bug Y2K and its ramifications deserve special attention as this problem pertains to the question of health care in America.

The state of the medical institutions in terms of preparedness really, I think, mirrors the state of the public and private sector. Some institutions have completed their evaluations, and remediations and are in the final stages of testing. Others have elected to do nothing. The larger private institutions have, to a great extent, been able to drive their health care systems into some semblance of readiness, although the majority are behind schedule and overbudget.

In general, the level of readiness of the outlying facilities, especially the municipal and county hospitals, lags behind the larger private hospital groups and health care systems. The unique environment of medical facilities, coupled with the extraordinary variety of procedures, operations, administration hardware, all of this makes the problem in health care more complex than in other industries.

The problem is compounded by the fact that failure of these systems does not just involve an economic risk, but really a risk to life, to the welfare of the patients involved.

The repercussions of these problems will undoubtedly be litigated over the course of many years in the future. Yet the effect of the loss of a single loved one will be felt a lifetime. We are dealing with human life. And in a limited examination of human health care systems I have been involved with, some patterns have emerged which could assist other health care institutions in their efforts to resolve these problems.

It is quite clear that many of the larger, hospital-based health care systems have recognized the enormity of the challenge and have sought the very best available assistance and shared information among themselves. These institutions have established their own websites, have posted the results of their internal testing of the hardware of the various departments, and this sharing of information has gone on on an informal basis.

However, it should be recognized that searching the Internet for sites with information on any subject is not an easy task. It is very time-consuming, very arduous. The current search engine architecture is really based on data bases which report out on printed material, rather than on webpages. We feel very strongly and recommend to the committee that the committee ask the Congress to establish a super health care website.

The point of this is to create a repository of the results of the 500 best medical centers across the country, which could then serve as a resource, not only for medical centers of their size, but for all health care facilities. The administration of this site should be supervised by, for example, an NIH, FDA, another organization chosen by the secretary of Health and Human Services, but what we really need is the accurate and faithful transfer of information.

We recognize that this site must not assume any liabilities or make any guarantee, but it would serve as a focal point, one single focal point on the Internet easily accessible to all health care providers and patients. The maintenance of this, which might be the Y2K Medical Internet Library, should be undertaken by a world class Internet systems integrator and maintained on a constant and continuous basis.

This would allow all health care professionals the benefit of reviewing, with a high level of confidence, the work and the results carried out at many other institutions, and will avoid their having to painstakingly review each website looking for answers on even a specific piece of technology. It is clear that the formal collecting and posting of these results is designed to accelerate the process of driving the health care system into compliance, making it easier for the smaller providers and rural hospitals, community hospitals, those that have more difficulties.

And it will mitigate and reduce the costs of the whole system and of the process for everyone involved. It will have the advantage of making the rural, county, innercity, public-private health care providers share in all of the latest breakthroughs and information.

It is important to realize that while we are planning for success, that there will be some failures in the health care industry. And I think, just statistically, we can expect that. Some of these may

be foreseeable, but because of the enormity and complexity of the problem, it is imperative that an emergency planning process in health care be started immediately. Planning for future failures must occur, or we will have failed to plan because there will be inadequacies; which is not to suggest that we have become filled with anxiety and panic, but let us calmly look at the best practices and take action now.

The likelihood of system failures is increased because of the interconnectivity of the data flow. One health care facility did unknowingly cause another to fail by transmitting corrupted data. This data may cause the system and an institution to crash. Despite the fact that the data base and software is compliant. Such a situation could occur, for example, if a nursing home with limited resources would transmit corrupted data to a primary care institution, to the hospital taking care of the patient.

This data could cause the hospital system to freeze, or worse yet, lead to misinterpretation which could lead to an inappropriate treatment plan and with potentially fatal results.

Because we live in a complex, multifaceted environment, it is important that we consider the possibility that the current resources for health care may be additionally stressed by a number of natural disasters such as have been discussed this morning, or by failures in other industries such as the power industry; and if they fail to remediate their systems, it is important to realize that a substantial amount of health care services are rendered by county and municipal hospitals, for whom the problem of compliance not only is complicated by the lack of funds but, at this point, lack of time.

It is therefore very important that we develop a national plan for response to possible regional failures of the health care system. This plan should rely upon the expertise and capabilities of government's own systems and have available the military hospitals as well as the assistance of major medical centers, possibly the Veterans Administration Hospitals.

In terms of impact economically, there are two levels of concern. The first is the price of bringing health care into compliance in a given timeframe. And in the face of ever-increasing health care costs, there's no doubt that the costs of improving and correcting the year 2000 Y2K problem for health care will run into billions of dollars. It is estimated that the majority of health care product suppliers alone, not service suppliers, will spend on an average more than \$1½ million each to simply deal with the issues of compliance in their own companies.

This is money which in the aggregate represents \$2 billion and which will not be spent on new products, on new services. These costs do not take into consideration the costs of litigation, which is predictable and which has been estimated to add an additional \$4 billion for health care product suppliers alone.

Major health care systems in urban areas are finding that not only the problem has become complex as they try to become Y2K compliant, but that their initial budgets are woefully inadequate. One institution which had initially budgeted \$40 million has already spent \$46 million, and they have not finished testing half of their systems. The overall costs are probably going to be well beyond \$60 million for that one institution, and on and on it goes.

However, we must not only think of the direct costs, but we have to think of the indirect costs of health care, and the consequences. These costs represent the loss of income tax revenues as the effort of many individuals and companies are focused not on improving efficiency or developing better services, but merely the effort to maintain the services at the level they existed prior to January 2000.

It is with this in mind that we invite the committee to consider forming a special separate task force of technology experts with expertise in health care to evaluate and recommend potential actions which would lead to a more efficient process in that sector of the economy for the evaluation and the proposition of policies which could lead to an improvement in the way—in the compliance of the health care system under emergency conditions.

The problems before us are really of very serious scope. No administration has ever had to deal with this before, and it is really a virtual plague which has really been thrust upon us inadvertently. Nonetheless, it does threaten our society. Never has a society been so betrayed by its own efforts to create a better quality of life for all its citizens. Failure in the health care field will be measured in terms of human suffering and the suffering of friends, family, neighbors, your constituents across America.

We personally recognize the very extraordinary effort of this committee to address these issues and to address them in a timely manner. We understand that. We congratulate you, Mr. Chairman, and members of the committee. We are prepared to assist you and your best efforts with our best efforts and our thoughts in any way to resolve and avoid the difficulties inherent in not dealing with this problem.

We will all be standing tall when these questions have been faced and resolved, God willing. But I would like to say that we thank you for the opportunity of bringing us here today to speak to these issues and to address the concerns which you obviously have for the people of America.

Thank you.

[The prepared statement of Ms. Heckler follows:]

Testimony by

Ambassador Margaret M. Heckler

Before

**Government Management, Information,
and Technology subcommittee**

March 22, 1999

Honorable Chairman Horn and members of the Committee, after hearing the report of the gentleman from FEMA I wish to develop a couple of thoughts and draw your attention to the increasingly pressing problem of the "Millennium Bug - Y2K" and its ramifications to the well being of the country as it pertains to the delivery of health care to the general population.

The state of medical institutions in terms of preparedness unfortunately mirrors the state of the public and private sector. Some institutions have completed their evaluation and their remediations, and are currently in the final stages of testing, while others have elected to do nothing. The larger private institutions have to a great extent been able to drive their associated health care systems into some semblance of readiness, although the majority are well behind schedule and over budget. In general, the level of readiness of the outlying facilities especially the municipal and county hospitals lag far behind the larger private hospital groups and health care systems.

The unique environment of medical facilities - coupled with the extraordinary variety of procedures, operations, administration and hardware - makes this problem many times more complex than in most industries. The problem is compounded by the fact that failure of these systems does not simply pose an economic risk but threatens the very life and welfare of the patients involved. The repercussions of such problems will undoubtedly be litigated over the course of many years to come but worse yet the effect of the loss of loved ones will be felt for a lifetime. In a limited examination of the health care systems, certain patterns seemed to have emerged which could, if properly reviewed, assist other health care institutions in their efforts to confront and resolve these problems.

It is clear that many of the larger hospital-based health care systems have recognized the enormity of this challenge and have sought qualified assistance and have shared information among themselves. These institutions have, on their own, established web sites and have posted the results of their own internal testing and of the testing of the hardware of their various departments. This sharing of information has been done on an informal basis.

However, it should be recognized that searching the Internet for sites with this type of information is not an easy task. The current search engine

architecture is primarily based on databases, which essentially reports on printed material rather than web pages.

It is important to recognize that there already exists a multitude of excellent web sites -- both private and federal -- with an enormous amount of information, however what is lacking is a site where there is a critical evaluation and specific criteria for the posting of reports. A site that would protect both the quality and security of the information that is being disseminated. We must guard against those unscrupulous individuals or entities that might alter or falsify the results of the tests thereby dangerously misleading those who would rely on this information. The quality of the material must be evaluated. It is important to recognize that many suppliers are not in a position to completely evaluate their own material. It is not uncommon that during the production lifetime of a specific piece of equipment that the manufacturer may substitute one chip set for another and that although the current systems are compliant earlier production units despite their bearing the same model numbers are not compliant.

We therefore recommend that the Committee ask the Congress to establish a, "Super Health Care Web Site." The site to be the repository of the results of the top 500 Medical Centers and serve as a resource for all health care facilities. The administration of this site should be supervised by the NIH, FDA or similar organization. Thereby assuring the faithful transfer of information. We recognize that this site must not assume any liabilities or make any guarantees but rather serve as a focal point through the Internet, easily accessible to all health care providers and patients. The maintenance of this "Y2K - Medical Library," should be undertaken by a world class Internet systems integrator and maintained on a continuous basis. This would afford all health care professionals the benefit of reviewing with a high level of confidence, at one site the work being carried out at many institutions rather than having to painstakingly review each web site at each hospital one at a time. It is clear that the formal collecting and posting of these results is designed to accelerate the process of driving the health care system into compliance and mitigate the cost of the process. It will have the added advantage of making the information more easily accessible to rural, county, inner city, private or public health care providers.

It is important to realize that there will be some failures within the health care industry. Some of these failures will be foreseeable others may not. Because of the enormity and complexity of the problem it is imperative that

an emergency planning process be started immediately. We must have a contingency -- PLAN FOR HANDLING FAILURES -- OR -- WE WILL HAVE FAILED TO PLAN

The likelihood of system failures is increased because of the interconnectivity of data flow. Many hospitals have not established data protection services. One health care facility can unknowingly cause another to fail by transmitting corrupted data. This data may cause the system in an institution to crash despite the fact that its database and software is compliant. Such a situation could arise if for example a Nursing Home with limited resources would transmit corrupted data to a primary care institution. This data could easily cause the system to freeze or worse yet lead to a misinterpretation, which in turn could lead to an inappropriate treatment plan with potentially fatal results.

Because we live in a complex, multi-faceted environment, it is important that we consider the possibility that the current resources for health care may be additionally stressed by any of a number of natural disasters, or by failures in other industries, such as the power industry if they fail to remediate adequately their systems. It is especially important to recognize that a substantial amount of health care services are rendered by county and municipal hospitals for whom the problem of compliance is complicated not only by the lack of funds, but also by a lack of time. It is, therefore, urgent that we develop a national plan for response to the possible regional failures of the health care system. This plan should rely upon the expertise and capabilities of the government's own health care systems, such as the military hospitals, as well as perhaps the assistance of the major medical centers.

In terms of economic impact there are two levels of concern. The first is the price of bringing the health care system into compliance in the given time frame and in the face of ever increasing health care costs. There is no doubt that the cost of correcting the "Year Two Thousand - Y2K" problem for the health care system will run into the billions. It is estimated that the majority of health care product suppliers alone (not including service suppliers) will spend, on an average, more than one and one half million dollars (\$1,500,000.00) each to simply deal with the issues of compliance. This is money, which in the aggregate represents more than two billion dollars, and which will not be spent in the development of new products or services. These costs do not take into consideration the cost of litigation,

which has been estimated to be an additional four billion dollars for health care product suppliers alone.

Major health care systems in urban areas are finding that not only is the problem become more and more complex as they engage in the process of becoming "Y2K" compliant, but that the initial budgets are woefully inadequate. One institution, which had initially budgeted 40 million dollars, has already spent 46 million dollars and has only finished testing approximately half of its systems. The overall cost will probably be in the range of 60 million dollars. These are not isolated examples but rather they represent the findings of the majority of the larger institutions.

However, not only must we consider the direct cost of the resolution of this problem but we must also consider the indirect cost. These cost represent the loss of income and tax revenues as the effort of many individuals and companies are focused not on improving the efficiency and developing better services but rather the effort to maintain the services at the level that they existed prior to January of the year 2000. It is with this in mind that we invite the committee to consider forming a separate Special Task Force to evaluate and recommend potential actions which might lead to a more efficient process for the evaluation and proposition of policies which could lead to greater efficiencies.

The problems before us are of a magnitude and scope that no previous Administration has ever had to deal with. This virtual plague, which we inadvertently embedded into the bowels of our institutions, is poised to rise up like a Trojan Horse and destroy us from within. Never has a society been so betrayed by its own efforts to create a better quality of life for all of its citizens. Failure here will be measured in the form of human suffering: in the suffering of our friends, our neighbors, and your constituents. We personally recognize the extraordinary effort of this Committee to address these issues in a timely manor and respect the efforts that you have undertaken to face this Herculean task. We stand prepared to assist and commit to bring to bear our best efforts and our best thoughts to help in any way possible and in the end despite these difficulties we will all be standing tall - God willing.

In closing we would like to thank the Committee for the opportunity to address it, and we would like to entertain any questions that the Members of the Committee would care to address to us.

Mr. HORN. Well, we thank you very much for that thoughtful statement. We will write Mr. Koskinen this afternoon to suggest that idea. It is more appropriately done by the executive branch, and he has about 30, 35 working groups in a lot of these industrial areas.

When we were in Cleveland, we had a witness from the Cleveland Clinic Foundation who noted that we do, and I think you referred to it, have a website nationwide where all of the emergency equipment in hospitals throughout the Nation can plug into that, with the manufacturer of the piece of equipment, the actual design number, so that not everybody has to reinvent the wheel, once the manufacturer tells you what type of substitute microchip you can have and so forth.

So some of that, as you suggested in your own statements, is underway. But I think you're absolutely correct in terms of the great difficulty and the tremendous number of health care institutions and hospitals, and under different managements all over America, it is very difficult, especially in the smaller communities that you can see three members here come from originally, now that we live in urban America.

We will now proceed with the next witness. We will save the questioning for later once you are all done. And the next witness is Mr. Michael Humphrey, the business director for telecommunications and information, Public Technology, Inc.

Mr. HUMPHREY. Thank you, Mr. Chairman. Members of the committee, ladies and gentlemen, I would like to make a few brief comments, let you ask questions as you see appropriate.

Just for the record, PTI was created in 1971 as the technology arm of the National Association of Counties, the National League of Cities and the International City/County Management Association. So we represent really local governments and their technological needs across the country.

Mr. HORN. Was one of your offices at California State University Long Beach? There was a public technology group there.

Mr. HUMPHREY. No. We have competition out there.

One of the things that we discovered in last December was that a large number of local governments were not prepared for the year 2000 effort. We did a survey. We found something like 57 percent of all city managers in towns and cities over the size of 2,500 did not think the Y2K problem was an issue.

Because of that, our board of directors, which is composed of our sponsors I just mentioned, asked us to create a tool kit I am going to make available to you. It is a tool kit for really an awareness. This is a real serious problem, and it is a bit dated now, but I think you will find it useful. Also, most of that information is on our website, which is available.

I want to talk just briefly about what local governments do, and I don't need to tell you this, but I think it is important to understand that almost all emergency services are delivered through local governments. The public safety answering points in this country are run by local governments; not FEMA, not the States, but local governments. And if electricity or dial tones fail, those organizations, they will not know where to dispatch citizen help. They will not know where to send ambulances, police or fire. And so it

is extremely important to local governments to understand that the impact—potential impacts of Y2K are enormous and have grave, serious conflicts.

Also local governments don't do a lot of glamorous things. They collect the garbage and treat wastewater, but these are all vital, important pieces of the infrastructure that we know of. We believe we can turn on the tap and get a drink of water out of the hydrant without fear generally of any sort of bacteria. However, most of these services are highly interdependent with local private industry.

For instance, I mentioned electricity. Electricity is provided in about two-thirds of local governments by investor-owned utilities; privately owned, investor-owned utilities. Much of the water systems are initially treated and gathered and presented to the local entity. Insurance companies rely upon police reports to be available and most of these reports are done through the use of computers. So, there is a terrific interdependence upon local government.

The other point I wanted to make about that is local governments have the first obligation to respond to emergency situations. A friend of mine, Manny Garcia, in Miami-Dade was talking about the emergency management plan for the county and how they used it successfully with Andrew. When Andrew went through the south part of the county, they worked hard simply by pulling off the plan and executing the plan. They found things they had to redo and things that wouldn't work. But this is an important function of local government is to be prepared in case of problems either of their causing or of the organizations' in their communities causing.

So what is the likelihood? Everybody wants to know the same thing. I hear the speakers this morning talk about what is the likelihood. I don't know, and I do not care, and it doesn't really make any difference, and neither does it make any difference for local governments. They have to be prepared to respond to the situations that are presented to them. And if they do not, we fail. Not just them; we fail. And our society's most vulnerable citizens are at risk.

If it happens, "it" being some sort of Y2K event, I would argue that it is not going to be a localized event, it is going to be a widespread event. Take the issue of electricity. If we lose electricity in this country the way it is defined and created, the grid protects itself from shorts. It protects itself. It shuts itself down in case of disaster. The blackout in the Northeast many years ago was created by a \$3 switch, which we have replaced by an embedded chip. But the point being that this huge infrastructure has not done this. We have not gone through this. We have not had this kind of an issue. And the recent ice storms in Montgomery County and elsewhere illustrate an interesting point. We sent men with bucket trucks, heavy-duty guys that split high-voltage wire. We are going to need people who understand what an embedded chip is. That is not those guys in those bucket trucks.

Mr. HORN. I missed that last word. What was it?

Mr. HUMPHREY. Bucket trucks, cherrypickers. Sorry. That is the Oklahoma vernacular.

Mr. HORN. We have a lot of your citizens in California.

Mr. HUMPHREY. I want to read one thing here. If an average person bought a modest amount of food and bottled water and withdrew cash and obtained flashlights, it is probably a good thing. But what happens if everyone does those in the final days of 1999? What would happen if I told you a really serious thing was going to happen, and then I told you it was likely to start happening January 1, 2000? Finally, what if I told you I was not confident that our government and our private institutions were prepared to handle it? What do you think would happen? I think I know what would happen. I see predictions of snow in the Washington area, and I realize suddenly that the ability to get bread, milk and videos is gone at that point.

There are three things I would like to ask the committee. One was the chief administrative officer, Bruce Romer, for Montgomery County testified in front of the U.S. Senate Special Committee on the Year 2000 Technology Problem. I think you and Senator Bennett are the only two people doing things—I am only joking, but sometimes it seems that way. They proposed that the Federal Government help local entities develop regional capabilities.

They did a test, as you know, on December 21st of last year. They proposed doing one regionally for this year, and then replicate that in the remaining 9 months across the country. They project that costs will be \$7.3 million for the city or the regional areas and \$1.5 billion across the country, and these are pretty bare minimum numbers, but they take care of overtimes and that sort of thing.

The second thing I think important for the Federal Government, and I appreciate the position that Mr. Witt and FEMA are in in trying to deal with emergency problems, but the second real important issue is the Federal has assets that local governments could use, can help use. They are probably not going to be useful in a nationalized, mobilized way. They are probably going to be most useful locally. And in my prepared testimony I talk about the city of Albuquerque needing to get a commitment with the Army National Guard in case of no electricity so they can continue to provide electricity for their treatment plant, which is a very serious problem in Albuquerque.

The third thing is there is kind of a feeling, a rosy, feel-good feeling about this problem from the Federal Government. It is an “it can’t happen here” kind of syndrome, in my opinion. We don’t want to panic people; therefore, we are not going to tell them bad news. The people in industry call it “happy talk.” The Y2K people, some of which are here in this room, will talk about that as happy talk.

I think the American people are very smart and savvy people. I think if you tell them the truth—we don’t know, we don’t know how big a problem it is, we don’t know how big the risk is, we don’t know what the situation is for them—I think they will respond to that. They have historically, and I think that would be the third thing is to project a position that I don’t know, we don’t know what the problem is, but we are working hard to fix our own systems. We are working hard to develop emergency management responses in case there are problems, but we need your help and your community to help resolve these issues. We need the American Red Cross, the volunteers, we need people in each community to come

together to make that community a better place in case there are problems. That is the message. Thank you very much.

Mr. HORN. Well, we thank you for that helpful statement, and in the question period we will get into some of the underlying things that does it happen at who's leadership level.

[The prepared statement of Mr. Humphrey follows:]

TESTIMONY TO
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON
GOVERNMENT REFORM AND ITS SUBCOMMITTEE ON
GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

March 22, 1999
By Michael Humphrey
Business Director
Public Technology, Inc.

Mr. Chairman, distinguished members of the Committee, Ladies and Gentlemen, thank you for the opportunity to testify before this distinguished body and on this very important issue of Emergency Management and the Year 2000 issue.

I would like to take a moment and introduce Public Technology, Inc. PTI is a nonprofit organization dedicated to advancing the development and wise use of technology by city, county, and state governments. Founded in 1971, PTI is the technology organization of three respected national organizations: The National League of Cities (NLC), the National Association of Counties (NACo), and the International City/County Management Association (ICMA).

PTI's members are among the most technologically advanced and innovative local governments around the country. These cities and counties are living laboratories that assess needs, seek technology solutions, and use collaborative management techniques to achieve success in service to their communities.

Members have a direct impact on the final outcome of PTI's work, by their participation in PTI's technology task forces and in the Urban Consortium, a network of progressive cities and counties. Together with PTI's President Dr. Costis Toregas and the Board of Directors, members annually undertake an assessment of local government needs and define PTI's work program for the coming year.

PTI's five task forces focus on technology solutions in the areas of energy, environment, transportation, public safety, and telecommunications and information. I am the Director the latter task force and oversee those program areas. The membership serves in an advisory capacity while deriving value from peer exchange. The broad variety of projects offer something for everyone in local government: printed guidebooks and CD-ROMs, on-line listserves and bulletin boards, workshops and focus groups, pilot R&D projects, award programs, and transfer of technology solutions.

What has PTI done in Y2K?

PTI, with its sponsors, and under the direction of its President, Dr. Costis Toregas has launched the Y2K & YOU Campaign to make local appointed and elected officials aware of the impact of the Year 2000 problem. As part of the Y2K & YOU campaign, the Y2K & YOU tool kit, containing a comprehensive package of resource materials on the Year

Before the Subcommittee on Government Management, Information, and Technology

2000, including a video explaining the issue, was developed last year and is being made available to each of you. The Y2K & YOU tool kits were distributed free of charge to members of each of the campaign sponsoring organizations. To date, over 20,000 tool kits have been distributed. Please see our Y2K & YOU Internet page (<http://www.pti.nw.dc.us/y2k/index.html>) for current and additional information on this vital subject.

Members who need additional copies of the tool kit, or non-members who wish to purchase the tool kit may do so by calling PTI's Publications Center as 1-800-PTI-8976 or contacting the Publications Center via e-mail at pubs@pti.org.

Who is Michael Humphrey?

I am PTI's business director for telecommunications and information. I have worked with local and state government information technology departments for over 20 years at Tulsa County, OK; the Corporation Commission for Oklahoma; Prince George's County, MD and now Public Technology, Inc. As a business director for PTI, I staff the Urban Consortium Telecommunications and Information Task Force (UCTITF) composed of 50 of the largest most progressive local government information technology and/or telecommunications managers across the Country.

How will local governments be affected by Y2K?

To understand the impact of this technological challenge upon local government, one needs to understand what local governments are responsible for in this Country.

Many of the most important services, largely taken for granted by the citizen, are delivered or coordinated by local government. In virtually all jurisdictions, public safety is a function of local government. This includes staffing and managing the public safety answering points (PSAPs) - where all emergency services are dispatched. It includes secondary public safety activity too, such as record keeping which are vital to the insurance industry. It includes managing an ever increasing number of court records and criminal history information.

Most local government services include the delivery of water, the collection and treatment of sewage, as well as garbage collection. Local government services generally include traffic signal maintenance; and in some jurisdictions, other utility services such as the generation and distribution of electricity.

Many of these services are inter-dependent with private services, or functions. Some are collaborations of activities. For instance, most the telecommunication services in this country although primarily privately owned and operated, depend upon the use of rights-of-way owned and maintained by local governments.

All of these services are heavily dependent on automation applications. In most large cities the E-9-1-1 dispatching center is operated through an important marriage of

telecommunications, radios, and computers using software "glue" that holds it all together - software that often contains only a two digit century. Equally problematic is the fact that most of these services are very interdependent. For instance, if the record keeping functions of modern police agencies fail, then insurance companies can not get important reports. Without police reports on burglaries, for instance, many insurance companies will not pay homeowners claims. Virtually all aspects of local government operations are tightly coupled with non-governmental, private company activities.

This inter-dependence means that it is not enough for local governments to remedy their own applications, but local governments need to prepare for problems in other, non-governmental, organizations too. In that sense any serious disruptions from Y2K problems will dramatically affect local governments. For instance, the failure of dial tone in this Country would mean that no PSAP will be able to dispatch emergency services. Why? Because emergency officials will not know what citizens need those services nor would emergency officials know where those citizens live. Ultimately, regional electrical outages would have the same effect as batteries wane and electric generators run out of fuel. Or to put it another way, should any major supplier of electricity or local telecommunications services fail, for any significant period of time, local governments will be ineffective in allocating police, fire or ambulance resources.

Some of the surrounding Y2K issues are hidden and not intuitive. For instance, much has been written about the "embedded chip" issue. Most computer chips (those microprocessors that drive personal computers, telephone switches and VCR's) have something called a Real Time Clock. Few of these devices carry a four-digit century in a way that can be conveniently used. While it is obvious to most people that such devices can cause turn of the century problems if they are not, as we say "Y2K compliant". But what is not so obvious is that some timing devices (e.g. the device that will do some thing every so many seconds) also rely upon these Real Time Clocks. These devices repeatedly subtract the values of a Real Time Clock from a stored version of the Clock until the proper timing interval has occurred. The result? Prior to the turn of the century, they work fine. But after the turn of the century, that device will never do the next operation and will therefore fail even though it may not "care" about calendars or dates *per se*.

What is the likelihood of Y2K failures?

Unfortunately, my crystal ball, like everyone else's, is very cloudy. No one really knows. After all we have never done this before. But some really smart people are predicting real significant problems. Others see the same issues and are very optimistic. As Congressman, once again, you are being asked to make public policy without public proof. But the "proof" may be (we won't know until after the fact, will we) the lives of society's most vulnerable citizens. Which means "waiting to see" what will happen is not an option. As you will see, however, there is good news, since I argue that, ultimately, it makes little difference.

Before the Subcommittee on Government Management, Information, and Technology

I am fond of reading the article entitled "Millennium Tragedy in Urbanville: A Report Highlighting the Impact of the Year 2000 Crisis and Its Effect on Public Safety within Greater Urbanville" by Martyn Emery. This British work of fiction is in the form of a memo written in February of 2001.

What makes it so great, in my opinion, is the writer's perspective – from the other side of the Century. If nothing happens no one will care what you do, or how much was spent during remediation. But, on the other hand, should something occur, particularly if it is significant, everyone will ask what you did - did you do enough?

In the final analysis, I doubt if the public will be very forgiving. The public will expect civil order, public safety and the most basic human comforts. But how does a local government deliver services in the event of a significant disruption of utilities? For instance, who would provide warmth in Maine?

Preparation is the key

What local emergency managers strive to provide is a workable plan that will maintain a certain level of support. When hurricane Andrew roared through south Miami-Dade, the local emergency management team went to work, dusted off its hurricane plan, and began to execute it. As bad as that weather disaster was, it would have been worse if the County did not have a hurricane disaster plan. We must now concentrate on making sure that local government's emergency management team have a suitable contingency plan for a Y2K disruptions. The Boy Scout motto of "Be Prepared" still appears to be a fitting motto for local emergency management officials.

What is different about this potential crisis?

Unlike most natural disasters, should Y2K disruptions occur, everything will look normal. In fact there will be two obvious differences should this disaster happen: one, there will be no infrastructure damage; two, this will not be a localized problem (i.e. it will not be like the recent ice storm in Montgomery County Maryland).

In the event of Y2K problems, there will be no obvious infrastructure damage, no broken ice-covered tree limbs. Instead everything will look normal – except it won't work. What can be affected? No electricity or dial tone would be the worse scenario. Security systems, electrical voltage variations, elevators, timers of all sorts could be the second level of problem. Any controller that relies on an embedded chip is susceptible.

Since these outages do not involve obvious infrastructure problems, a different kind of repair is needed. Instead of tough, rugged people with bucket-trucks splicing 1200-volt lines, we would probably need people who are used to replacing circuit boards and computer chips.

Secondly, and perhaps the most problematic of potential Y2K failures, is the likelihood that any outages will be widespread. If one investor-owned electric utility has Y2K

problems then probably many utilities will experience similar difficulties. If security elevators begin to fail then that make and model can be expected to fail all over the Country. It only stands to reason that a buyer for any major industry will buy lots of one thing. For instance, if the requirement is for 100 switches, it is probable that an institutional buyer will find one switch that is the "best buy" and buy 100 of them. It is reasonable that buyers from around the country in various industries will be making a very similar analysis.

All of this suggests that large-scale outages or many outages could occur. Since we are looking for repair people with a particular and rare skill and since outages may well occur on a large-scale basis, then it appears two results are likely. One, it will take a longer than usual time to find the problems and replace them. Two it will take an additional length of time to find sufficient skills, since little "mutual aid" seems probable. In short, it seems reasonable that outages, due to Y2K problems, may occur over wider areas and be harder to fix.

Human nature

So what are individuals going to do? Already there are suggestions on the Internet that range from hoard lots of food and fuel (and be sure you have protection, too!) to sites which suggest one should prepare for a potential hurricane. Unfortunately almost all of this advice tends to cause individual action. Almost all of this advice tends to create anti-societal behavior.

If the average person bought a modest amount of non-perishable food and bottled water, withdrew a few dollars cash, and obtained flashlights, etc. today or tomorrow, it would be good advice. But what happens when (or if) everyone does those things in final days of 1999? The mention of snow in a weather forecast for Washington, DC means that bread, milk, and videos will suddenly disappear from the shelves. When I first moved here I was stunned to find out that people abandon their cars on the "beltway" during really heavy snowfalls. All of this is amusing as we think about it, but what would happen if I told you a really serious thing going to happen. Then I told you when it was likely to start happening - January 1, 2000. Finally what if I told you I was not confident that the government or private industry was prepared to handle it? How much credibility do we have? How much credibility do independent groups in society have?

Community Action is the key

After watching lots of approaches to this problem by well-meaning people, I have concluded that the only viable approach is to involve citizens of the community. We already expect the American Red Cross to be the primary provider of human care; i.e. warming centers for instance, should they be needed. This is a volunteer organization. What if Government, at all levels, encouraged community groups who are concerned about the Y2K problem to volunteer to these organizations in their own communities? What if Government generally advocated that these community groups should come to City and County halls to organize themselves in a massive attempt to make their

Before the Subcommittee on Government Management, Information, and Technology

community a better, more equipped community for any problems presented by the passage into the next millennium?

Elected officials would not have to take an official position about how bad conditions might get during a Y2K disruption. They could simply encourage community activists to help the government make their community a better place to live. Concerned citizens, left on their own, may well do things that will be anti-societal. For instance, reputable authors are suggesting that people stock up on food and water, migrate to less populated areas and "protect themselves". Other equally reputable groups are suggesting one should withdraw extra money from their bank account. These actions, if conducted now, by a few people in a community, are probably not harmful, but when masses of people begin to stock-pile food and water, withdraw money, and seek their own methods for protection, then the safety of the individual and the safety of the community is threatened. Collectively these actions become dangerous and anti-societal.

In fact there are many functions of a normal working community that government does not normally effect, nor should it. But many of the individual actions being proposed will cause other effects and understandably governments will be motivated to try to do something about it. The fact that the U.S. Treasury plans to print an additional \$50 Billion in currency is a recognition that the Y2K event may be composed of two kinds of events. The first will be the effects of large groups of people heading the advice of Y2K consultants.

Perhaps a three-step approach will benefit local governments the most

First, Montgomery County Maryland's Chief Administrative Officer, Bruce Romer, supported by the President of Public Technology, Inc., Dr. Costis Toregas, has testified before the U. S. Senate Special Committee on the Year 2000 Technology Problem that the Washington DC metropolitan area will need \$7.3 Million to conduct a regional readiness test. Proposing similar tests, Romer asked for \$1.5 Billion for local governments across this country. There is still time for local officials to revamp their local emergency management plans to cover possible outages caused by Y2K disruptions. And there is still time to test those plans much like the December 21st test of Montgomery County Maryland. And there is still time to mobilize the citizens into constructive groups. But local governments will need additional resources.

Secondly, if the Federal government, and thereby the State governments, would make it a policy to help local governments in combating any possible effects of this problem, a maximum benefit would be achieved. For instance, the City of Albuquerque, NM, because of its geographic location, will have significant sewage treatment problems in the event of a Y2K electrical power disruption. It is probably not practical for the City to purchase a backup generator just to power this plant. However, the Army National Guard has portable generators and could possibly provide a backup contingency for this possibility. But the Army National Guard does not feel it can guarantee those generators because there is a belief that the Guard would be Nationalized if such an event were to occur. If Federal agencies, and thereby State agencies, were instructed to help local

Before the Subcommittee on Government Management, Information, and Technology

governments plan for contingencies and given the authority to make firm contingency commitments it would solve some of the toughest decisions local officials have to make.

Finally, there is a perception given by many at the Federal level that everything is going to be fine. There will be no disruptions due to Y2K problems. We all certainly hope that rosy prediction is true. However, no one really knows. We have never done this before. We know there are devices that will malfunction - what we don't know is how many will malfunction and what the effect of those malfunctions will be. Is the falling dominos theory valid? Will outages on one area adversely affect other areas causing huge disruptions because we are so interdependent? The American people are a smart, savvy people. Isn't it better to tell the American public that we are working hard to alleviate all of the computer problems we know of but in the final analysis we don't really know what will happen?

For the first time that I can remember, all of the major local government associations - the National Association for Counties, the National League of Cities, and the International City/County Management Association, along with their technology arm, Public Technology, Inc., are all saying the same thing: "Be Prepared". These local government associations are saying the Y2K issue can be a real problem if it is untreated. Because of the "Y2K And You" campaign thousands of local governments are inventorying their applications and making adjustments to their contingency plans. We would suggest that government generally take a slightly different approach - an approach that says, "We don't know how bad it is likely to get, or if it will get bad at all. But your government is willing to work along side you, in your community, to stomp out the effects of the Y2K Bug!"

Thank you for the opportunity to address you today.

Sincerely,

Michael Humphrey
Business Director
Public Technology, Inc.

Mr. HORN. Dr. Morentz is next. Dr. James Morentz is president and chief executive officer of Essential Technologies, Inc. Welcome.

Mr. MORENTZ. Thank you very much. I am going to start out a little bit differently than the prepared comments because I bring 25 years of experience in applying technologies to emergency management. As a result I would like to take a minute or two to offer a historical perspective on technology and emergencies and then draw on the confluence that exists today between traditional emergency management and the Y2K issues. Finally I'll point out both a gap and an opportunity in government preparedness.

In 1975, when I finished my doctoral dissertation on managing a disaster in Africa and how communications technology affected that management, there was no emergency management field, and there certainly was nothing that would pass as a body of knowledge in technology applications to emergency management.

In the past 25 years a lot has changed. IBM created a computer hardware standard that really energized an entire industry. Microsoft created new universal software standards for operating systems that allowed software companies for the first time to write commercial software because there were sufficient people that we knew we would not go out of business.

FEMA was created and then recreated by James Lee Witt to provide professionalism and organization among emergency managers across the country. College programs grew, from George Washington University here in town, to the University of Wisconsin, to North Texas State University, all of which are now providing degree programs in emergency management.

On the technology side, Jack Dangermond of Environmental Systems Research Institute really created the entire field of geographic information systems, an incredibly important component of crisis decision support.

Satellite multispectral imagery arrived to help us understand the natural world around us far better than ever before, and the progression of communications has improved in ways that we only dreamed about. In the early days when amateur ham radio was the only form of wireless data transmission that existed, and even then with land line communications, modems limped along at 30 characters per second and really made the exchange of meaningful crisis management information impossible.

Today, the Iridium satellite system that is about to be launched replaces with 3-pound devices entire suitcases of electronics, making response to a crisis faster, better, and more informed.

And I would like to say out of my basement emerged the company that created the field of crisis management software that has now provided more than 10,000 systems to government and industry around the world that helped save lives, protect property, and preserve the environment.

All of this is by way of reflection on the improvements and the people who make up emergency management and the technology that supports them. This is especially important today as we move toward the year 2000 when the Y2K problem poses a risk that all crisis planning and response organizations in government and the private sector should be attending to with commitment.

To me, the most important thing that should be remembered about the Y2K risk is that it is really just the latest potential crisis. The consequences of Y2K failures are the same consequences we in the profession face every day. A utility outage can result from an ice storm as well as Y2K. Sewage treatment failures can result from floods as well as Y2K. Food shortages can result from hurricanes as well as Y2K. Disruption in the source of raw materials for manufacturing plants can result from earthquakes as well as Y2K. Failures in telephone systems can result from tornados as well as Y2K. And the shutdown of hospitals across an entire city can result from a terrorist releasing biological agents. Clearly the list could go on. But the emergency management profession has progressed significantly in our ability to handle crises just like the ones that may occur in Y2K in large part because of the broader uses of technology, the same root cause of Y2K, to improve the crisis management processes.

At the same time these improvements in emergency management have been incremental and achieved only with struggle. As a result I would like to suggest that the Y2K problem is an event of distinction because it presents both the problem and an opportunity. Y2K is a marvelous confluence of a real-world problem that is predictable in its timing, probabilistic in its effects, and manageable by an in-place infrastructure much in need of focus that Y2K provides.

The emergency management profession can bring much to bear on the management and the consequences of Y2K failures. The Congress and the administration need to provide that focus, first in government and then in the private sector, in order to maximize the ability of existing emergency management organizations to handle this problem.

Now this is not a difficult task. It is a matter of continuing the policy the government started to be prepared for Y2K by extending it to include a reinforcement of the information infrastructure for Y2K and, therefore, for all of emergency management.

Stated most directly, an in-place information system for managing crises has been evolving across the Federal, State and local governments in recent years. Y2K offers an opportunity to A, use, B, build on, and C, expand this system to provide a permanent resource for managing all hazards throughout the United States.

The initiative that should be undertaken is to use both existing and new crisis management centers, linked by software that has already become the de facto standard for Federal Government emergency planning and response. The combination of operations centers with an information management system will provide government with an exceptional quickly implemented Y2K contingency management capability that can easily support the Federal response plan that you heard discussed by folks from FEMA earlier.

At the present time there are a couple of Federal agencies, notably FEMA and the Coast Guard, that are beginning to look at the potential of what I am saying, the potential for creating rapidly stood-up crisis response centers focusing on Y2K, automating the emergency planning process, carrying out contingency plan tests in the coming months, deploying to every desktop across the Federal Government, and State and local governments an intelligence gathering tool that will help monitor the Y2K events as they unfold,

and then to successfully managing the Y2K contingency response to any incident across the country.

By providing a Y2K focus on crisis management, the effort expended in this particular problem will provide substantial benefits for overall crisis management to the Federal, State, and local governments for years to come in all types of natural, technological and terrorist weapons of mass destruction.

To conclude, I think it would be helpful if we could just take 1 additional minute to give you a glimpse of the technology that can help manage the Y2K consequence management that is currently in use in quite a few Federal agencies, and if this actually works—yes, there we go. What you are seeing up on the screen [slide 2] is the software that is in use in about 5,000 licensees across the Federal Government. About half of the approximately 30 major contingency management centers for Y2K that need to be set up are using this software.

Any contingency plan begins with the assessment of the potentially vulnerable infrastructure that is available in the system. Here [slide 3] you can see geographically shown the hospitals in the State of Washington vulnerable to Y2K failures. The product's next set of pages [slide 4] that focus on Y2K help to organize the contingency plan and operating procedures in a series of response scenarios, so in a sense we are, through the software, set to respond to a Y2K incident.

What you see now on the screen [slide 5] is an Internet browser-based Y2K alert that every morning we are going to recommend, beginning in July, the companies and agencies that have this software have each of their individuals who have a computer log in to the Y2K alert. Every day there will be a changing message about Y2K informing them about an organization's response or about government's response or about the larger issues of Y2K. This provides good, positive, constructive information to this network of people who are beginning to think about Y2K and how we can all get prepared to deal with it starting in July.

Then if something actually happens, there is a Y2K alert management system on the desktop of everybody in an organization, from the supply chain for making automobiles or to the Department of Energy here in the United States. And I maintain the first indication of Y2K failure will come from an administrative assistant's desk where they see the first indication of something odd happening, or at the plant floor, where the difficulty occurs. That gets entered, [slide 6] and that information then gets immediately transmitted back to a command center that focuses on Y2K in two respects: identification to see whether this, in fact, is a problem, and then what do we do about the consequences associated with that problem [slide 7].

In the software that exists now, that gets translated into an operations log [slide 8] that then instantly gets translated into a contingency plan by the software [slide 9] that allows people to begin to respond to the emergency [slide 10].

Thus we are drawing together using the very technologies that present us the Y2K problem, forcing them to be our solution to Y2K. All of this is available and ready to go with a tremendous

number of licensees in the Federal, State, and local governments needing now simply a focus.

I thank you for your attention.

Mr. HORN. We thank you for that very helpful statement. I am sure we will have a lot of questions about it when we get to the Q&A.

[The prepared statement of Mr. Morentz follows:]

Improving Federal Y2K Contingency Management with a Permanent All-Hazard Information System

*Testimony by James W. Morentz, Ph.D.
Essential Technologies, Inc.*

Executive Summary

As the Federal Government moves forward with its plans for Y2K Contingency Management, an important principle needs to be kept in mind:

Y2K is one crisis among many that Federal Departments and Agencies have been preparing for and responding to for many years. Contingency planning for Y2K embodies the same fundamental elements as contingency planning for every other type of hazard including utility failures, hurricanes, terrorist events, or hazardous materials spills. As a result, it is important to Y2K success to recognize that an in-place information system for managing crises has been evolving across the Federal government in recent years. Y2K offers an opportunity to (a) use, (b) build on, and (c) expand this system to provide a *permanent* resource for managing all hazards throughout the United States.

This paper summarizes the currently evolving crisis information management system and goes on to describe a way in which Federal government Y2K Contingency Management can benefit from this system by speeding the implementation of a government-wide Y2K planning, monitoring, and response operation. This operation includes both existing and new crisis centers linked by a software product that is the de facto standard for Federal emergency planning and response. The combination of operations centers and an information management system will provide the government with an exceptional, quickly implemented Y2K contingency management capability that can easily support the Federal Response Plan. Moreover, after the focus on Y2K is over, the effort will have immeasurably strengthened the Federal government's crisis management capabilities for all types of natural, technological, and terrorist weapons of mass destruction events.

The Existing Contingency Management System

Across the Federal government, through no systematic plan but rather through good individual decision-making, a crisis information management system network has been evolving over the past decade. At the present time, a single software product has been used -- at various times and with various levels of success and commitment -- to plan for and respond to all types of disasters throughout the Federal government. The present, in-place licenses for that single software product include:

- FEMA's National Emergency Management Information System (1,800 licenses)
- U.S. Army Reserve Component Automation System (4,500 licenses)
- U.S. Air Force (more than 300 licenses)
- U.S. Navy (more than 50 licenses)
- Army and Air National Guard Readiness Centers have licenses
- Department of Transportation licenses for the DOT HQ Transportation Emergency Center
- U.S. Coast Guard (one district and one license for CG HQ)
- The Department of Energy has licenses for more than 10 DOE facilities
- EPA has an inactive license
- NASA HQ has a license, as do 12 NASA facilities
- One Bureau of Reclamation district office has a license
- More than half of all Corps of Engineers district offices have licenses
- FBI (30 licenses in its Strategic Information Operations Center)
- The White House Situation Room (one unused license)
- General Services Administration (one license)
- The District of Columbia Office of Emergency Preparedness (five licenses)
- Every county in the States of Maryland and Pennsylvania have licenses
- More than 30 State Emergency Management Offices have licenses
- Every State Army and Air National Guard has licenses
- HQ U.S. First & Fifth Armies (more than 75 licenses)
- Tennessee Valley Authority (12 licenses)
- FEMA's Emergency Management Institute (14 licenses)
- National Institutes of Health (three licenses)
- VA Medical Center (one license)

Many of these licenses were purchased for a specific disaster and fell into disuse because of lack of commitment on the part of the agency. Other licenses are in daily use for mission critical operations and reporting.

The software does exactly what Federal government Y2K contingency management needs to do to accomplish its goal of assuring the continuity of operations of the Federal government. The software helps government personnel on many levels assess risks, write contingency plans, exercise those plans, monitor Y2K events, and manage an effective response of people and resources to manage the consequences of those events. It does this in both a planning mode and in real-time response. It has been proven in the field and used in major command centers and on mobile response units by Federal agencies to support their Emergency Support Functions during the activation of the Federal Response Plan. It is used as both a standalone, single-purpose tool and as a nationwide operations management system.

For Federal government Y2K contingency management, the opportunity exists to use the software to rapidly stand up crisis response centers, to automate the

planning process, to carry out contingency plan tests in the coming months, to deploy to every desktop in the Federal government an intelligence-gathering tool that will help monitor Y2K events as they unfold, and to successfully manage the response to any Y2K incident. All of this can be done in part by using the existing commercial-off-the-shelf software product that is already used in many locations throughout the Federal, as well as state and local, government. By providing a Y2K focus on crisis management, the effort expended on this particular crisis will provide substantial benefits to the overall crisis management capability of the Federal government for years to come.

Information Management for Y2K Contingency Management

With the right information system, government officials can effectively address five separate functions in Y2K Contingency Management. Those functions are Y2K Risk Assessment, Contingency Planning, Contingency Exercises, Y2K Failure Monitoring and Alert, and Response Management. Each of these major functional areas in Y2K Contingency Management is highlighted below.

Y2K Risk Assessment

As with other potential disasters, the Y2K threat analysis begins with the identification of risks of failure and their potential impact on the operation of the organization. More specifically, organizations must maintain:

- An inventory of software and hardware used for mission-critical processes which include:
 - Information and Communications
 - Electrical Power Systems
 - Gas and Oil Transportation and Storage
 - Heating, Air Conditioning, and Personal Utilities
 - Finance, Administration, Human Resources
 - Transportation
 - Water Supply Systems and Sanitation Systems
 - Safety, Security, and Emergency Services
- An inventory of all other important processes in which software and Y2K fixes present a risk.
- Risk profiles of processes and systems, including failure probabilities and the effects of failures.
- An inventory of personnel who will be available for technical "fix on failure" deployment.
- Lists of additional, off-payroll personnel on call (consultants).
- Lists of suppliers who are tied into the "supply chain" and whose own failures put an organization or process at risk.
- An assessment of suppliers' compliance with Y2K remediation and contingency plans.
- An on-demand, real-time briefing capability for CEO/Board of Directors.

Y2K Contingency Planning

Y2K consequence management extends across different levels of people in various departments who must be involved in developing Y2K contingency plans. An information system must encourage a structured planning process that allows for periodic tests of the plan to assure readiness and further plan development. The resulting Standard Operating Procedures (SOP) become automated checklists for use both during an exercise to test the effectiveness of the planning process and during a real Y2K event.

Y2K planners must build, store, retrieve and display:

- The "triggering events" that identify a specific failed system based on reported symptom(s)
- The steps or procedures to implement when systems do fail.
- Dynamic Standard Operating Procedures that guide a response to a Y2K consequence management effort
- The identification of initial contacts for systems failures.
- The identification of "fix-on-failure" teams for potential deployment.
- "Switch-over" alternatives for failed systems.
- Triage - which systems to fix first -- which are mission critical to the continuity of the organization.
- A supplier/vendor inventory of failures.
- Plan development through exercises.

Y2K Contingency Training and Exercises

The Y2K Contingency Planning software can be used to simulate failures in systems and the consequences of those failures. The actual system can then help staff work through the resolution of those failures for the purpose of testing and improving the plans that have been written.

- Training programs evolve from the Contingency Plans, providing educational material for all potential participants in a Y2K response
- Individual and group training is supplemented by table top exercises using simulations derived from the plans and incorporated into software for delivery
- Simulations test the success of training, plans and Standard Operating Procedures.
- Results of simulation exercises are used to improve training materials and the planning process.
- An automated training and exercising system allows for participation of remote sites through electronic delivery of simulations.
- Encourages the review of lessons-learned and for effective follow-up actions.

Y2K Failure Monitoring and Alert

Effective use of information technology allows every desktop in an organization or across related organizations, to be turned into an intelligence-gathering station. Most important, Y2K Monitoring begins in 1999 with an internal employee-relations program to provide information about the organization's Y2K plans and what every employee can do, both at work and at home, to minimize negative consequences of Y2K.

- A Y2K monitoring system turns every desktop into intelligence-gathering station
- Every desktop, everyday begins to get the Y2K preparedness message out to every employee
- Employees become attuned to potential Y2K idiosyncrasies and will become better able to distinguish problems from impending catastrophes
- Y2K reports are forwarded instantly to a Y2K command center that will interpret the possible consequences of the event and, if required, post the notification to the organization's incident log for subsequent response tracking
- With an Internet-based Y2K monitoring system, the same early-alert capability can be extended to suppliers by enforcing their use of the system to identify unfolding problems

Y2K Response Management

A Y2K information management system allows widely distributed incident managers to track the deployment of resources, teams of experts, and other response capabilities according to plan to resolve any incidents arising from a Y2K failure. With an information system, users will be able to:

- Keep a journal of all events and early signals of failures (from extended e-mail monitoring).
- Manage kit deployment of teams - personnel, software, analysis devices, other hardware for "Fix-on-Failure" response teams.
- Track and "journal" all feed-in systems from vendors and other facilities throughout the supply chain.
- Capitalize upon a real-time briefing capability for managers up to the CEO and Board of Directors
- Provide critical statements to the press on the organization's capacity for response and recovery.

Using EIS™ Software for Y2K Contingency Management

A *de facto* standard has been established across the Federal government for crisis management software. The software, developed by Essential Technologies, Inc. (Rockville, MD) was designed to manage information for all types of incidents and can be used throughout the major phases of Y2K contingency management, including the pre-incident phases of assessment,

planning and exercising and the trans-incident phases of monitoring and response.

In the pre-incident phases, Essential's EIS/GEM product can be used by people in various departments to develop Y2K contingency plans and test those plans. This is the way to get started. The software encourages a structured planning process that fully incorporates periodic tests of the plan to assure further plan development. The resulting SOPs become automated checklists during an exercise to test the effectiveness of the planning process and results. Then as agencies complete their Y2K contingency plans, they can be easily imported into the EIS software.

Once a plan is produced, EIS/GEM is the repository for the results of the planning process (specifically SOPs) and is used on a real-time basis for tracking Y2K incidents. EIS/GEM can be used in its Local Area Network configuration or, in its client/server configuration (with Oracle or SQL Server relational databases), it can be "extended" to work throughout an entire enterprise.

At the same time that a plan is created, the organization's ability to monitor Y2K incidents as they unfold is implemented with another Essential Technologies product called Y2K Alert. This Java-based Internet/Intranet software will be accessible from every desktop in the organization. Thus, Y2K Contingency Management can begin with virtually every employee who becomes a "monitor" of the possible Y2K threat. This software can be put in use months before the date change for the purpose of fostering among employees an awareness of Y2K and how to deal with any consequences. Each day, employees can log on to Y2K Alert and receive a new message briefing them on Y2K preparedness by the organization and by individuals. By incorporating daily awareness of Y2K into the business process, employees can be turned from the "uninformed" into the "understanding advocate" of responsible Y2K planning.

The combination of the pre-incident use of EIS/GEM software for Y2K risk assessment, contingency planning, and exercises and the trans-incident use of Y2K Alert on every desktop to monitor Y2K failures provides crisis and business managers with an enterprise-wide Y2K contingency planning capability that is useful in governments and corporations of all sizes.

Plus, the added benefit for every organization is that in 2001 and beyond the Y2K crisis management system remains not only useful, but even more important, can be used for everyday incident management in the organization. Whether preparing for emergency medical response to workplace accidents or the evacuation of a building following a fire or earthquake, or the evacuation of an entire complex or town in the face of a hurricane or hazardous materials spill, the same software system that proved successful in the high-profile Y2K effort will be there in the future to support those who face crises and emergencies on a daily basis.

A Proven Solution for Y2K Hazards

The range of hazards being predicted as a result of Y2K is almost endless. Among those dangers cited most often are power failures, transportation accidents, industrial mishaps, and civil disorder - all resulting from the failure of our automated information infrastructure.

Virtually all of these potential disasters are ones that have been managed successfully - time after time, by different organizations in different parts of the world -- using the EIS family of software. Since 1985, emergency professionals have relied on Essential's family of crisis management systems to prepare, respond and recover from countless incidents - large and small, short-term and long-term, from minor local incidents to full-scale national disasters. A few examples are provided below. (For more, see the web site [<http://technews.essentech.com/>](http://technews.essentech.com/))

Power Failure Forces Sheltering, Water Support

EIS users in Arizona experienced back-to-back severe thunderstorms in the summer of 1996 that caused major power failures that left thousands of people without power (including much-needed air conditioning and telephone service) for days. Maricopa County's emergency officials used their EIS software to help the American Red Cross and local utility companies locate emergency generators for water well pumps and dry ice suppliers. They also used EIS to locate and open shelters (especially for the elderly) and monitor storm damage throughout the County.

Officials Monitor Response and Recovery Efforts following Northridge Quake

Government officials in California used EIS to communicate electronically with each other and with FEMA officials during the 1994 response to the Northridge earthquake. California officials sent FEMA data and maps that provided valuable information for situation analysis and damage assessments, which sped up the Federal government's response to the major crisis. Government personnel stationed at the Pasadena Disaster Field Office (DFO), the then U.S. Sixth Army EOC at the Presidio (now the Fifth Army based in Texas), the California National Guard EOC and the National Guard Bureau in Washington D.C. shared valuable information using EIS. Examples of that information include: a description of transportation lines impacted by the quake, the locations of National Guard tent sites, U.S. Army Corps of Engineers water distribution sites, American Red Cross shelter sites, and lists and descriptions of plants and facilities (including power plants) in the estimated damage area.

Tracking Road Conditions on the Internet

After seeing how Virginia's Department of Emergency Services (VDES) successfully used EIS to manage emergencies, officials at the Virginia Department of Transportation (VDOT) decided to use the software to manage transportation information. Today, EIS software is the foundation

for the State's Virginia Operational Information System (VOIS), which is used by VDOT personnel to monitor and track road conditions, traffic incidents and construction projects statewide. However, VOIS is also easily accessible to personnel in other State agencies and the Governor's office so that information can be easily shared any time of day or night. In addition, portions of VOIS have been posted on the Internet to assist the general public. For example, in the winter of 1997, VDOT used VOIS to post real-time road conditions on regional maps of the state during a severe winter storm. Internet users who visited the site were able to choose from a menu of regional maps which provided a color-coded view of current road conditions. (To look at this site, click on:

<http://www.vdot.state.va.us/roads/eoc.html>.)

Nuclear/Fire Incident plus Airplane Crash

Many EIS users have relied heavily on the software in situations where they found themselves managing several incidents simultaneously. For example, in February 1993, as hundreds of Pennsylvania emergency personnel participated in a regularly scheduled nuclear power plant exercise, a seven-alarm fire broke out in a pesticides facility, which caused the evacuation of 1,000 residents. Also on the same day, a commercial freight plane crashed near Scott Air Force Base. Because officials in the Pennsylvania Emergency Management Agency (PEMA) Emergency Operations Center had automated their emergency information on EIS, they were able to effectively monitor the three events simultaneously and could fully support local emergency managers by locating and dispatching personnel and resources as needed. In addition to the three incidents, PEMA officials were also hosting a contingent of senior government officials from China, who had requested permission from the U.S. State Department to observe the exercise.

Conclusion

In 1981, I testified before a Subcommittee of the House Committee on Science and Technology chaired by Albert Gore, Jr. I concluded by testimony with the admonition:

Unless a consistent policy and program for using information technology in emergency management is developed, three years from now emergency programs in the localities in this country will not be as well managed as a local barbershop or as a local butcher shop. Inexpensive computers will have made such an impact on small business that even the smallest will have more knowledge and more analytical power at their fingertips than the office that is charged with protecting the entire jurisdiction from catastrophe and leading the community survival from a nuclear attack.

In the 1989 book, *Strategies and Systems for Disaster Survival*, I noted that I was "half right." While no "consistent policy and program" was created, the computer revolution had come to emergency management.

Now, a decade later, I am still half right. The Y2K threat demonstrates that individual organization implementation of technology to improve crisis and contingency management is still the primary means of decision-making. Consistent policies and programs -- for something as abundantly clear as Y2K -- still find leadership only with great difficulty. Failing such leadership, and the development of a Federal Government, if not National, direction, the management of the consequences of Y2K failures has to be questioned. I hate to think that, despite all of the technology at our fingertips, it still will take individual heroic efforts to create the contingency management infrastructure to ease into the Year 2000 with the likely disruptions overcome without turning them into a disaster.

To those who have been managing crises for decades, Y2K is just another hazard. Like other hazards, with Y2K they will rely on their proven plans and policies, which are backed by an array of technological tools, including EIS™ software. The licenses exist for this software in many Federal agencies, in the majority of State emergency operations centers, and in hundreds of local emergency management offices across the U.S. With this foundation of proven technology already in place, officials should continue to depend upon, and build upon, what exists to maximize Y2K contingency management.


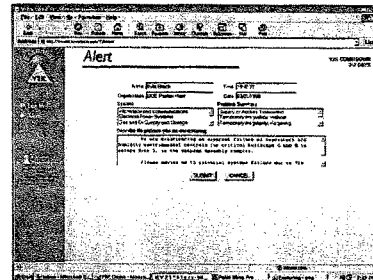
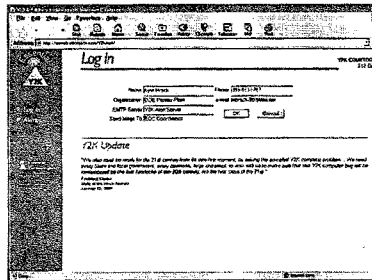
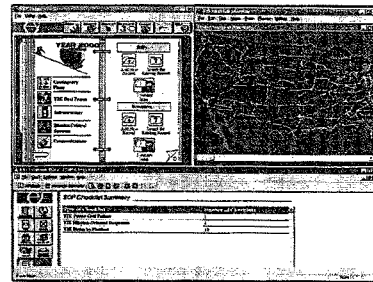
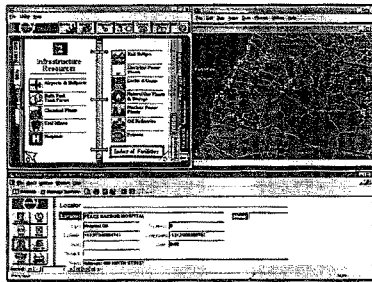
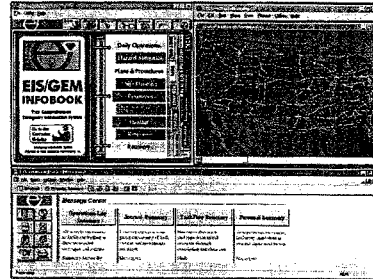
**Improving Federal Y2K Contingency Management
with a Permanent All-Hazard Information System**

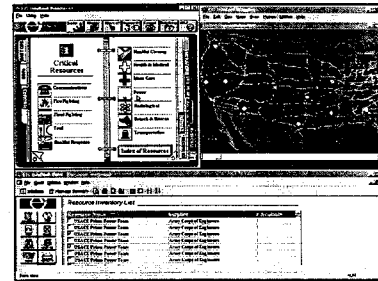
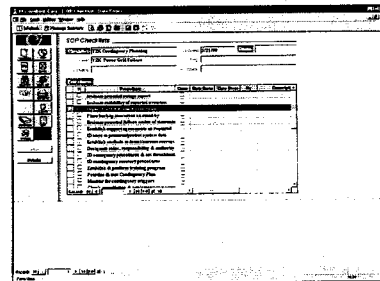
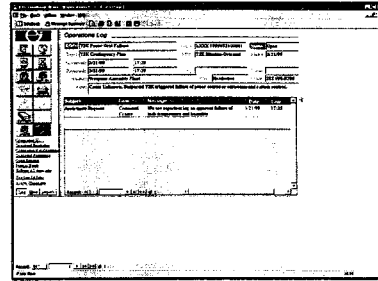
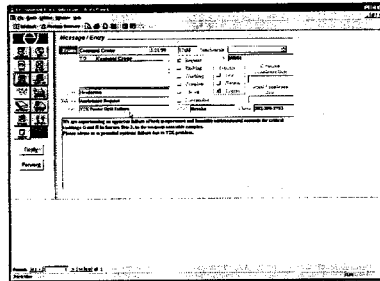
EIS/GEM Software from Essential Technologies, Inc.

Testimony before the Emergency Management Hearing & Workshop
Sponsored by the Subcommittee on Government Management, Information, and Technology
of the Committee on Government Reform
U.S. House of Representatives

March 22, 1999

James W. Morentz, Ph.D.
CEO
Essential Technologies, Inc.
Website: www.essentialtech.com
800-999-5009



Mr. HORN. We now have our last panel witness Mrs. Phyllis Mann, the president-elect of the International Association of Emergency Managers. You might wish to tell us a little bit about the organization and then go on to your very helpful ideas.

Ms. MANN. Thank you. The International Association of Emergency Managers represents 1,700 emergency managers both with local, State, Federal, military systems and across the world, not just in the United States. We are aggressively seeking emergency managers both through Italy, Australia, England and many other countries. Everyone cleaves to our organization because we are the one organization that will accept any and all emergency managers for their face value what they do at the local level.

In emergency management—and, Chairman Horn, I will take you at your word today, we are going to have a family discussion here today. I am sorry Mr. Turner walked out because Mr. Turner is absolutely wrong. He should have been preparing his daddy with that generator, especially if his daddy lives in Texas. In Texas you never know what is going to happen, be it the boll weevil that is coming your way, or the storms that they have experienced, or the floods. So the very least I would do if my dad lived in Texas is not only buy him the generator, which I am sure Mr. Turner could afford to do, but I would teach my dad how to turn it on.

And that is what is going on in the United States today. Same with you, Mrs. Biggert, is that here we—you are in Illinois. I would assume today in the back of your vehicle that transported you here to this meeting that you have an emergency kit in your car, and at the very least in your office you have comfortable shoes to wear just in case when we walk outside that door day that the wonderful weather that we are having turned to rain and then snow, and we had to slide along the city sidewalks.

This is what we are seeing in our level of government. We are—and I am sorry I don't consider myself the lowest form of government. I always considered myself the highest form of government. You all are here to serve me.

Mr. HORN. Let me hasten to say it was none of the Members of Congress that made that statement.

Ms. MANN. I understand that. I truly understand that. But I did. I always looked at Federal Government as the agency that serves me as the local government. Here we go. This is our problem at the local level, and I made sure that in coming here today I articulated this to your staff because I can mince no words with this. I don't need another tool kit. I am tired of tool kits. I am tired of contingency plans. It is the local level in government that has all hazard planning. I am ready for any hazard that is hitting my community. We have plans. And, in fact, I was kind of chuckling to myself assuming that you all have found all these chips. Well, I have some doubt. I really have some doubt that you found them all. And so this is what we are doing at most local levels.

I can tell you exactly where most emergency managers that are professionals will be on New Years Eve. We will be in our emergency operations centers just in case. We will have stood up our emergency operations centers somewhere between December 27th and 29th. At that point, some of them are very sophisticated, like I am sure Ellis Stanley has in Los Angeles. It is a designated room

with computers and generators and satellite radios. And obviously I am a “wanna be,” I would like all of that, but I live in Kitsap County, WA. I am a 1-hour ferry ride away from Seattle. We are a peninsula. I know exactly what is going to happen during the Y2K transition in my community because it happens all the time when we have power outages. Whenever there is bad weather in the Northwest, peninsulas like mine do without. We do without power. We have experienced this frequently, and there is not one area of the United States who hasn’t done without power.

A good example of power disruption just because somebody punched into the line was in San Francisco just, what, a couple of months ago. Do you know that the only operating facility in downtown San Francisco was Nordstrom’s? Now, for those of who you don’t know what Nordstrom’s is, it is a very sophisticated upscale shopping store. They were also not only able to check you out using manual systems, but their generator came on, and they could still make you a latte. There were very few—

Mr. HORN. I sorry; I couldn’t hear that.

Ms. MANN. A latte, cappuccino. But that is what we are talking about when we are talking about any hazard that affects the public.

Somebody here keeps talking about panic. I am sorry, we do anecdotal research. I have yet to see the scientific data on this, but here it goes. I have been an emergency manager since 1991 paid by local government. I have, prior to that, been a volunteer with the American Red Cross, which I still am as a disaster volunteer and instructor. Would somebody please tell me where in the United States we panic when we have an emergency? I have yet to see panic. I have seen hungry people, I have seen people standing in line for their water, but I have yet to see people panic after a natural disaster. Y2K is the preparedness for the winter storm. If you are ready for the storm, you will be ready for Y2K. Why are we so afraid to tell the public let’s get ready?

One of the things that consistently is happening throughout the United States is this inconsistent message, and we heard it today. And our friends at FEMA are our partners in preparedness, but they had an opportunity today to say let’s get ready just in case, but in between that sentence were 10 other sentences that discounted the fact that we just don’t know if we are going to be ready.

So here it goes. If we told the American public today, let’s get ready just in case, and let’s just swag it, let’s just use a good old standard 7 days in a natural disaster. We ask you to get ready independently for 3 days on your own, and that is because the 3 days is not for the citizen, it is for me. It is for me, the local government, to reconstitute myself. So if Y2K is going to be widespread, it is going to be intermittent disruptions throughout the communities, then the very least we should do is tell our citizens let’s get ready for 7 days, and if you start buying your groceries today, and bought 1 extra day of food, that is all I am asking for your family. If you did this once a month, you will have 7 days of food by October. So then you would not have to worry if the video shop and the little “Handy Andy” was not open. You would have it there in your house.

By all means you should have flashlights, for goodness sakes. We have power outages throughout the United States. You have should medicine. I am sorry for Mr. Turner. I do not recommend a 90-day supply either, but I think that every American who is on critical medication should always have 30 days of medication on hand at any given time. So what is the difference? This is what I ask my citizens and especially my seniors: "Why don't you have 30 days' worth of medicine on hand?" And the answer is the insurance carriers will not allow it. They will not fund it. So we have a golden opportunity this year to say, all right, insurance carriers, let's get them ready. Let's get this 30 days' worth of medicine. What is wrong with 7 days' worth of food?

And last but not least, I will tell you this: This is what I am doing about my financial records. In October, I am taking all of my 401(k)'s—they are not numerous—I am taking my 401(k), my IRA, I am make taking my mortgage, although they could drop that one at any given time, I am taking any critical record I have from October November, and I am moving them to my safety deposit box in the bank because it happens to be a fireproof area. If I get deleted during the transition to Y2K—and you and I both know you can get deleted any time, it is only a computer—then I am going to be able to reconstitute my life.

In Kitsap County, WA, we are going to do the same service for our senior citizens. If they get deleted, if anything happens, we have trained caseworkers that will help our seniors reconstitute their life. We don't want them to panic, but they will if we do not give them straight information.

So I will tell you this, Chairman Horn, if Washington, DC, cannot tell the American people how to prepare, then the International Association of Emergency Managers is about to. We are about to tell you how to get ready for 7 days. We are go to join our partners in preparedness with the Red Cross and lead you down the path, and what we think you should do here in Washington, DC, is join us.

I will not—I repeat, I will not get on an airplane December 31st. I am paid to have common sense. I might just wait a couple of extra days just in case, and I think that that is what we all should be paying attention to: Just in case, let's get ready. Thank you.

[The prepared statement of Ms. Mann follows:]



TESTIMONY
before the
HOUSE GOVERNMENT REFORM COMMITTEE
GOVERNMENT MANAGEMENT, INFORMATION & TECHNOLOGY SUBCOMMITTEE
March 22, 1999

on behalf of
THE INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS (IAEM)

by

Phyllis A. Mann, CEM
Kitsap County (Washington) Department of Emergency Management
President-Elect
International Association of Emergency Managers (IAEM)

International Association of Emergency Managers
111 Park Place
Falls Church, Virginia 22046-4513
phone: 703-538-1795 • fax: 703-241-5603 • e-mail: iaem@aol.com • Web: <http://www.iaem.com>

Chairman Horn and members of the subcommittee:

Thank you for inviting the International Association of Emergency Managers to speak with you today about how local emergency managers are preparing for the challenges of Y2K, and what we perceive as our greatest needs at the local level.

My name is Phyllis Mann, and I am the emergency management coordinator for Kitsap County in Washington State. As the current President-Elect of IAEM I will have the honor of representing our association starting in November of this year, into and through the transition to the year 2000.

The International Association of Emergency Managers is a 1,700-member organization which represents the interests of emergency management professionals in local, state and federal governments, the military, private business and the non-profit sector, both in the U.S. and in other countries, including Canada, the United Kingdom, Italy, Australia and others. On a daily basis, our members help their communities or their organizations plan for, respond to and recover from a wide variety of emergencies — hurricanes, winter storms, floods, fires, droughts, earthquakes, chemical spills, transportation accidents, infrastructure breakdowns and others. Lately we've added terrorist activities, cyber-terrorism and, of course, Y2K.

The Preparedness Message

At our IAEM mid-year meeting just over a week ago, we spent more than a morning struggling toward a consensus position on Y2K from the emergency management perspective. The basic premise we agreed upon was this:

The transition to the year 2000 will pose no unique or additional *impacts* beyond what we already are subject to from other hazards. We already use comprehensive, all-hazards emergency plans to guide our preparedness activities, our public information outreach, and our response and recovery activities. So if we analyze the possibilities of Y2K-related disruptions and add to our plans any

different twists to the impacts, we can prepare for Y2K just as we would prepare for another type of storm.

To cite an example that should hit close to home in the Washington metropolitan area, many of our communities prepare for ice storms. Loss of power and downed phone lines are likely results in serious ice storms, as many of you know on a personal level. Power loss in some cases leads to lack of water service. Ice storms and major snowstorms also can lead to delayed shipments of goods to grocery stores, pharmacies and local businesses. These are the kinds of possible effects that emergency plans are designed to address, and they are among the potential effects of Y2K-caused disruptions. We address them for storms; we can address them for Y2K. And we are doing our best to do that.

In IAEM, the consensus about what we should be telling our communities is to prepare for a possible storm — including its after-effects — lasting about seven days. We are looking for a consistent, nationwide message to that effect. If our citizens receive consistent advice, they are less likely to get confused and panicky, wondering why different people are telling them different things.

If some localities offer differing advice, they should explain the circumstances that make them say that. In my own community, for example, we're suggesting a somewhat longer period of self-sufficiency, because we're a peninsula in Puget Sound that typically finds itself at "the end of line" for service delivery, and somewhat isolated in an emergency. Hurricane experiences in some Florida communities have shown that a severe storm can cause disruptions of service for up to two weeks; some of them are suggesting a two-week period — but this is consistent with the kinds of preparations they would encourage for the hazards they face during any year.

Y2K Differences

With Y2K, we know the "storm" is coming, and we know *when* it's coming. But there *are* several factors which make Y2K somewhat different:

- (1) There are many unknowns, and probably will be up to the last minute;
- (2) The effects are likely to be spread across many communities, even if they are not of massive proportions in any one place; and
- (3) There is so much advance warning that those first two factors mean the public has plenty of time to let concern about the unknown grow into worry, if not panic.

Those differences translate into special challenges for emergency managers.

Information. Our foremost challenge is to plan appropriately in the face of the enormous uncertainty surrounding Y2K. Our massive dependence on computers, the ubiquity of microchip-operated equipment, and the national and international interdependence of the networks and systems we rely on for delivery of goods and services make "fixing" the Y2K technical problem a daunting task. And despite heroic efforts in many quarters, the problems will *not* be fixed everywhere in time. We know there will be problems; it's very difficult to provide a reliable forecast of what and where they will be, or exactly what the effects will be. So we have to make assumptions NOW — while there's still time for us as governments and for our citizens to prepare in an orderly way — about how comprehensive our preparedness needs to be.

At the local level, we are looking for two kinds of credible information that we feel we don't have right now:

(a) *Credible threat scenarios.* We know that the President's Council on Y2K as well as your subcommittee and the Senate's special committee have been releasing assessments of progress in various sectors. Our difficulty is that a national overview is of limited value to us as we plan locally. Whether 90% of the electric utilities in the country are positive that they will experience no Y2K-related disruptions is of less interest to me than whether the remaining 10% are all in Washington State. We need at least some regional assessments. And we need reliable information, delivered to us from a credible source, with updated "weather forecasts," if you will, concerning the

severity and location of the impending Y2K "storm."

Many of us are good managers, but "technologically challenged." We need solid answers in terms we can understand, to questions such as: how is the power grid connected, and is there a real threat of "cascading failure"? What does that mean? How does it work? If there's a problem, where will it be felt?

Some of the reports that are released also seem to be deliberately given a rosy hue to avoid causing undue alarm. Of course, we don't want to arouse alarm unnecessarily. On the other hand, if there is cause for concern — and there certainly are alarmists out there saying there is — we need to know, so people can prepare themselves gradually in an orderly way. If we want to tell citizens to have emergency supplies of food on hand for a few days or a week, we have to tell them now, so they can buy a few cans each week ... not in December so everyone is trying to make massive purchases all at once.

(b) *Credible information on what is being planned at the federal level.* We hear various reports, word-of-mouth, about what national leaders are saying about their plans for responding to any disruptions that do occur. Are states or the National Guard Bureau making plans to have Guard units ready? Are medical teams being pre-positioned? To plan adequately at the local level, we need to have this information directly, from a source we know and trust. If state emergency management offices are told, they can get the word out directly to local communities ... without the need for an announcement that goes to the world-at-large.

We have a real concern about such federal-level plans, however. Many of these human resources that are called upon in the federal response plan for disasters are vital assets in the local community. Because of the potential for disruption in any community, we certainly don't want our own resources called up to help someone else, if they are needed at home. And we won't know that in advance.

Widespread effects

Even though we don't expect a total collapse of our infrastructure or simultaneous devastating effects, it is possible for Y2K-induced effects — power outages, transportation problems,

communications disruptions, etc. — to strike numerous communities across the country at the same time.

What this means to us at the local level is that Y2K will call for a different level of planning, because we may not be able to call upon our neighboring communities for mutual aid. They may be busy responding to the same kinds of problems we are. So we recommend emphasizing self-reliance even more than usual. This is one reason why we suggest one week's worth of emergency supplies, where normally we would ask citizens to be prepared to be on their own for three days (72 hours).

The long lead time

The length of time this Y2K threat is before us has two faces: we have more time to prepare because we know when this threat will materialize, if at all; but there also is more time for the public's fear of the unknown to make our citizens prey to scare tactics, hype and misinformation. Usually, disasters occur too fast to allow concern to build to dangerous levels.

But in the case of Y2K, there is a vast publicity machine out there (including the Internet) being fed by alarmists. In the face of that, we simply must be honest with the public about what we know and what we don't know. Blanket assurances, up against the alarmist rhetoric, will only arouse more suspicion. Many of us at the local level are trying to provide detailed and honest information, and to urge citizens, despite what we don't know, to prepare as they would — or as we have told them repeatedly over the years that the *should* — for a storm. We are concerned that the federal government is not taking the appropriate leadership role to issue a national message.

What we are doing and recommending

Our policy statement. Our complete IAEM policy statement is attached with this testimony, but essentially we urge communities to prepare for Y2K as they would for a storm, with added emphasis on self-reliance. We recommend that preparations include:

* Performing a risk analysis that covers food, utilities, energy, protective services, transportation, health care, communications, information dissemination, government, education and the economy;

and evaluates the need to activate an Emergency Operations Center for the transitional hours.

* Revising the community plan for any contingencies revealed by the risk analysis. We suggest the model released recently by FEMA as a good guidance tool.

* Conducting an aggressive public outreach campaign. Many voices need to proclaim the same message: prepare for Y2K as if it were another type of storm. Use standard preparedness advice from the American Red Cross and from FEMA's Community Family Preparedness program. It also has to include detailed facts about how the community as a whole is preparing for Y2K — the status of remediation efforts, business continuity planning, and emergency preparedness and response plans.

In addition, IAEM recommends that FEMA serve as the warning and notification point for dissemination of accurate information of any genuine infrastructure problems during the transition. IAEM recommends that FEMA and state emergency management offices provide technical assistance, training and funding to local jurisdictions for the transition. IAEM also has prepared some "helpful hints" for emergency managers for educating their communities; these have been checked for consistency with messages being issued by the Red Cross, FEMA, the banking community and others.

Our survey. Individually, in our local communities, IAEM members, like other local government departments, are making technical assessments and taking remedial action to make sure computer systems operate through the changeover to the year 2000. Unfortunately, we can't report that everyone is ready ... that is why we developed our statement to urge our colleagues in emergency management and other parts of local government to take the "storm" approach to Y2K.

An IAEM on-line survey of emergency managers has drawn 240 responses to date. Following are a few highlights from the results:

- 229 are aware of the potential problem;
- 219 report their organizations are actively working to ensure their systems will be able to handle the Y2K problem;
- 84 report the computer systems in their organizations are fully prepared (some of these responded

as early as last November);

- On a scale of 0-100%, participants judged the compliance and operational readiness of their communities' emergency management program, communications, equipment, warning systems, 911 and related systems to be an average of 55% compliant;
- The degree of cooperation among local community agencies averaged 60%;
- The degree of interaction between state and local emergency management organizations on Y2K issues is scored at an average of only 54%, on a scale of 0-100%;
- Participants judge the operational readiness of local jurisdictions to be 52% (on the 0-100% scale);
- On the same scale, participants rated the availability of guidance, information and assistance at 51%.

Besides these steps, local actions include:

Media campaigns; brochures on readiness; local cable channel programs; town meetings; hotlines where citizens can call to check on progress of Y2K compliance for the city or county, utilities and local business and industry; and coordinating drills and exercises to test contingency plans for continuity of operations and response to emergencies. In a show-of-hands poll at our recent IAEM mid-year meeting, most members present were planning to staff their Emergency Operations Center over the New Year's weekend ... just as a precaution. That should not be taken as a negative signal — emergency planners and managers are paid to imagine the worst and prepare for it. We do that, so our citizens can have confidence of knowing that someone is taking the watch.

In short, we are preparing for Y2K as we prepare for a storm, with added consideration of the three factors listed above that give the Y2K "storm" its own character. How long the storm will last no one can predict. In some parts of the country the storm may pass by unnoticed. In other areas it may cause disruption in essential services, power, fuel or food. We know that the storm is brewing, and landfall is expected on or around December 31, 1999. We hope the storm will pass, but we cannot predict the outcome.

So, as with other hazards, we are: making plans so that essential services will continue despite any

disruptions; coordinating plans and exercises with other departments in our jurisdictions as well as providers of electric, communications and health services; and urging our citizens to prepare to be self-sufficient if necessary for a number of days.

We have been delivering that message for years — perhaps Y2K is a golden opportunity to catch everyone's attention at once, so the whole nation can focus together on reasonable, orderly preparation for any type of emergency. The Boy Scouts have been saying it for years, too: BE PREPARED! If Y2K passes without a hitch, we will all have gained something: we will at least have our emergency preparedness kits ready for the next winter storm.

**INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS
POSITION PAPER
Regarding Year 2000**

The International Association of Emergency Managers feels the transition to Year 2000 will pose no unique or additional impacts beyond what we already are subject to from other natural hazards. Due to the potential widespread nature of this event, however, we actively encourage self-reliance in our citizens and governments.

IAEM recommends preparing for the transition into the year 2000 by doing the following:

1. Perform a risk analysis.
 - a) The analysis should, at a minimum, review food, utilities (electric, natural gas, water and sewer), energy (fuel), protective services (Police, Fire, EMS, Emergency Management), transportation, health care, communications, information dissemination, government, education, economy.
 - b) Each local jurisdiction should include examination of the necessity to activate an Emergency Operations Center for the transition. In addition, it would be helpful to preplan personnel issues for critical departments for the transition.
2. Review comprehensive emergency management plans.

Revise the community plan for the contingencies in response to the Year 2000 risk assessment as necessary. A good example of this can be found in the Federal Emergency Management Agency's "Contingency and Consequence Management Planning for year 2000 Conversion" plan at <http://www.fema.gov/y2k>

3. Put in place an aggressive public outreach campaign. IAEM recommends local emergency managers help their citizens prepare for the event as for other events such as a storm. A storm could pass by or could disrupt critical functions. In preparing for a storm, you will be ready for any natural hazard that could affect your community.
 - a) Each jurisdiction should develop and expose the public to consistent messages. It's best when these messages are coordinated with nearby communities so our citizens don't hear conflicting information. All our many voices should say the same thing. As with any natural hazard, your best resources are your neighbors.
 - b) IAEM recommends NEMA, NaCO, NLC, NGA join us in the single message of adopting the philosophies of the FEMA/ ARC Community Family Preparedness Program.

IAEM recommends that FEMA serve as the warning and notification point for dissemination of accurate information of any genuine Y2K related infrastructure problems during the transition.

IAEM recommends that FEMA and state emergency management offices provide technical assistance, training and funding to local jurisdictions for the transition.

IAEM recommends we all be ready, just in case!

Food and Water: IAEM recommends using the guidance of seven days preparation as a nationwide consistent message. People should store foods that their families like to eat on a daily basis. Canned and dry goods work great in storms. Remember, if the power goes out, eat your refrigerated items first. Each family member needs up to one gallon of water per day.

Medical Information/Prescriptions: In emergency planning the biggest concern is personal health and safety. Individuals may need daily medication. Plan to have extra on hand for at least 30 days, just in case!

Bills, Banking & Payments: Make copies of car, rent/mortgage, credit card payments, bank statements, IRAs and other important financial and payment records. For questions about automatic payments, check with the bank.

Cash: IAEM recommends keeping money in checking or savings accounts. Remember pens and paper have no computer chips - checks work!

Fuel: Keep vehicle gas tanks filled.

YOUR NEIGHBORS! Neighbors can be the best resource people have during emergencies. Plan with neighbors now, to help each other during the storm.

Let's be ready, just in case!

Bulletin

INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS

INSIDE SPECIAL FOCUS ISSUE

Y2K
FEMA's role
Where are we?
IAEM survey
OMB report
County survey
ERRI survey
Y2K session from
IAEM conference

Inoculating Ourselves Against the Y2K "Bug": A special-focus edition of the Bulletin

"While we remain hopeful that continuing progress on Y2K remediation in all critical sectors will prevent any major failures, we nonetheless believe it is imperative that government organizations at every level begin to formulate plans now to respond to the various types of disruptions that could occur as a result of the Y2K problem."

— Letter from Senators Bennett and Dodd, U.S. Senate Special Committee on the Year 2000 Technology Problem, October 26, 1998

What Are We Talking About?

The Year 2000 — or Y2K — confronts us with "the millennium bug." This bug stems from the fact that computers and software, including microprocessors that govern many other products, have been programmed with two digits to indicate the year (98, 99).

When the year 2000 rolls around, these systems may recognize "double zero" (00) as 1900 instead of 2000. Symptoms: equipment stops running or generates erroneous data.

There is a technical "cure," but it takes huge amounts of time and people-power, both of which are running short.

So, as the Senators (above) and others suggest, the focus must shift to contingency planning.

That is the theme of this special Bulletin. Who is doing what? Where can you turn for guidance? What are the likely scenarios you should plan for? What should you tell the public about becoming prepared?

This is only the beginning ...

Frankenstein, Dracula & Y2K: Just Another Scary Monster

by Michael Martinet, Area Coordinator, Los Angeles County, California

Y2K is scaring a lot of people, people almost like you and me. People who use technology, but don't really understand it. People who never thought about their reliance on technology — until now.

One thing that I have learned over the years (or have I just intellectually reinforced a prejudice?) is that the more things change, the more they remain the same. People want their leaders to reassure them that all is well. Even if all is not quite well. "Make us feel good about ourselves and our lives. That is why you are our leaders."

A few days ago, I received a phone call from a senior citizen in the community. She wanted to know what the "city" was doing to prepare for Y2K. She also wanted to know how she should prepare for Y2K. She asked my advice. Some of her friends were buying land in the Sierra Nevada

(continued on page 5)

FEMA's Role: Preparedness, Response, Emergency Services

by Kay C. Goss, CEM, FEMA Associate Director for Preparedness, Training, and Exercises

Disruption of computer-based systems as a result of the "millennium bug" during the transition to the year 2000 poses a potentially serious risk to the continuity of operations of government agencies, public utilities, and businesses, and the well-being of individuals. The importance of planning for possible computer disruptions and preparing to deal with their consequences cannot be emphasized strongly enough.

Every organization and every individual, in public and private life, has an obligation to learn more, take preventive steps, and prepare to deal with the consequences of problems that cannot be prevented.

Three-Part Role

The Federal Emergency Management Agency (FEMA) is actively supporting the efforts of the President's Council on Year 2000 (Y2K) Conversion to address Y2K-induced computer failures and consequences. Our role covers three distinct but interrelated areas: Emergency Services, Responses to Emergencies, and Preparedness and Contingency Planning.

It is important to note that FEMA has no authority or capability to prevent computer disruptions, beyond its own agency, or to respond to the causes of computer disruptions. Like other federal agencies, a major priority of FEMA's is to ensure that its own computer-based systems are Y2K compliant, and to report its progress periodically to the President's Council on Year 2000 Conversion through the Office of Management and Budget.

Emergency Services Sector

Through the President's Council, FEMA chairs the Y2K Emer-

gency Services Sector (ESS) Working Group. The ESS Working Group is reaching out to organizations that work with federal agencies in emergency response, to increase their awareness and encourage them to assess their readiness to operate normally leading up to, during, and after January 1, 2000.

FEMA also heads the Catastrophic Disaster Response Group under the auspices of the Federal Response Plan (FRP). This group

Association of Emergency Managers (IAEM). Both groups are assisting FEMA in identifying the needs of and preparing pertinent emergency preparedness guidance for state and local emergency management organizations. NEMA has convened a special committee with several state representatives to work with FEMA to address Y2K preparedness and contingency planning issues, and IAEM has voluntarily surveyed more than 700 local

FEMA will prepare contingency planning and preparedness guidance, exercise support, and training assistance over the next several months...

is developing a special supplement to the FRP to deal with the consequences of potential Y2K failures. FEMA will ensure that all FRP agencies maintain readiness for responding to all types of hazards and conducting recovery operations in accordance with their FRP responsibilities. As the lead agency for the FRP, FEMA is striving to ensure that FRP agencies work with their partners in the state and local communities, to promote awareness and undertake contingency planning.

Preparedness and Planning

In the emergency preparedness and contingency planning area, FEMA has implemented an outreach program to the emergency management and fire services communities to heighten their awareness of and sensitivity to Y2K issues and to help increase their preparedness levels.

To facilitate this outreach, close coordination has been established with two of FEMA's key constituency groups, the National Emergency Management Association (NEMA) and the International

jurisdictions on Y2K compliance and preparedness. The efforts of both organizations in addressing the Y2K issue are sincerely appreciated by FEMA.

State Assessments

This fall, FEMA's regional directors contacted all the state emergency management directors, asking them to assess their level of Y2K compliance and preparedness for dealing with the consequences of Y2K failures. This assessment addressed the potential impacts of Y2K failures on state and local governments, the status of state and local efforts to fix Y2K problems, funding for Y2K fixes, overall readiness at the state and local level, Y2K contingency planning, guidance that is needed, and the likely impacts of Y2K problems in 2000.

Voluntary assessments were completed by more than 90% of the states. They indicated that most state level agencies have resolved or are planning to resolve the vast number of Y2K-related

(continued on page 4)

New Certified Emergency Managers (CEMs) Approved November 7, 1998

Robert J. Andrews
Clark Co. Ofc. Of Emerg. Mgmt.
Las Vegas, NV

Robert C. Bohlmann
York County EMA, Alfred, ME

David J. Cary
Deschutes Co. Sheriff's Ofc.
Bend, OR

John Bland Ellen
City of Conroe, Conroe, TX

Janet L. Gibbons
Davis County Schools
Farmington, UT

Michel S. Pawlowski
FEMA, Washington, DC

Regina Phelps
Health Plus, San Francisco, CA

Tyler Smith
Metro Dade Co. Fire Rescue Dept.
Miami, FL

CEM's Recertified

Edward B. Abel Jr.
Kathryn Gerk Aguirre
Paul E. Bragg
Michael L. Brock
C.R. Brown
Carl Carlos
Neill M. Clement
Bernard Cook
Nancy H. Crowley
Donald G. Elrod
Gary A. Fried
Herbert Gehring
Donald B. Gould
Walter G. Green III
Lyn Gross
Don Hudgins
Daniel Joseph Inman
Robert W. Kinsman
Jerome Mansfield
Scott W. Meyer



Eunice Mommens
James W. Pitchford
George Souderes Jr.
Barbara G. Taylor
Barry Valentine
Christine A. Van Horn
Mary Ann Winters
Donald G. Wiseman
W.R. Zwierschke

Lifetime
Alan Breazeale

Emergency managers who earned their certification during 1998 and were present for the IAEM annual conference in Norfolk in November joined their colleagues at the awards banquet and accepted a toast in their honor.

FREE Software to Help You Cope with Terrorism & Weapons of Mass Destruction

Call Now to Get Your Choice of Two New Products — FREE! — When You Purchase
EIS/GEM, The World's Finest Software for Comprehensive Emergency Management

Domestic terrorism is a top priority for crisis managers and security professionals all across our nation and perhaps no aspect is more serious than the nuclear, biological, chemical (NBC) threat. EIS/GEM InfoBook™ — easy-to-use software that combines data, maps, models, and communications — is the recognized standard for all-hazard emergency planning and response throughout government, industry, and the military. Now, we are introducing two complementary products to help you train, exercise, and respond more quickly and effectively should the "unthinkable" occur:

- The EIS/GEM Security SuperTab is an important supplement to EIS/GEM designed to provide precisely the information you need for vulnerability assessments and SOPs, as well as step-by-step response guides for all kinds of security breaches — including bomb threats, kidnapping and hostage-taking, civil disturbances, workplace violence, and the movement/security of critical individuals.
- NBC Warning! is state-of-the-art plotting and reporting software. It generates a plume model that accurately predicts the impact of nuclear, biological, or chemical agents (sarin, anthrax, nerve gas, etc.) and displays that plume footprint on your maps.

To qualify for this special offer you must be an IAEM member and call us no later than January 31, 1999. You'll receive your free software whenever you buy EIS/GEM. That's all there is to it!



Call 800-999-5009 or 301-284-3000 Today!

Essential Technologies, Inc. • 1401 Rockville Pike, Suite 500 • Rockville, MD 20852 • Website: www.essentech.com

GEMADIAEM2

Y2K: FEMA's Role (continued from page 2)

issues involving critical emergency preparedness facilities, systems, and services. A significant number of states are making good progress, and report that their mission critical systems will be compliant by the middle of 1999.

All states have formed Y2K planning committees, have an office that is designated with primary responsibility for coordinating Y2K activities, and have established Internet Web sites on Y2K. No states responding to the assessment indicated that they would not be in compliance by January 1, 2000.

Information from the states about Y2K compliance in local jurisdictions was sketchier, but many of the states have already embarked on or plan aggressive outreach programs with their local jurisdictions — including meetings, conferences, workshops, individual visits, personal telephone calls, training, exercises, public announcements, etc. Some states did report that there are local jurisdictions now compliant or working hard to close the gap.

States' Concerns

State assessments identified several areas of concern. The issue cited most often was the limited or nonexistent funding, and limited availability of technical resources and staffing to assess, test, and validate systems and fixes. Many states complained that the excessive number of surveys they are being asked to respond to on Y2K is hindering their ability to work on the problem.

The states fully recognize the diminishing time available to become Y2K compliant and the urgent need to correct associated problems, but only limited contingency planning has been completed. Some states requested that a central clearinghouse of information for addressing Y2K

problems be established and that guidance on contingency planning be developed.

Other recommendations included using FEMA's Emergency Education Network (EENET) broadcasts to disseminate information, sharing best practices, and exchanging information from the different sectors reporting to the President's Council on Year 2000 Conversion.

What to Expect from FEMA

As part of the preparedness outreach to state and local governments, FEMA will prepare contingency planning and preparedness guidance, exercise support, and training assistance over the next several months to assist state and local jurisdictions in addressing many of their concerns. This assistance will take several forms:

- guidance on Y2K contingency planning and preparedness, to include such things as tool kits, checklists and job aids;
- a clearinghouse that can be used to exchange Y2K information;
- publications to share exemplary Y2K practices;
- national and regional-level seminars and exercises conducted during the winter and spring to focus on the consequences of Y2K failures;
- Y2K exercise packages and seminar information for state and local organizations to use in meeting their own needs;
- training to prepare state and local officials, business, and industry for managing Y2K failures; and
- broadcasts through the Emergency Education Network of programs for emergency managers on the implications of Y2K.

Some very progressive Y2K programs have already been developed and are available from

both public and private sector organizations describing the Y2K issue and providing information on making systems compliant, testing, identifying corrective measures, and contingency planning.

Most of these materials describe computer system problems and where they are likely to be encountered; how to address the problems in software and operating systems; the importance of working with vendors and others to identify and correct problems; the criticality of testing to confirm compliance and when to upgrade systems; the importance of completing contingency planning and developing work-around solutions before the conversion in 2000; and the importance of not panicking and at the same time not becoming over-confident.

Critical Connections

It is now more important than ever for organizations in the public and private sectors to review their activities and identify those that are dependent upon systems that could be impacted by Y2K problems or by systems to which they are connected. This will help identify operational vulnerabilities and simplify the process of preparing backup plans and procedures.

Contingency plans need to address the loss of critical and lifeline services and infrastructure (power, telecommunications, water, etc.) so that the ability to function and to serve and protect the public will not be compromised. If there should be system failures, backup plans and procedures that have been developed in advance and thoroughly tested will help ensure a semblance of normalcy and a smooth transition into the year 2000. Each day brings us closer to the new millennium. By being prepared individually, organizationally, and as a society, we will be able to weather this storm together.

Scary Monster (continued from page 1)

mountains for their "Armageddon" get-away. They were also cashing out of banks, buying gold, and burying it. All this as a hedge against the chaos they believe will follow Y2K. She wanted to know if she should do the same.

Some professional acquaintances of mine own an emergency supply business near downtown Los Angeles. They report a 20% increase in business, and their sales of water barrels have doubled this year. Based upon their conversations with their customers, this increase is entirely due to Y2K. One of their customers told them he had just purchased a shotgun and 5,000 rounds of ammunition.

What's going on here? Are we professional disaster planners out of the information loop? (I guess it wouldn't be the first time.) No, I

think this is mostly a crisis of confidence. A crisis of confidence in our own ability as a nation, and as a people. In fact, this crisis of confidence over Y2K may be a far larger problem than "real" Y2K events themselves. Let's hope so anyway. But if the bark is worse than the bite, we still have to deal with those who are intimidated by this scary digital dog.

A hundred years ago, one of the functions of older people was to be the repository of knowledge. After all, it took a lifetime to acquire the knowledge to be held in esteem as truly knowledgeable in the ways of the world. Today, however, in 20 minutes on the Internet, I can know more than my father, grandfather and great grandfather combined. Today the elders of our technotribes are 16 to 20 year old kids who have mastered computer technol-

ogy. But, they have the bones of knowledge without the meat of experience.

So where does that leave us as a profession? We have to stretch. We have to do some new things that we haven't had to do before. Most often disasters happen so fast that people don't have time to worry and get real scared.

But Y2K is different. People have the time to work themselves up into a real frenzy. Tick, Tick, Tick. Worry, worry, worry, panic. Our biggest job may be to instill confidence in our employees, co-workers, and citizens. This isn't something we have had to do before a disaster in the past.

Tick, Tick, Tick, Tick. The term "juggernaut" has its origins in India. It describes a large heavy cart which carried an idol of the god Vishnu. It would be pulled along during religious celebrations, and his worshipers would sometimes get so excited that they would throw themselves in front of this (unstoppable because of its weight) cart and be crushed to death. We now use this term to describe anything that gathers momentum and is unstoppable. Are we being exposed to the danger of an unstoppable juggernaut of fear because of Y2K? Possibly.

So we need to do what we do best. Preparing for disasters. Being prepared will instill confidence in those who may be a quart low on self-assurance. We need to work with each other and our own agencies to put out good solid information about our plans and preparations for dealing with Y2K. We need to talk to community groups, PTAs, Lions, Rotary, Soroptimists, senior citizen groups and get out the word that we are preparing, planning, and are optimistic that we will cope with Y2K just as we have coped with every other disaster in our path. In fact, because we have so much time to prepare, this may not be a disaster at all.

9th World Conference on Disaster Management

Seminars and Workshops on:
Y2K Contingency Planning • Bomb Threat Management •
Critical Incident Stress Management • Public Safety
Communications • Incident Command System
• Many other areas relating to Emergency Management

June 20-23, 1999
Hamilton (Ontario) Canada

Discounts for IAEM Members
Register on-line at
<http://www.wcdm.org>

Canadian Centre for Emergency
Preparedness
P.O. 2911, Hamilton ON L8N 3R5
Canada
1-800-965-4608



WHERE ARE WE?

IAEM Surveys Local Communities on Y2K Preparedness

Around the country, 172 people responded to an IAEM online survey, to help FEMA assess local communities' readiness to deal with Y2K. Here's the tally of the results:

■ 95% said they are aware of the potential Y2K problem;

■ 92% said their organizations are actively working to ensure their systems will be able to handle Y2K conversion;

■ 34% reported that their organization's computers are fully prepared.

The survey asked respondents to assess readiness and cooperation on a five-point scale — 0 - 25% - 50% - 75% - 100%. Here's how they answered:

■ Extent to which emergency management program and related operations (911, EOC, warning systems) are compliant and operationally ready: About one-fifth said they were 25% ready; a third said 50% ready; another third said 75% ready; and 11% said they were 100% ready.

■ Degree of cooperation between the emergency management organization and other community agencies: About 7% said none; one-fifth said 25%; one-fifth, 50%; nearly a third said 75%; and about one-fourth said 100%.

■ Degree of interaction among the local, state and other localities' emergency management organizations: 7% said no interaction; nearly one-third said 25%; one-fourth each were at 50% and at 75%; fullest cooperation was reported by 11% of respondents.

■ Extent of jurisdiction's operational readiness: 9% said they were 100% ready; about a fourth said 25% ready; and about one-third each put themselves at 50% and 75% ready.

■ Availability of emergency preparedness guidance and information: The percentage of respondents at each point on the scale were — 0 (6%); 25 percent (25%); 50 percent (27%); 75 percent (30%); and 100 percent (12%).

Four open-ended questions asked for feedback on model state of local initiatives, unique problems, special Y2K-related issues, and "other comments."

The following comments are reflective of many that were received through the survey:

■ "We need credible threat scenarios from the President's Y2K group to guide local planning. The El Niño of 1998 was equaled only by the media's coverage. Y2K = El Niño squared."

■ "There is a sector of the population seeking information on this topic. Y2K awareness is providing us an opportunity to increase the level of all-hazard preparedness within the community. The trick will be to achieve this without playing into the hands of the zealots who are preaching doomsday scenarios."

■ "Today is our first meeting with the utilities, power, water, gas, sewer and hospitals. I am looking to discuss the big problem. I'm not concerned if the power company can send the bills out on time. I am concerned if the power will be on or not."

■ "My major concerns are twofold: I am concerned from a mitigation standpoint about the potential for panic in the public as a whole, because of a lack of accurate information. I would like to see a clearinghouse set up for emergency management personnel to access accurate information that can be conveyed to the public.... General ammunition in

the form of good and consistent information to take the wind from the sails of those taking the 'sky is falling' approach."

■ "We need current, accurate, reliable information concerning the risks and probabilities. ... Continued statements from national leaders that credible actions can be taken to avoid an unpleasant New Year's weekend should be made, with suggestions on what to do."

■ "Small, local governments and special districts are in dire need of assistance in identifying which of their infrastructure or critical systems could be impacted, how to test those systems and cost-efficient methods of correcting the problems."

■ "Y2K problem is feeding on itself and growing beyond reality. Needs federal level media campaign now!"

Resources Cited

(1) Wisconsin Dept. of Administration has compiled "Countdown 2000: A Handbook for Local Governments and Schools." Web site at <http://www.y2k.state.wi.us/>

(2) Article by Capers Jones, "Year 2000 Contingency Planning for Municipal Governments." <http://www.wangelfire.com/mn/infocrest/capers989.html>

(3) Lubbock, Texas was among the first to conduct a Y2K exercise. Emergency manager (and IAEM member) Ken Olson offers (for \$20) a packet that includes a video, newsletter, exercise script and news releases. Contact him by e-mail: KOlson@mail.ci.lubbock.tx.us

(4) Metropolitan Washington Council of Governments best practices manual (\$45). On the Web: <http://www.mwco.org>.

(5) State of Texas guidance to municipal governments: <http://www.dir.state.tx.us/y2k/resources/guidebook2000.html>

(6) Peter deJaeger's Web site: <http://www.year2000.com>.

OMB Reports on Federal Systems

The Office of Management & Budget (OMB)'s seventh quarterly report on federal agency progress on the Y2K problem, released in December, found that 61% of 6,696 mission-critical systems are Y2K compliant.

Eleven agencies have achieved OMB's most favorable rating, Tier 3. Among these agencies, 84% of mission-critical systems are Year 2000 compliant.

The Small Business Administration is the first agency to complete work on all of its critical systems; the Social Security Administration says 99% of its critical systems are now Year 2000 compliant.

OMB said it will work to ensure that agencies have the resources for their Year 2000 efforts. The Omnibus Appropriations Act, signed Oct. 23, included emer-

gency funding of \$1.1 billion for defense-related Year 2000 conversion activities, and \$2.25 billion for non-defense activities.

As of November 15, 1998:

- Of critical systems not yet in compliance, 30% are still being repaired, 7% are being replaced, and 3% will be retired.

- Agencies are developing contingency plans for systems that are not expected to be ready by March 1999, and continuity of business plans to ensure that vital public services will continue. Agencies have made progress on assuring that data exchanges with other systems, particularly systems operated by the states, will occur without problems.

Review the entire report on the Web: <http://www.cio.gov/new.htm>

NACo Assesses County Y2K Preparedness

In a recent survey conducted for the National Association of Counties (NACo), half of the nation's counties said they have strategic plans to tackle the Y2K problem. The survey, conducted by National Research, Inc. in November, covered 500 counties in 46 states.

Of the 16 counties with populations above 500,000, all but one have already prepared a countywide plan, while 74 of the 119 counties below 10,000 in population have not.

While some counties are operating without a strategic plan, 77% are aware of the Y2K problem, and are taking steps to assure compliance. More than one third reported completing their system assessment — finding out exactly what computers and equipment require attention — while 41% said they were more than halfway there.

Seventy-six counties, or 16%, said they are ready for the big day. About 24% have nearly completed repairing or replacing their systems. Twenty-one percent said they are a little more than halfway to three-quarters complete.

As their top three priorities, counties have tagged general government administration, taxation and finance, and emergency response, according to survey results.

Big dollars have been directed toward compliance, and many more are budgeted. Counties in the survey estimated the total cost of Y2K compliance will top \$283 million. NACo estimates that before New Year's Day 1999, it will cost America's counties about \$1.7 billion to achieve Y2K compliance. A majority of 86% said funding for compliance would come from the county's general fund.

<http://www.naco.org>

Emergency Services Sector Surveyed

A readiness survey of the emergency services sector (fire, police, emergency medical) showed that more than three-fourths think their agency is internally prepared for Y2K, but less than one-fourth have effective contingency plans for the external effects of possible Y2K problems.

The survey, which drew 212 responses, was conducted by the Emergency Response & Research Institute (ERRI) based in Chicago. Clark Staten, executive director of ERRI, concluded, "I am not assured, at this point, that fire, police, EMS and disaster chiefs are paying enough attention to this Y2K problem."

All who answered said they had heard of the Y2K problem and understand its basic implications for their agency, yet just under 75% expect to be affected. About 63% said Y2K is a serious problem, but

solvable; 13% said it is "vastly overblown." About 5% called it "a potential catastrophe in the making."

Nearly 30% of respondents said their agency or department has a specific plan to deal with potential problems on New Year's Eve 1999. Less than half, however, said their department is now effectively prepared. Nearly 10% answered "don't know" to that question.

Asked to put an "x" next to all other agencies their department is working with on preparedness for Y2K, fewer than 10% listed any single entity, including power company, health/human service agency, water department, gas company, state emergency planning agency, FEMA, nuclear facilities, businesses, hospitals, fire or police departments or EMS agencies.

For more information, contact ERRI on the Web (<http://www.emergency.com>) or by phone (773-631-3774).

From the IAEM Conference

Emergency Managers Pack Y2K Conference Session

One of the hottest tickets at the IAEM conference in November was the session on the Year 2000 problem. Member Kathleen Henning, CEM (Montgomery Co., MD) talked about her county's preparations, and brought with her one of the county's technical consultants, Pat Finucane of Klein Technologies, Inc. (Vienna, VA).

"It's not too late," Henning emphasized.

"It's not a technical problem," at least for emergency managers, she added. In the article on page 14, she describes preparations for a full-scale exercise on Y2K in her county.

But at the conference session, Henning described the problem briefly, reviewed dates (not just Jan. 1, 2000) when problems can be expected — see the box at right — and discussed possible impacts on local government of Y2K-related failures and how to prepare contingency plans.

Possible impacts cover: emergency 9-1-1 and dispatch, utilities, tax collection, licenses and permits, Dept. of Motor Vehicles, finance, payroll systems, traffic lights, and many more. "Embedded" microchips — many of which also depend on dates — may create sporadic failures in electrical transmission, water and sewer systems, medical devices, telecommunications, and building systems (heating/cooling, elevators, security).

Keys to Success

To be successful in planning for Y2K calls for several critical factors, she said:

- Make everyone part of the solution.
- Triage — make the best use of your resources.
- Maintain a sense of urgency.

- Communicate, communicate, communicate!
- Constantly assess vulnerabilities.
- Establish contingencies.

You must have support from elected officials, Henning emphasized, plus a Y2K project office (or other technical people) who can point out the potential "weak links" where you should target your planning. A public/private partnership is essential, since most local governments lack enough staff to deal with an issue of the breadth of Y2K.

Montgomery County established six focus groups to address critical business functions: public safety, transportation, communications, utilities, health services, and commerce. These match the focus of a 17-jurisdiction regional council of governments, which developed a Y2K best practices manual.

Contingency Plans

Even if all internal systems are compliant, all organizations depend on others for power, information, supplies and revenues. Evaluate these external dependencies and make contingency plans in case these sources are interrupted, Henning advised.

Perhaps the most critical is our dependence on infrastructure, she said. Here is where the Emergency Management Group (EMG) — Montgomery County's multi-agency planning umbrella — plays a role.

The EMG is organizing for Y2K action using its existing committee structure. They are assessing the readiness of critical public safety systems and suppliers, evaluating various Y2K scenarios, reviewing and updating disaster plans, and developing contingency plans where needed.

Possible scenarios include extended utilities outages, a metropolitan-wide telephone outage, and weather-related conditions. Neighboring communities have to work together, too, to identify resources, set priorities for restoration of services, and share resources and technical information, she urged.

The Technical Side

Klein Technologies, Inc., which has worked with Montgomery County, offered the engineer's point of view on Y2K problems, in the person of Principal Engineer Pat Finucane.

His primary message was that Y2K — the inability of computer logic to properly translate two-digit year data beyond 99 — has no "silver bullet" fix. It's a multi-level problem, involving hardware, software, applications, data and networks.

You will have problems, to some degree, he said, because there is not enough time and not enough resources to find and

(continued on page 9)

Y2K: Dates

To expect problems

- Jan. 1, 1999: Systems that look one year ahead may fail.
- July 1, 1999: New fiscal year for many.
- Aug. 21, 1999: GPS rollover date.
- Sept. 9, 1999: Many computer systems use 9/9/99 as a file purge date.
- Oct. 1, 1999: Federal government and others begin FY 2000.
- Dec. 31, 1999: The largest date some older systems can store.
- Jan. 1, 2000: Rollover will halt, confuse, or otherwise disrupt many systems and devices.
- Feb. 29, 2000: Many systems will not recognize leap year.
- Oct. 10, 2000: First time date field uses maximum length.
- Dec. 31, 2000: Some systems may not recognize the 366th day.

Conference Session (continued from page 8)

correct all the systems. He suggested the following logical, sequenced approach, starting with an inventory:

- Prioritize the systems to be fixed.
- Be prepared to "kill" or isolate systems that won't be fixed - i.e., those systems which will not affect people, safety or infrastructure.

- Stay focused on the task of risk mitigation, a task which calls on you to: fix hardware first; correct or update operating systems; correct current data; then check and fix data interchanges; fix system relationships to other systems; and if there's time, correct historical data.

Stop the problem from getting worse by controlling system growth, purchasing only compliant equipment, and requiring only four-digit years on all forms and data.

Finucane also discussed embedded microchip systems which are "suspect," including those in temperature sensors and smoke detectors, subassemblies with timing functions (traffic controllers), manufacturing and process control computer systems. In building systems, watch out for hidden links between systems, he warned: a non-compliant system can take down systems with no Y2K sensitivity.

And one other caution: even new PCs may not be compliant, because of a common practice of recycling BIOS chips.

Finucane also gave details on client servers, PCs, operating systems, networks and telecommunications.

For more information: Klein Technologies has posted the presentation materials (Y2K Technical Overview) on their Web site: <http://www.kleintech.com>. Click on Y2K from the home page, then view or download the file.

What Are We Planning For?

by Jeffrey M. Modic, American Information Engineering Corporation

Note: This article is an excerpt from the keynote address to a California Rural Government Y2K Conference on Oct. 28, 1998. The author, who helped California State Senator Tim Leslie organize the conference, tries to define the range of consequences that might be expected to stem from Y2K-related failures.

It seems hard to believe that in little over a year from now, at the stroke of midnight, Year 2000 will arrive. January 1, 2000 is the perceived beginning of a new century and a point in time that will give people a sense of well being, of new beginnings, and reason for great optimism. It is also this same point in time that will determine whether we have met the first serious challenge of the Information Age.

A design flaw in millions of the world's computer programs will result in their failure to recognize the arrival of the year 2000. After midnight on the last day of "99" computer systems worldwide will interpret "00" as signifying the Year 1900, not 2000. Computer system reaction to this situation will range from producing erroneous information to shutting down all processing. ... If left uncorrected, Y2K has the ability to disrupt the economy of the entire world and diminish the quality of life of every person on the planet.

... [It] is reasonable to expect that most mission critical systems will be in some state of readiness. But considering the amount of work that still remains and the limited time remaining in which to accomplish it, it is now physically impossible to have all systems ready. ...

One of the federal government's most important roles in the coming months will be to develop assessments of what is likely to be the impact of the year 2000 problem in key sectors of the

economy. Although this information will probably not be available until the first quarter of 1999, we can look at a conservative scenario based on analysis of the best information available. Much of the following information has been distilled from testimony before the U.S. Senate's Special Committee On The Y2K Technology Problem, and the public comments of folks like Senator Robert Bennett, Alan Greenspan, and Dr. Ed Yardeni.

- The power grid will work. There may be power shortages. Expect brownouts and regional blackouts, and in some areas of the country, isolated power failures. There is some risk that the grid may disassemble, but the power grid as a whole should not go down.

- Our financial systems will work. Expect to still be able to trade stocks on the major US exchanges. Don't expect to trade stocks on most other foreign exchanges, but our domestic exchanges will probably work. Expect insurance companies to attempt to remove or void their coverage for Y2K related accidents.

- Our banking systems will work. ATMs will work. There is a high probability that some individual banks and credit unions may go bankrupt. Expect banks to honor their credit cards and checks. I wouldn't expect to do business with a bank outside the U.S. But the banking system as a whole will probably work.

- Water: Assuming that power is available, water will be available in most municipalities. There are probably some places where the water system will break down and those communities will face serious difficulties. But water systems as a whole will probably work.

(continued on page 10)

What Are We Planning For?

(continued from page 10)

■ **Health care:** There are health care entities that may go bankrupt because of interruptions or delays in their revenue collections, particularly from state and federal programs. There are medical machines that will fail in ICU units. Medical supplies and prescription drugs may run short due to delays in shipping. There are hospitals that are far enough away from other hospitals that they have no backup, and if they have a failure in some of their machines or in some of their supply lines, there will be people affected in terms of patient care.

■ **Counties and cities:** There is a high probability that some cities and counties may go bankrupt because of interruptions or delays in their revenue collections accompanied by significant increases in their operating expenses. Expect substantial increases in the demand for all public services. Expect enormous increases in the demand for emergency services.

Expect a major tear in the social fabric of every community in this country if the government cannot deliver welfare, social security, retirement and other entitlement checks.

■ **Communications:** Phones will work. Expect peak overloads, normal for holiday periods. Expect some sporadic regional disruptions. Don't expect to get a dial tone in most other countries.

■ **Oil and gas:** Expect that we will probably be back to rationing until our international supply lines are compliant and secure.

■ **Transportation:** Expect that there will be rationing and delays. The air traffic control system will work, but expect there probably will be flight rationing. Some airlines will not have airplanes in the air. Don't expect any form of transportation to work at the same

level that it currently is operating at now. If shipping and transportation is rationed, expect that supplies deemed mission critical will take priority over private enterprise shipments. If you employ a just-in-time inventory approach which depends on timely freight deliveries, that's not good news. If you depend on importing or exporting products, that's not good news. If you're in the leisure hospitality business, expect travelers and tourists to remain close to home. The expected situation come January 1, 2000, is best summarized in a recent statement by U.S. Senator Robert Bennett (R-Utah), who heads the Special Committee on the Year 2000 Technology Problem. He said, "I do not expect widespread failures of electricity, water, telephone, transportation or financial systems, but I do not predict a rosy transition either."

About the author: Jeff Modic is president of American Information Engineering Corporation, an information management services company based in the San Jose, California area. His e-mail address is: jmodic@aiecorporation.com. More detailed comments from the author are included in a rebroadcast of an online/audio Global Y2K Action Conference held Nov. 27. Go to <http://www.y2kactionday.com>.

Planning:

John A. Koskinen

Testimony to Senate, Oct. 2, 1998

(John Koskinen is Chairman of the President's Council on Y2K.)

Through the outreach efforts of our more than 30 sector working groups, the Council is encouraging agencies and organizations outside the Federal Government to prepare two types of contingency plans. First, we are stressing the need for organizations to develop a plan that addresses internal system failures. For this plan, an organization needs to be asking, and answering, key questions such as: If some of our internal systems fail, how will we continue our core business processes?

The second type of plan needs to address the potential for failures in external systems upon which organizations depend for their day-to-day activities. These systems can run the gamut from those that help to provide basic services, such as water or power, to those that support the activities of key vendors or suppliers.

Organization heads need to ask themselves: What are our critical external dependencies? Are any of those dependencies likely to have problems? How will we function if they do?



**Community
Alert
Network Inc.**

One call to reach many.

Toll free: 800-992-2331

e-mail: cancalls@ix.netcom.com
<http://www.can-intl.com>

*The View From the Top:***An Interview with the President's Council on Y2K**

Questions still race far ahead of answers as more and more people — including emergency managers — learn more about the Year 2000 (Y2K) Millennium Bug.

The primacy of questions is even evident at the top, based on a December 9 interview with Jack Gribben at the President's Council on Y2K Conversion. The *Bulletin* asked two questions at the forefront of emergency managers' concerns: (1) What is the most likely scenario we should be planning for? and (2) How should we advise citizens to prepare, to avoid panic?

The short answers were: (1) It's hard to tell ... there's "no certainty about where we'll see failures or how extensive" they will be; and (2) It's "a little premature" to be giving advice on preparations, until more is known about the answers to question one.

Which Scenario?

The view from the President's Council right now is that "the basic infrastructure will hold," meaning the power grid, communications and other vital systems, Gribben said. But there will be disruptions in some areas. "If I had to guess now," I'd look at those sectors where not much remediation has been started yet, such as smaller businesses and smaller local governments, which may experience interruption in local services.

For the big picture, the President's Council is gathering assessments from its 30 sector groups, to try to develop a sense of where failures could be most likely. As these assessments are reported, they are posted on the Council's Web site (<http://www.y2k.gov>, under "information sharing"). The Council also is

working on its first public report distilling the sector assessments.

These assessments have a broad, national scope, because one of the major aims they serve is to help gauge the level of federal response that will be required, Gribben explained. To get regional or local information, he advised, talk to service providers at the local level.

Message to Citizens

It's premature to advise citizens how to prepare, Gribben suggested, noting that the prevailing attitude at the President's Council is that "people panic when they don't have information." Thus the focus right now is on assembling that information through the sector assessments.

Giving the public a clear idea of where governments and businesses stand along the spectrum of work required to deal with Y2K-induced problems will help dispel panic, he said. Meanwhile, more knowledge about where failures are likely to occur will guide advice about reasonable preparations to recommend.

Asked if any federal agency would take the lead on developing recommended public guidance, Gribben said the President's Council would be the most likely candidate for that task — but probably not until mid-1999.

There is "no evidence that people should be disrupting their lives in a significant way," he declared, because "we don't believe" there will be massive failures lasting 6-8 months, as some are speculating. Whatever happens will be "more transitory — a couple of days" perhaps ... but there really isn't good information yet, he said.

Another topic of concern to state and local officials is funding

to deal with Y2K efforts. Gribben said Congress has been responsive in appropriating money for federal agencies to remediate critical systems, plus approving contributions to the World Bank for remedial efforts in developing countries.

While there's probably not much more coming for state and local governments, he did explain that some federal agencies have announced that Y2K projects will be considered eligible for funding through certain grant programs. As an example, he cited the Department of Transportation's intelligent transportation systems grants, but said he knew of no central clearinghouse that pulled together this type of information.

What's Next?

In 1999, the President's Council will focus increasingly on contingency planning for potential Y2K-related failures and disruptions, Gribben said. (See also the excerpt from Council Chairman John Koskinen's Senate testimony in October, printed on page 10.)

Resources

As sources of guidance for local officials, Gribben suggested:

■ Public Technology Inc. PTI — an arm of the National League of Cities, National Association of Counties and International City/County Management Association — has an information campaign for local officials called "Y2K and You." For information, visit the Web site: <http://www.pti.org/membership/Y2K>, or call 1-800-PTI-8976.

■ National Association of Counties (NACo). Web site: www.naco.org

■ President's Council Web site: <http://www.y2k.gov>. This has sector assessments, press releases and testimony, plus links to Web sites of every state. One good example from the state level is the guidebook for local governments prepared by the state of Texas.

Emergency Managers: Planning, Exercising

Emergency Management Planning for Y2K

by Chief Chuck Lanza, CEM, Director, Miami-Dade County (Florida)
Office of Emergency Management

Year 2000, Y2K, the millennium bug, whatever you call it, it is more than a computer problem.

It has its origin in computer programming that was done many years ago. A simple activity of reducing the year from 4 digits to 2 digits to save valuable memory has given rise to this problem. At that time computer memory was expensive and conservation of that memory was very important. Today, we are faced with how systems will react when the computer clocks are turned to 00 as we usher in the Year 2000. If computers that are critical to transportation systems, communication systems, or the production of electricity fail, many other failures may occur. These failures could affect our lives and our communities.

World-Wide Impact

Not since World War II has there been a threat that looms so large as to affect the entire world. Businesses and government are spending billions of dollars to prepare computers and computer systems for a smooth transition into the 21st century. The computer transition, with many or only a few failures, could cause varying degrees of disruption to services that we depend on every day of our lives. Electricity, water, transportation are only a few of those services. No matter what, if any disruptions occur, citizen response is critical to success or failure of society's response.

For example, if we are uninformed or ill-prepared to deal with loss of services, panic could

ensue that could far and away exceed the extent of the actual disruption. On the other hand, if individuals are given the tools to prepare themselves, their families and the community, it follows that they will be ready for disruptions of services, will work together to maintain order, and will foster a rapid recovery. I, for one, choose the second option: educated and prepared individuals and communities.

Four Principles

In the emergency management community, comprehensive emergency management plans are written around four basic principles: We began our planning process by identifying the threats Y2K failures may have on our community. Needless to say, nobody is certain how many disruptions will occur nor can we know what the resident's response to failures will be. In his July 7, 1998 article, "The Year 2000: Social Chaos or Social Transformation? Part 4", John Petersen presented four scenarios that were developed by David Isenberg from Isen.com. Although all four scenarios are insightful, two are very important to emergency managers and are used as the premise for our plan. Mr. Isen's scenarios can be viewed at <http://www.isen.com/archives/980515.html>.

The main determinants in the scenarios are disruptions and public response. In its simplest form, disruptions will either be isolated or multiple, and the public's response either coherence or chaos. Two scenarios that

should be addressed in any Y2K response plan are: 1) isolated disruptions that are associated with public chaos and 2) multiple disruptions that are associated with public coherence.

The "Whiff" Scenario

The first scenario, labeled "whiff of smoke," is representative of a situation where a person yells fire in a movie theater. The Y2K parallel exists when a community does not understand the situation or does not have confidence in its leadership to provide protection. This situation can be addressed in the comprehensive plan by identifying public officials to provide continuous and credible public information. Media relations are imperative to prepare and disseminate information on what can be expected and what government has undertaken to protect the community. Public service announcements similar to what are done for hurricanes, earthquakes, and floods can help reduce fear.

The "Bad" Scenario

The second scenario is the antithesis to the first. Things are bad. There are multiple disruptions in the essential services, but the community is not in chaos. Instead, they are working together as a community to deal with the problem. I have seen this situation once, following Hurricane Andrew when the community came together to work through their problems. One resource that was available to us following the hurricane, which will not be available in a Y2K event, is the thousands of other communities who lent a hand. In this situation we will need to be self-sufficient, as every community is likely to have some degree of disruptions

(continued on page 13)

Planning for Y2K

(continued from page 12)

and different levels of chaos. We want our activities to be directed towards minimizing chaos.

In a nutshell, all Y2K compliance activities are being undertaken to reduce the potential for major disruptions. All emergency management planning activities will be directed towards minimizing chaos and moving the public to coherence. Success of compliance activities and in public coherence will move us to an area where Y2K will have the least effect on the community.

Identifying Functions

In preparing our response plan, we identified and prioritized functions and services. Many of these are based on functions and services presented in Ed and Jennifer Yourdon's book, "Time Bomb 2000." They are as follows:

1. Food and Water
2. Utilities (electric, natural gas, water and sewer)
3. Energy (fuel)
4. Protective Services (police, fire, and EMS)
5. Transportation
6. Health Care
7. Communications
8. Information Dissemination
9. Government
10. Education
11. Economy

For each function and service every community should undertake the following activities:

- Identify threats
- Develop threat monitoring procedures
- Identify actions that may eliminate the threat in advance
- Identify actions that may be taken to minimize the impact of the threats if they materialize

Two Kinds of Mitigation

There are two general areas of mitigation which relate to Y2K. The first involves activities currently going on to identify and

correct software problems, as well as hardware and embedded chip incompatibilities. Businesses and government throughout the world have undertaken the task of trying to avert a major crisis with varying degrees of vigor and success.

The second area deals with what emergency managers are doing to mitigate the impact of system and infrastructure failures that might occur if attempts to head off Y2K problems don't succeed. These failures can and will affect our communities in a variety of ways, and we must be ready. You can assume from the attention being paid to the potential for a system failure that we believe it will not be possible to completely avert large scale Y2K impact.

The Miami-Dade County Office of Emergency Management (OEM) has developed an approach that utilizes the goals and steps suggested by Capers Jones and the Yourdons. It involves each Miami-Dade County department taking responsibility for assessing their own Y2K situation. More specifically, each department must develop a method of assessing post event disruptions in regard to severity and projected duration. The cost of mitigation and additional costs, should actions become necessary to minimize the impact of threats, must also be estimated.

Community Awareness

Community awareness is a major concern for contingency planners. If the public is not accurately informed of potential Y2K software problems, they may respond inappropriately. This could result in problems greater than what might have been caused by an actual Y2K related disruption. Keeping with the theme of all entities accepting responsibility of preparing for potential impacts of the Y2K disruptions, development

of Y2K public education and preparedness programs for residents of the community, is imperative.

There is a possibility, however remote, that communities will not be able to access resources from outside their jurisdictions. All plans must address that possibility. The underlying theme for all planners is self-sufficiency.

About the Author: Chief Lanza has been Director of the Miami-Dade County (Florida) Office of Emergency Management (OEM) since August 1995. Since joining Miami-Dade Fire Rescue in 1978, he has also been the Chief for Communications and Emergency Medical Services and Director of the Office of Trauma Services.

In the last 10 years, Chief Lanza has faced major challenges from Hurricane Andrew, the crash of ValuJet Flight 592, the Ground Hog Day Tornado, and most recently the fire on board the cruise ship *Ecstasy*, heading public safety for Super Bowl XXXIII January 31, and planning for Y2K and terrorism.

He has a weekly column, "Global Problems with Local Solutions" at www.y2ktimebomb.com. He also hosts his own Web site www.ChuckLanza.com and is releasing a video soon on Y2K preparation. His e-mail address is chuck@ChuckLanza.com

Resources

The author's favorite resources:

■ Ed & Jennifer Yourdon's book, *Time Bomb 2000: What the Year 2000 Computer Crisis Means to You!*, Prentice Hall, NJ, 1998

■ Capers Jones, Chief Scientist at Software Productivity Research, Inc. wrote the book, *The Year 2000 Software Problem: Quantifying the Costs and Assessing the Consequences* and many articles including "Y2K Contingency Planning for Municipal Governments." (<http://usa.nedstat.net/cgi-bin/viewstat?name=Municipalplan>)

Y2K Exercise**Testing People, Not Just Computers***by Kathleen Henning, CEM, Program Coordinator, Montgomery County, MD*

Note: The author prepared this summary just before a scheduled December 21, 1998 full-scale exercise in Montgomery County, MD, one of the acknowledged leaders in Y2K preparation.

As the countdown to Year 2000 draws closer, many governmental and private organizations have moved into the testing and evaluation phase of their preparation for potential multi-system failures or disruptions to critical systems. Emergency managers need to be ready to respond to potential critical mission failures in communication, utilities and public works, transportation, health care, financial, business, public safety, legal, human resource, or other systems that may be impacted. Training and exercises can help to reach the goal to be better prepared for Y2K disruptions.

People & Systems, Not Just Computers

In many large jurisdictions and organizations, system analysts have been hired and organized into special Y2K Project Offices, or they work internally within offices and groups. Their role is often to conduct system and risk analyses, and ensure that business continuity plans are in place. They are working within the organization to test equipment, identify potential areas for corrupted data or system failures, and suggest remediation efforts for equipment.

Their efforts to fix or replace the equipment should not overshadow the efforts to diagnose and improve our emergency response capability to potential systems failures created by the Year 2000. After all, Year 2000 presents people and system problems, not just computer problems.

Training of Personnel

As emergency managers we need to remember that the training of essential personnel and the updating and testing of contingency plans is an essential component of our mission. One effective way to test the system is through progressively more difficult and complex drills and exercises.

Y2K training and exercises can follow the format established in courses at the Emergency Management Institute (EMI) for natural and technological hazards. Y2K contingency plans and testing can be designed into drills, orientation sessions, tabletops, functional, and full exercises. The key to success is to focus on the needs of the personnel and the testing of contingency plans which should be a part of our existing Emergency Operations Plan.

First Step: Orientation

Identifying the critical components of Y2K contingency plans is often the hardest step for state and local governments to start. This can be included in the most simple types of exercise – the drill or orientation session. During the orientation session, for example, the overview of both the technical and the emergency response perspectives to the Y2K problem can be shared with participants.

They are given familiarization training on the existing Emergency Operations Plan and updates to the contingency plans. They learn about risk analysis, embedded chips, system testing, and how contingency planning needs to be done at both the work unit level and in the multi-agency emergency management group. They can also be motivated to work through issues by having the elected officials or members of the executive staff present the orientation.

Drills and Focus Groups

Drills and focus groups help fine tune the skills needed for a particular type of response. A drill can help various governmental agencies work through the process of prioritizing critical missions, assigning resources, and identifying system shortfalls for Y2K initiated problems. Focus groups can be organized by subject matter, such as health care, public safety, or business and finance with work sheets to help them. Another drill might include an activation of the Emergency Operations Center with the testing of primary and backup communication paths as a simulation of "First Night" of the Year 2000. Drills are particularly effective as training tools to build depth in the organization. They also assist Y2K specialists who may be activated to an Emergency Operations Center to better understand the emergency response system.

Tabletop Exercises

The tabletop exercise draws together representatives from various agencies who are presented with a series of difficult problems which they are assisted in working through in a structured setting. Tabletop exercises are particularly effective when agencies are in the early stages of their Y2K remediation efforts or want to test the inter-relationships of responding organizations.

Tabletop exercises take areas such as public information, liaison with outside agencies, operations, logistics, planning, or administration/finance and test them more thoroughly in a multi-agency response setting. The "lessons learned" section often highlights new areas which need to be addressed or proposes major changes to the contingency plan.

Lubbock, Texas was the first in the country to publicly conduct a tabletop and share its lessons

(continued on page 15)

Testing People (continued from page 14)

learned with other jurisdictions. Lubbock also took advantage of the exercise by attracting media attention to motivate the participants and assist other jurisdictions with their planning efforts.

Building in Triggers

Activation of the Emergency Operations Center with timed and increasingly stressful simulations and messages of Y2K multi-system failures can be an extremely effective functional exercise. Functional exercises can often include time compressions. For example, the first phase of the exercise may include the 9-13 hour window prior to clock rollover to Year 2000. This gives participants an opportunity to "learn" from reported system failures in the Asian and European arena before the event occurs in their area. Messages about embedded chip failures are triggers that can be worked into the scenario where agencies must identify how they would locate these chips in their own systems.

Phase Two

Phase 2 might be the initial period after the clock rolls over, or it might be during a simulated worst case scenario when various public and private systems simultaneously or progressively fail. Triggers from the contingency plans are then included in the exercise, such as when temperatures drop below 20°, when phones don't operate due to a PBX failure, when generator supplies are exhausted, or when a main-frame computer system has data corrupted by a "millennium bug" virus. These exercises can be made far more realistic by including the input of your Y2K system analysts in designing and customizing the scenarios to your region and capabilities.

Real Time Testing

When state and local governments are ready to take the plunge, then full scale exercises can be conducted. These include full activation of the Emergency Operations Center and real-time testing of systems. This might include actually rolling clocks over to the Year 2000 during 1998 or 1999, with resources on standby. Another component may be departments which are presented with "simulated system failures" but which must implement their contingency plans real time with evaluators in the departments observing the plan as it goes into effect.

Montgomery County Maryland has chosen to test its system in both these ways. We will have a better view after the December 21st exercise.

Each jurisdiction must review its own contingency planning strategies and its liability issues as testing begins. As emergency managers we need to keep the focus on the training of essential personnel and the testing of contingency plans, and not just on the testing of computers. An effective way to jointly test our people and system is integrated testing through progressively more difficult and complex drills and exercises.

Montgomery County News Updates from the Author:

- Dec. 4 — Montgomery Co. Fire Administrator Gordon Aoyagi spoke to Maryland Emergency Management Association on Y2K contingency planning.
- Washington Metropolitan Council of Governments plans a multi-jurisdictional Y2K exercise using Montgomery County's December 21 exercise as baseline.
- Maryland hires contractor for Y2K Risk Assessment of all

RESOURCE LISTING

Y2K is notable for the vast amounts of material out there for you to digest. Some of it's good; some not. But most of it is best found on the Internet — and it's changing daily.

If you don't have Internet access, please send in on how we can help you stay informed. Several authors have told us their favorite sources of information; these are included at the end of their articles, as well as with the page 6 story on the IAEM survey.

There also are several "umbrella" Web sites:
 ■ The federal Chief Information Officers Council, which has a gateway for Y2K information directories: <http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm>

To go directly to the page with links to all state sites and names of state coordinators, plus numerous local government sites: <http://www.itpolicy.gsa.gov/mks/yr2000/state.htm>

■ The President's Council on Y2K Conversion has sector assessments and other excellent information: <http://www.y2k.gov>

■ Senate Special Committee on the Y2K Technology Problem has hearings testimony: <http://www.senate.gov/~y2k/>

■ OMB quarterly reports show up first at <http://www.cio.gov/new.htm>.

Also see the listing in the June issue of the *IAEM Bulletin*, p.13.

counties. State plans Y2K multi-jurisdiction exercise July 15th.

• Montgomery Co. presents Y2K Powerpoint program with Small Business Administration on business continuity planning with emergency managers. Will be available on the Web: <http://www.mo.md.us/Year2000>.

Y2K Contingency Planning - Seven Steps to "Plan B"

by David A. Johnson, FBCL, CBCP

Is the end of the world nigh? Are massive power black-outs, global telecommunication breakdown, and collapse of the world economy just around the corner?

Will the Millennium Bug bring about the end of civilization as we know it?

Probably not. Despite the hype and hysteria about Y2K, a catastrophe of Biblical proportions is unlikely.

This is not to say that the rollover will be a non-event; the problem is not going to go away.

Disruptions Inevitable

Disruptions are inevitable. Technology has never been without its problems: unanticipated failures occur, and, in due course, are rectified. In most cases, the impact is minor, but even when the impact is major the world goes on. What is unique about the Year 2000 situation is not that we will be facing technological failures of an unprecedented nature, but rather of an unprecedented number.

Major disruptions will undoubtedly occur, and will likely be dealt with "in due course." The vast majority of disruptions, however, will be minor. Unfortunately, due to sheer numbers, "due course" for resolving minor disruptions may be days, weeks, even months.

Businesses the world over, therefore, must brace themselves, not only for potentially major disruptions of finite duration but also for any number of minor disruptions of indefinite duration.

A Starting Point

Development of contingency plans is an absolute necessity, but where does one begin? The number of potential scenarios for

technological failure in the year 2000 seems overwhelming.

Globally, this is indeed the case, but from the perspective of an organization's individual business units the number of relevant scenarios will usually be manageable. If each business unit approaches the problem calmly and methodically, there is no need to feel overwhelmed.

1. The first step in the contingency planning process is simply to list each discrete function or service for which the business unit is responsible. This list should include every function or service, not just those that are perceived as the most critical.

2. The second step is to perform a "quick and dirty" vulnerability assessment for each business function, based on its level of technological dependence. A simple ranking from 0 (no technological dependence) to 3 (absolute technological dependence) will suffice. A brief description of each of these dependencies should be documented.

Note that no consideration need be given to the technology's anticipated level of Y2K compliance. However, consideration should be given not just to internal dependencies but to any external dependencies which could affect operations (for example, by disrupting the supply chain).

3. The third step is to perform another "quick and dirty" assessment, this time of the potential impact to the organization if the business function could not be performed for an extended period of time (i.e. several weeks). This impact could be quantitative, such as loss of revenue, or qualitative such as loss of reputation. Again, a simple ranking from 0 (no significant impact) to 3 (unacceptable impact) will suffice.

4. The fourth step is to multiply the two rankings. The higher the resultant number, the more critical it is to develop contingency plans for the specific business function. Top priority, obviously, must be given to functions with a combined ranking of 9, followed by those with a ranking of 6, then 4, and so on in diminishing importance.

5. The fifth step is to identify those scenarios which could realistically occur, and which would disrupt the business function. These scenarios could range from major technological failures of finite duration, such as loss of power or telecommunications, to minor technological failures of indefinite duration such as malfunctioning office equipment or computer programs. While there may be several possible scenarios, only those relevant to the specific function need be considered.

6. The sixth step is to develop a contingency plan for each scenario. The goal of the contingency plan should be to maintain an acceptable level of operations for the anticipated duration of the disruption, or to ensure resumption of operation within an acceptable period of time. The contingency plan may entail alternate modes of operation, utilization of alternate or backup technologies, reduction in service levels, even temporary suspension of the function.

The plan need not result in business as usual, but should at least mitigate the impact of the disruption to an acceptable level. In all cases, the contingency plans should be kept as simple as possible. The more complex the plans, the less likely they are to be effective.

7. The seventh and final step is to validate each contingency plan. At a minimum, this should involve a detailed walk-through of the plan with other members of

(continued on page 17)

Seven Steps to Plan B (continued from page 16)

the business unit, and perhaps members of other business units. If possible, the plan should be tested under actual operating conditions, or at least under simulated operating conditions.

In addition to ironing any wrinkles out of each plan, validation will help ensure that members of the business unit are prepared for the actions they may have to take if Year 2000 problems arise.

Long-Term Dividends

While the challenge of Year 2000 contingency planning is not insurmountable, it will require a significant commitment on the part of each business unit. This is a commitment well worth making, not just to cope with the rollover of computer dates, but to cope with technological failures in general.

Unless the Millennium Bug really does bring about the end of civilization as we know it, we will continue to be a technologically dependent society. Major and minor disruptions, for whatever reasons, will continue to occur.

The effort spent now incorporating contingency planning into our business processes will pay dividends long after January 1, 2000.

About the author: David A. Johnson is a Business Continuity Planner with over 30 years' experience in information technology. He has been a member of several Y2K compliance projects, conducts workshops, and is assisting agencies across North America develop Y2K contingency plans. He co-chairs the 9th World Conference on Disaster Management (see ad, page 5), and works at the Canadian Centre for Emergency Preparedness with IAEM Board member Marg Verbeek. He can be contacted at 1-800-965-4608 or djohnson@ccep.ca.

Y2K: Emergency Response Preparedness - Preemptive Action

by James Bowen

The Y2K issue has received international attention. This article suggests steps you and your organization can take to minimize the potential for disruption of service.

A Suggested Plan

Each person on a response team can begin with their own equipment. Start with what ever equipment you work with directly — a computer terminal, a GPS location device, radio or video equipment, etc.

The simplest question — is this equipment in any way dependent on a date, either in the software or the hardware? If the answer is an unqualified no, then relax; otherwise some action is necessary.

The more difficult question is — will this piece of equipment continue to respond correctly when the date rolls over to the year 2000 and beyond?

If the answer is no or unknown, the testing and remediation should be started at once. The supplier, technical support people or an external consultant can devise test and remediation plans to provide assurance that the oncoming dates will not affect the equipment.

The next question is — is my equipment connected to any other equipment electronically. If the answer is yes, then;

Does my equipment supply or receive data through this connection? If yes, there may be a problem.

Embedded systems offer special challenges. The code that drives the system is often not available for scrutiny by expert programmers, and the presence of hidden clocks in the hardware is often very difficult to determine; the only recourse is an assessment based on a carefully crafted test

procedure. Test procedures and protocols should be developed and executed by those with a knowledge of the appropriate critical dates, and the means to adequately test the effects of a rollover on these dates.

Trial Run

The assessment procedure involves isolating each individual component in a system, and determining if it has a time system that records or displays time and dates. Each component must be tested for a selected sequence of date rollovers. When each piece is determined to handle the rollovers, then they can be connected and the whole system tested for rollover compliance. In general, this is not a simple task and experts in the various components and in the overall system need to be consulted to determine an adequate test.

Risk Assessment, Contingency Planning

Even after a satisfactory test of critical dates, there remains the possibility that a failure will be induced by some unknown date rollover. The obvious solution is to assess the risk of losing a piece of equipment, and entering the contingency planning phase.

Contingency planning is based on the degree of confidence in the results of the assessment and the trial run and in the perceived risk of a failure. In general there are four courses of action: Do nothing, do a work-around, repair the equipment, or replace the equipment.

Do Nothing suggests that all possible testing for compliance to Y2K rollover dates has been conducted and there is reasonable assurance that the system will go

(continued on page 18)

Preemptive Action (continued from page 17)

through the millennium rollover without induced failures. It could also imply that plans in place for handling equipment failure provide that a Y2K-induced failure can be handled in normal fashion.

Work-arounds are often available to make equipment usable, even though the basic operation may be influenced by a date rollover. Many equipment manufacturers have suggested, published or made available work-arounds for their equipment.

Repair or replace are obvious solutions. Repair suggests that the manufacturer or a supplier has the means to adjust the code or other parameters so the equipment is insensitive to the date rollovers. Replace is an obvious solution that is typically limited by capital funds.

The Final Word

The advent of the year 2000, like death and taxes, is inevitable (and more predictable). Embedded microprocessor chips and associated software can cause problems at critical time points. For embedded systems, testing is the only means of determining if a problem exists; and even exhaustive testing may miss some hidden pathology. Some 50 million embedded systems exist world-wide, and perhaps only 5-8% may have problems; the question becomes is your equipment one of the 5%?

If your team has not begun a Y2K assessment program, the time to start is now.

About the author: James Bowen is Vice President of CompEngServ (<http://www.compengserv.com>) which provides Y2K services and the SitRep2200 emergency management software product.

James Bowen, Coordtek Inc., Suite 300, 19 Fairmont Ave., Ottawa, Ontario K1Y 1X4, CANADA. 613-722-3008. <http://www.sitrep2200.com>

Y2K and Schools

by Rick Tobin

Note: Below is an interview with Jerry Dalluge, Manager, MIS Office, Minneapolis School District, which has 50,000 students, 8,000 full-time staff and about 100 school campuses. The interview was conducted by Rick Tobin (see below).

Q When did you start working on the Y2K issue at your campus? **A:** In 1997. Much of critical applications software is being handled by outside vendors. CSC1 is one of our main vendors. They have software specialized for schools: accounts payable, receiving, budgeting, and all other financial applications including such things as stores and warehouses.

Q What is your role in dealing with the Y2K problem? **A:** Anything on the administrative side, all networking, operating systems, servers and hardware including mainframes.

Q Has your campus formed a team to address Y2K? If yes, who are the team members? **A:** Several teams were formed for different parts of the problem. Three teams were formed for specific mainframe applications: student records, finance applications, and payroll/human resources.

Q Are you focusing only on software problems, or are you also looking at embedded chip problems, facility impacts, outside vendors, etc.? **A:** The District has looked at all of these factors. There is also a facilities team, separate but cooperating with the computer operations teams.

Q Did you use any outside assistance such as consultants, software, other schools or Web sites? **A:** The District was overwhelmed at first by the input from consultants. It became clear that the District would get the basic focus through cooperation with consultants, but much of the

work had to be done within the District. ...

Q What are the biggest issues your campus is facing because of Y2K? **A:** Critical applications must be covered first: payroll, grants, financial processes and networks. But no one in the country can guarantee that any operation is 100% Y2K compliant — but we can deal with the little that isn't because of the work we've done ahead of time.

Q Have you already identified critical operating systems and prioritized them for recovery activities? **A:** Yes, that was one of the first things the teams completed.

Q Have you done any actual testing of system software or any hardware to date? **A:** Yes. The financial and student accounting system will be tested this December 1998. This is critical because these computer systems start registering students early next year for the school year 1999-2000. If other school districts have not thought about this they may be surprised.

Q Any suggestions for other campuses starting the Y2K process? **A:** Do not underestimate the amount of time this will take. If you have old software, don't try to reengineer it because in many cases it will take more than a year to fix it.

About the author: Rick Tobin, now President of TAO Emergency Management Consulting, earlier worked for the California Office of Emergency Services. He developed a Web site for campus emergency planning at: <http://www.disasterrecovery.net/>. The CAMPUSAFE site includes articles, boilerplate plans, checklists, information on product vendors, links to other Web sites, and the monthly newsletter where this interview appears. Contact: Rick Tobin (530-622-2815; e-mail: rtobin@fothill.net).

Talking to the Public About Y2K

Red Cross Issues Y2K Preparedness Checklist

NOTE: The text below reflects a few changes made to the brochure by the Red Cross in January, 1999, following its (and our) first distribution. If you have an earlier version, please replace it with this one.

The American Red Cross has stepped to the forefront of the public education effort at the national level by publishing a pamphlet for the general public on Y2K, covering frequently-asked questions and offering guidance on how to prepare. The checklist is reprinted below, with permission.

The full text of the brochure is on the Web: <http://www.redcross.org/disaster/safety/y2k.html>

Printed copies are available through local Red Cross chapters, and the national headquarters is considering numerous requests from outside parties to reproduce the brochures in large quantities.

From the American Red Cross:

Because no one can be certain about the effects of the Y2K problem, the American Red Cross has developed the following checklist for you. These are some easy steps you can take to prepare for possible disruptions. All of these recommendations make good sense, regardless of the potential problem.

WHAT YOU CAN DO TO BE PREPARED: Y2K Checklist

Check with manufacturers of any essential computer-controlled electronic equipment in your home to see if that equipment may be affected. This includes fire and security alarm systems, programmable thermostats, appliances, consumer

electronics, garage door openers, electronic locks, and any other electronic equipment in which an "embedded chip" may control its operation.

Stock disaster supplies to last several days to a week for yourself and those who live with you. This includes having nonperishable foods, stored water, and an ample supply of prescription and nonprescription medications that you regularly use. See *Your Family Disaster Supplies Kit* for suggestions.

As you would in preparation for a storm of any kind, have some extra cash or traveler's checks on hand in case electronic transactions involving ATM cards, credit cards, and the like, can not be processed. Plan to keep cash or traveler's checks in a safe place, and withdraw money from your bank in small amounts well in advance of 12/31/99.

As you would in preparation for a winter storm, it is suggested that you keep your automobile gas tank above half full.

In case the power fails, plan to use alternative cooking devices in accordance with manufacturer's instructions. Don't use open flames or charcoal grills indoors.

Have extra blankets, coats, hats, and gloves to keep warm. Please do not plan to use gas-fueled appliances, like an oven, as an alternative heating source. The same goes for wood-burning or liquid-fueled heating devices that are not designed to be used in a residential structure. Camp stoves and heaters should only be used

out of doors in a well-ventilated area. If you do purchase an alternative heating device, make sure it is approved for use indoors and is listed with the Underwriters Laboratories (UL).

Have plenty of flashlights and extra batteries on hand. Don't use candles for emergency lighting.

Examine your smoke alarms now. If you have smoke alarms that are hard-wired into your home's electrical system (most newer ones are), check to see if they have battery back-ups. Every fall, replace all batteries in all smoke alarms as a general fire safety precaution.

Be prepared to relocate to a shelter for warmth and protection during a prolonged power outage or if for any other reason local officials request or require that you leave your home. Listen to a battery-operated radio or television for information about where shelters will be available.

If you plan to use a portable generator, connect what you want to power directly to the generator; do not connect the generator to your home's electrical system. Also, be sure to keep a generator in a well-ventilated area — either outside or in a garage, keeping the door open. Don't put a generator in your basement or anywhere inside your home.

Check with the emergency services providers in your community to see if there is more information available about how your community is preparing for any potential problems. Be an advocate and support efforts by your local police, fire, and emergency management officials to ensure that their systems will be able to operate at all times.

A Government Employee's Y2K Personal Preparedness Worksheet

by Michael Martinet, Area Coordinator, Los Angeles County, California

In general follow the usual emergency preparedness guidelines that are found in information distributed by the American Red Cross, your local office of Emergency Management and FEMA. Treat preparation for a Y2K event as you would any other emergency situation. However, due to the unusual nature, and possible widespread effects, a few other things should be carefully considered to achieve a maximum state of preparedness for your family.

Any and all of these special considerations may be either appropriate OR unnecessary depending on how actual Y2K events occur. The fewer Y2K events that actually happen, the less important these suggestions may be. However, at this time (fall 1998) no one has really good estimates of what will actually happen as the different Y2K dates pass.

These suggestions are provided for the consideration of government employees, who are designated as disaster workers in declared disasters, and may need to take an extra measure of preparedness because of their responsibility under the law. These suggestions are not necessarily made for the general population. Communities and neighborhoods are always encouraged to work together to help and assist each other in times of emergency and uncertainty.

The items in this list are prudent precautions for disasters in general and decisions about personal safety should always be made within the context of events that are happening. These ideas for you to think about should not cause you to worry. The effects of Y2K problems are not likely to have a severe impact on society, and local conditions may vary widely, depending not only on

Y2K event(s) (if any) and other conditions such as local weather, traffic or other emergency condition.

1) If problems are anticipated with the regional electrical power grids, turn appliances and electronic devices off to avoid either excessively low power, or power spikes which may cause damage to electrical and electronic devices.

2) If you store a lot of frozen food, you may want to re-evaluate how much you could actually use if you temporarily lost electrical power.

3) On or after January 1, 2000 check smoke alarms and other electronic safety devices to be sure they still work properly.

4) If you have an electronically controlled garage door opener or security gate, know how to manually operate them if necessary.

5) Fire officials caution against the home storage of gasoline. However, if you do store extra gasoline, be sure to only use approved safety containers and store them away from any source of ignition. In no case should any containers of gasoline ever be stored in a dwelling, or garage attached to a dwelling.

6) If utilities are disrupted, use extreme caution in using portable heaters and/or cooking devices indoors. Improperly vented heaters or cooking devices will give off carbon monoxide. Carbon monoxide is a colorless, odorless gas. When carbon monoxide collects in a closed unvented space it is a silent and deadly killer. Always vent rooms if these devices are used.

7) Plan a low key New Year's Eve celebration with people that live near you. Due to the uncertainty regarding the availability of electrical power and communications which could both affect your

ability to safely travel, it may be wise to remain near home, particularly if you are subject to emergency recall.

8) In the closing months of 1999, avoid, if possible, making any major life transitions such as moving or the addition or deletion of services. If there are problems with billing records, your history of recent charges can help you to establish what your normal bill should be. If you do make any transitions, keep every paper record associated with that change in the event that there are Y2K problems with records.

9) If possible, carefully consider elective medical or dental procedures in the few weeks immediately preceding and following New Year's Day 2000. If there are Y2K problems with your doctor or hospital, they may be minor. However, even minor problems can cause unnecessary aggravation and frustration.

10) Gather together hard copies (on paper) of all important financial records and bills. If your bank, financial institution or merchant has Y2K problems with their billing system, you will need those copies of your records to sort things out. Also keep all copies of your payroll check stubs and your 1998 tax returns just in case the IRS sends you a tax bill for \$763,000.00 (or whatever) Store these important records in a place that is safe and free from potential water or fire damage.

11) Although many Y2K dates immediately follow the holidays, try to keep a sufficient amount of cash available for such essential purchases as gasoline, food, medicine etc., in case there are problems with ATMs or your bank account. Withdrawal of large amounts of cash is not advised. Begin now to set aside a few dollars each pay day.

12) If you or a family member are dependent on medicines, anticipate this need in the event that your health plans have Y2K

(continued on page 21)

Employee's Worksheet (continued from page 20)

records problems. Order a few days extra medicine if your prescription will run out immediately after 1-1-2000.

13) Plan to maintain the "status quo" as much as possible. Anticipate business as usual, and plan on a regular return to work or school on January 3rd. But also be prepared to shift gears if the situation warrants.

14) Devise a family communication plan to contact family that are away from home at this time. However, don't get on the phone at midnight on New Year's Eve to call family or relatives. If there are any incidents, emergency responders may need phones for emergency communications.

15) Avoid unnecessary travel. Even though airlines and trains may be in full operation, hotel, car rental and airline reservation systems may have Y2K problems that could ruin a trip.

16) If you have natural gas devices with electronic ignition, check these devices to be sure that they are operating properly. If you are unsure of their status, call a certified repair technician. If you smell gas, open windows and doors to vent the room(s), leave the building and then call your local emergency services.

17) Unless you have a truly life threatening emergency avoid calling 911. Emergency services may be busier than usual, and a non life threatening call will just add to the system overload.

18) Have a clear understanding with your employer regarding your duty status in late December 1999 and January 2000. Know under what circumstances you would be needed at work on an emergency basis and how to determine if such an emergency exists.

19) As for any emergency, have a flashlight and plenty of spare batteries. If at all possible avoid the use of candles or other lamps that use a flame for illumination,

as they are a potential fire hazard.

20) Credit reporting bureaus are required to provide you with one free credit report each year. After January of 2000, take advantage of this service to ensure that your credit is being properly reported. Call a credit reporting bureau for the correct forms.

Exercise care in making preparations for any emergency or disaster. Because no one has ever experienced something like Y2K, no one can say for sure what will happen. There are some organizations and individuals that are predicting gloom and doom, up to the end of the world. These are extreme views. The scenarios presented by these extremists are highly unlikely and extremely speculative. If you have questions regarding your personal preparations, ask the emergency manager for your organization, or contact your local office of emergency management. Be aware that as in any other situation of uncertainty, scam artists and confidence games will abound. As with any other emergency situation, calm, carefully considered action is the best course. There is no more reason to panic in the face of Y2K than there is for any other disaster.

This list may not cover all possible exposures to Y2K related risks. Each agency must review their local situation and make their own risk assessment.

Disclaimer: Any Y2k information in this site is made under the protection of the Year 2000 "Good Samaritan" law. The author makes no express or implied representations or warranties, and does not guarantee the completeness, accuracy or timeliness of this information. Use this information at your own risk and assume full responsibility or any loss resulting from its use. The author will not be liable for any direct, special, indirect, incidental, consequential or punitive damages or any other damages whatsoever, whether in an action based upon a statute, contract, tort (including, without limitation negligence) or otherwise, relating to the use of this information.

GartnerGroup Releases Report on Y2K Planning For Individuals

Urging individuals to take a "long-term view" of Y2K preparations, the GartnerGroup — a respected organization looked to often for Y2K information and guidance — concludes that "a 'bomb shelter' mentality is not called for. Preparing for the new millennium should be much like preparing for a storm that will last less than a week."

In its recently issued Strategic Analysis Report on Year 2000 Risk Assessment and Planning for Individuals (Oct. 28, 1998), GartnerGroup puts the bottom line here: "Individuals should prepare for limited duration, localized failures of services and infrastructure rather than an apocalypse. The type and number of failures will vary geographically and cannot really be predicted. Individuals should ensure that they have at least two weeks' salary in cash and up to five days' contingency supplies of key consumable materials (e.g., medication, fuel and food) that they might need."

The full report can be found on the Internet at: <http://gartner6.gartnerweb.com/public/static/home/00073955.html>

It summarizes survey results of the state of readiness of business and government enterprises, provides a template for assessing personal risks by category, and offers commentary on a series of issues: banking, stock market, insurance, travel, personal and community contingency planning.

The two greatest risks for most individuals, GartnerGroup concludes, are: (1) being employed by an organization that suffers damage because it is poorly prepared; and (2) "participating in panic actions." Panic, they imply, can be avoided if individuals and communities take reasonable steps, just as they would (should) for a hurricane or winter storm.

Jump-Starting Your Community

by Michael Grill, Captain/Paramedic, Sierra Vista Fire Dept, Sierra Vista, AZ.

Note: This article is one of many responses that came to the IAEM Internet discussion list when a rural local police sergeant wrote to ask how to help his community prepare, and how to tap into the early planning efforts of a local group. To join the discussion list, send an e-mail to Majordomo@new-focus.org with the message: subscribe iaem-y2k

I am a Captain/Paramedic in a community of about 40,000 in SE Arizona. Last May, I was in the same position.

I scoured the community for help...looking for a citizen who I could approach that was "plugged into" the community via Rotary, Kiwanis, etc. I found this individual one morning at the Racquetball Club, and approached him. I explained that I needed his help. He was enthusiastic and told me to contact another person who was as concerned as I — a retired Chief Information Officer within our community. I contacted her, and we started having meetings at the fire station.

The first thing we did [was] agree upon our purpose. We crafted a mission statement that said, in part, our goal was to create a Y2K safe haven within Sierra Vista. We also began sharing information we found on the Internet.

In October, one of us was invited to speak to a local Rotary meeting. There we announced we

were having a meeting in the city council chambers, and invited all. On our November 1 meeting, we had 50 concerned citizens. [I gave] a PowerPoint presentation designed to build awareness. Another member of our group spoke about personal preparedness. At the end, we had folks sign a roster, [so we could] keep in touch and disseminate information.

Our second meeting was November 29th. However, prior to that we asked the Mayor to proclaim November 27th as Y2K Awareness day in Sierra Vista. This coincided with a newspaper article, speaking on the local radio, and the production of a tape which included our first meeting (we had it taped, since our council chambers has the capability). The

tape was shown, and continues to be shown on local TV at various times.

Our third public meeting was held on the night of December 9th. By this time, our core group of three had grown to four. We found that we had a member of our community who had just relocated from the Medford, Oregon area, and had been involved in their community effort re Y2K. He is also our hospital's chief information officer. Following the Rogue Valley format, on the night of the 9th we introduced and asked for volunteers to staff eight Action Teams. [That] moment marked our moving from information and awareness into action.

That has been our community's experience up to this moment. One word of caution: Although I feel I am very aware of the Y2K issues after extensive research, writing articles for Fire trade journals, etc. I am not the City's Y2K Czar. That role was appointed by our City Manager to the MIS Department chair. Therefore, there was some concern that, as a fire department and city employee I was "overstepping" my authority by being involved with this group.

However, I have talked with our fire chief, and, as our department's planning officer, he gave me the green light to approach the MIS manager and offer my help — which he jumped at! Therefore, at the moment, I am our community's public relations officer regarding Y2K when interfacing with the citizens' effort, which is ironic, because I am one of the three folks who initiated that citizens' effort.

About the author: Michael Grill, Captain/Paramedic with the Sierra Vista Fire Dept. in Sierra Vista, AZ, has been in the emergency services field since 1985. He teaches at the National Fire Academy (NFA), and is enrolled in the NFA's Executive Fire Officer Program. He holds a B.S. degree, is working on a Masters in Organizational Management. Contact him by e-mail at mtgrill@primenet.com.

Y2K Preparedness Is a Grassroots Movement: What Others Are Saying

... the government types don't quite know how to deal with citizen activists. I encourage us to all work together. Community preparedness will come from an educated public working together with government and the private and civic sectors to build resilient communities. — *Steve Davis, Montgomery Co., MD*

As of 1/1/99 my office is directing all of our energy into Y2K preparedness....We will need all the help out there to help our community prepare and that's where the grassroots efforts could help us. — *Phyllis Mann, CEM, IAEM President-Elect*

THE STONEPROOF BED®

Amazing 1 1/2" mat supports person weighing over 250 lbs.

- Comfortable Emergency Relief Personnel / Shelter Bed
- Compact / Portable
- Folded 7" x 28" x 19"
- Open 1 1/2" x 28" x 77"



"Comfort in the Field"

- 100% Water Resistant Nylon over Fire Retardant Foam
- Color: Royal Blue
- Price \$35.95 plus shipping (\$5 per case)

TO ORDER CALL
STONE PROOF® Toll Free 888-786-6773
www.brazosnet.com/biz/stoneproof/
US Patent # 5,726,067

SURVEY ON Y2K

The following survey was posted on the IAEM Web site (www.iaem.com) to help FEMA assess the state of readiness of local government and emergency management organizations. We are providing it here for those who do not have Internet access. If you have not filled this out online, please fill it out and fax your response back to headquarters at 703-241-5603. Thank you.

(Use the membership form below for your name and other information, if you're answering the survey.)

CIRCLE YOUR ANSWER

1. Are you aware of the potential problems facing all computer systems, called "Y2K", that involves your computer's ability to accommodate the change to the year 2000?

YES NO Don't Know

2. Is your organization actively working to ensure that its computer systems are able to deal with this potential problem?

YES NO Don't Know

3. Are the computer systems in your organization currently fully prepared to successfully accommodate the change to the year 2000?

YES NO Don't Know

On a scale of 0 to 100, where 0 might represent no Y2K preparedness in your community and 100 might represent completion of all preparedness activities, please give an estimate for each of the following:

4. Y2K compliance and operational readiness of your community's emergency management program, equipment, communications, activation and warning systems, emergency operations center, 911 systems, and other related operations:

0% 25% 50% 75% 100%

5. Degree of cooperation between your community's emergency management organization and other agencies in the community on Y2K activities:

0% 25% 50% 75% 100%

6. Degree of interaction between your community's emergency management organization with State organizations and with county and local emergency management organizations on Y2K issues:

0% 25% 50% 75% 100%

7. The extent of operational readiness of local jurisdictions:

0% 25% 50% 75% 100%

8. Availability of emergency preparedness guidance, information, or assistance in order to meet your community's needs for Y2K preparedness:

0% 25% 50% 75% 100%

These questions may require a longer answer, and a separate sheet of paper.

9. Do you know of successful or model state or local Y2K initiatives that can be shared with the entire emergency management community?

10. Do you know of any unique problems or issues facing your community related to Y2K compliance?

11. Do you know of any issues related to Y2K progress in FEMA's two specialized emergency preparedness programs, the Radiological Emergency Preparedness (REP) Program and the Chemical Stockpile Emergency Preparedness (CSEP) Program?

12. Your Comments or Questions?

If you answer nothing else, please let us know this: If you do not have access to the Internet, how can we help you stay informed about Y2K?

What information do you most need?

I WANT TO BECOME A MEMBER OF IAEM!!

Pay annual membership fee of \$100 (or \$250 corporate membership).

Fill out this form and mail with your check to IAEM, 111 Park Place, Falls Church, VA 22046-4513

Name _____ Title _____

Organization _____

Mailing Address _____

City/state/zip _____

Phone/fax _____ E-mail (if available) _____

☐ I can't join now, but send me information on the 1999 conference in Louisville, Kentucky, Nov.13-16, 1999

E.M. CALENDAR

- Feb. 1-5 Association of State Floodplain Managers (ASFPF) National Floodproofing Conference, Baton Rouge, LA. Contact ASFPF (608-274-0123; F: 608-274-0696).
- Feb. 7-10 National Emergency Management Assn. (NEMA) mid-year meeting, Washington DC. Web: www.nemaweb.org
- Feb. 7-10 State & Local Emergency Management Data Users Group (SALEMDUG) conference, New Orleans, LA. Contact Steve Burr, LA (504-342-1586).
- March 13-16 IAEM Mid-Year Committee Retreat, Emergency Management Institute, Emmitsburg, Maryland.
- March 22-24 Disaster Recovery Journal (DRJ) spring conference, San Diego, CA. Contact DRJ (314-894-0276; fax: 314-894-7474. Web: <http://www.drj.com>
- March 30-April 1 Partners in Emergency Preparedness 1999 Conference, Bellevue, Washington. Contact: Washington State Emergency Management (253-512-7046; e-mail: j.vollmer@emd.wa.gov
- April 21-23 Contingency Planning & Management conference & exhibit, New Orleans, LA. Contact WPC Expositions (908-788-0343, ext.135; F: 908-788-9381). Web: www.ContingencyPlanExpo.com
- April 26-28 Fire-Rescue Med, International Assn. of Fire Chiefs, Las Vegas, NV. Call 703-273-0911 or www.iafc.org.
- May 7-12 National Disaster Medical System (NDMS) Conference, Washington, D.C. Contact NDMS at 1-800-USA-NDMS and press the "star" key; or e-mail at ndms@usa.net, or on the Internet at www.oep_ndms.dhhs.gov

E. M. JobLine

Ft. Worth, Texas. Seeks Assistant Emergency Management Coordinator (B29). Annual salary \$36,612-54,924. Highly skilled professional to perform administrative work in the planning, coordinating and implementation of the City's Emergency Management Program. Requires equivalent to a Bachelors degree in Emergency Management, Public Administration or Business Administration, plus three years of increasingly responsible Emergency Management Experience. Prefer Office 97, Emergency Management software applications, EOC equipment management, computer mapping, supervisory experience. Send resume to: Fort Worth - Tarrant County Emergency Management Office, Attention: Gregg S. Dawson, 1000 Throckmorton Street, Fort Worth, TX 76102. FAX 817-871-6180; Phone 817-871-6173. Closing Date: January 29, 1999.

IAEM
National Headquarters
111 Park Place
Falls Church, VA 22046-4513

Mr. HORN. Well, we thank you for your ideas. Now let's discuss them. Vice Chairman Biggert.

Mrs. BIGGERT. Thank you, Mr. Chairman. I will start from the beginning.

Ambassador Heckler, I think that you have, you know, developed a plan with the super website. Would that include or is there now someone who would be capable of really dealing in the human services and the hospitals that would have the technical ability to be able to take what came in from other hospitals, synthesize it, and come up with something that could be readily found? I think that would be the most important thing. That it is not just a website where everybody pours in, but to be able to put it into some means that would be synthesizing what had taken place.

Ms. HECKLER. This is why the administration would have to be conducted by someone with the medical expertise. But the chairman referred to the Cleveland Clinic, which is an outstanding institution. Many of the outstanding institutions are doing everything possible and doing a great deal, but is your county hospital in your own congressional district aware? There are so many different websites now that one could spend an age looking for the right information on a specific piece of equipment, for example.

The need for the super health care website is simply pulling that together, and it would have to be administered. That is why I suggested it could be under the aegis of NHS or some designee of the Secretary of HHS, but the medical expertise would have to be there. The amount of testing that is going on now in the major institutions is revealing the weaknesses of the system, and there are weaknesses. Even with the certification, the embedded chips in so many medical devices can mean life or death if the wrong record is provided because the computer has crashed, the wrong person is treated, et cetera.

The medical expertise is essential, and the delivery of the information through a sophisticated technological world-class group that can provide it immediately on the site, because the information has changed, and there is so many thousands of particular products, particular situations that need to be reported. So you are absolutely right, we have to have this.

And I happen to sit on another—wearing another hat on a bank board, and I see in the bank on the audit committee, we are spending half the time of the committee on Y2K, on specific programs, and the financial institutions will be ready. But what we learned because there are regional collaborative arrangements from all the banks, and when a software package arrives with a flaw, and they do even though the manufacturer believes or the producer believes that it is perfect, they learn that it does not work at all, and then one bank will alert the producer, and the patches are put in, and every single software package has all of these patches so that you need both the medical expertise and the technological expertise to put this whole thing together in the right way.

But there is not a lot of time. Dealing with your medical problems is simply not something you can prepare in the way that you can put your flashlights in the back seat of your car or have your stash of 30 days of food or 7 days of food. Your medical emergencies arise, and the technological credibility, the integrity of the system

is under a most unusual threat. And that is why, frankly, dealing with this problem now is essential. We are late already, and there is no way the smaller hospitals will be able to cope so that it is necessary not merely to study the problem. We are past that. There are steps that can be placed, and it is combining those two.

Mrs. BIGGERT. Mr. Humphrey, you pointed out about the services of local government, and you said that in your assessment of the interruption risks, that it was going to be a larger-scale problem probably than we would expect. And I think most of all of us are used to emergencies. I know in my State or in my hometown we had the local phone company and the wire—we had an installation there, it burned to the ground, and in our town we were without any phone service for over a month, so people got pretty used to going down to the little phone booth that was the emergency phone booth that was set up. And fortunately it was about the time that cell phones really came into their own and certainly were increased a lot there. And that was a lot longer than we would expect an interruption of service.

And what I think is the problem, or what I see is the perception is that something can fail in this, and we have no idea that will come back on. When you have a phone company and the wires burn down, you know that they are going to fix the wires, and they are going to be able to come in and actually reattach, connect the fiber optics and they will be able to solve that. But with Y2K, since we are not going to know what is going to happen until that actual date, that how long there will be some interruption in service, and I think that is the fear that people have, rather than just that it is another emergency, it is one step further.

So, I guess that we need to know that the testing is so important, that things will work. But there still is that final hour when that turns over of what is actually going to happen. And I think that you are absolutely right to be prepared in every way we can, but I think that is why we have these hearings, to let people know that.

Mr. HUMPHREY. I think that is the key point that the lady at the end makes, and that is that not knowing what is going to happen means that we have to be prepared. And emergency management people have to make sure that their emergency management plan has Y2K problems in it that they know what they are going to do.

I was recently in Denver. Denver has dealt very well, I think, with the Y2K problem. But the one thing that they don't feel like they can do is provide warming shelters in the case of problems. They think that is a Red Cross problem. But the question I asked them, which they didn't necessarily want to hear, but I said, what happens if your nursing homes people begin to perish in your nursing homes? What are you going to do? And the point is they need to understand that. They need to understand what they are going to do, if anything. It may not be an appropriate role, but it is something that they have to consider, and it is hard, hard decisions to make.

Mrs. BIGGERT. Thank you.

Then going with that with Ms. Mann, I can understand that you don't want us to panic people, you don't want us—I think actually what we are doing is just the opposite, that we have held these

hearings to let the American people know and to know that there are concrete things that can be done, and that is why we have had these hearings.

You are absolutely right. I keep my boots most of the time, or I send one of my staff home to get my boots because I can't get out of the door. But there are emergency matters that you deal with and alternatives the way that you deal with the problem. But I think that what we don't want to have happen is that 3 days before this clock turns over, or 2 days or 1 day or at that time and say, well we have got a problem, let's just use our emergency measures, because that is not going to work, that we do have to be ahead.

We have had airlines that have come in and said that their executives are going to be in the air on January 1st because they are confident that their systems are going to work. I don't think that I want to be in the air on January 1st either, but that is up to everybody. But I think that with the articles that we have seen in the paper, the more exposure that there is to this, that people will get ready and not panic and go out and try and buy the supplies, the flashlights, the last couple of days.

So it concerns me that I think that this is what we have been trying to do, or that there have been articles about bank statements, making a copy of your bank statements ahead of time so that you have all of that because you may not be able to do that on that day. I think that you are right to be prepared, but I think that is what we are purporting to do here in these workshops and everything.

Ms. MANN. At the same time though, and this is what we see at the local level, is that we take one step forward and two steps back. So, for instance—and I wasn't going to use this analogy, but I will today, it is in my bag, and I will show it to you at the break. I was at the beauty shop getting ready to come to Washington, DC, coloring my hair so that you couldn't see all the gray, and I was sitting there reading a travel magazine, which I never read. I enjoyed it because it was about millennium traveling and how you can go on a cruise ship and go here and go there and how the FAA says that everything is just A-OK. Then I go back to my office and then I open up my mail, and there is my Emergency Preparedness News, a very reliable piece of information that I receive on a monthly basis, and it is citing Chairman Horn, and he is talking about the FAA report card. And this is what is happening at the local level, the FAA report card was not an A. In the travel magazine it led us to believe that it was an A. And this is what the American people away from the Beltway are experiencing is this inconsistent messaging.

So what I am saying is that there is nobody at the national level who is leading the preparedness charge. Mr. Koskinen and his team are doing a great job getting everybody ready with the infrastructure. At the same time we have not heard the President or the Vice President of the United States sitting down with the American public and saying, let's get ready just in case. We are a self-reliant system. We know that we have sustainable communities. That is the model of NACO is sustainable communities, but you at least have to tell them at a consistent messaging.

And you are absolutely right, we don't want to panic people, and we certainly don't want them filling up their gas tanks on December 31st; but what is wrong with saying to the Nation, let's keep our gas tanks full from October on? I mean, those are the types of messages that we are talking about. There is nothing wrong with saying that just in case.

But if you don't say it here—and all the hearings and all the task forces that you have going is for your infrastructure. This does not get out to the American public. I will tell you what gets out to the American public, and I consider this a national phenomenon that I think we should be studying. We couldn't get you ready for a hurricane because we see you shopping at the grocery stores as soon as the hurricane warning comes. And we couldn't get ready for a tornado. There they are stranded with nothing on their backs because they didn't do anything with their tornado kit. But for some reason Y2K is turning people on, and we are not seizing this opportunity. We are not making the direct connection between doing without—a potential doing without services and getting yourself prepared.

The government—and I mean here in Washington, DC, I can't wait to see this, but I am going to tell you at the local level I am not there to give you a glass of water. I will make sure that water is available to you that you can go get, but if there is no water, then you will have to go get it yourself through a government system. But that is not what you want to do. Most Americans don't want to do this.

So this is why I am saying, at your level here in Washington, DC, who is the national leader on Y2K? Who is telling the citizen—not the infrastructure, not the hospital, and not the utility, and certainly not me at local government—to get ready? Who is out there telling them to get ready? And that is what I think we are missing is the national leadership and advocacy for the issue.

Mr. HORN. If I might, if you would yield to me a minute or so, you are absolutely right. We have written the President. We have personally talked to him repeatedly, and said, you need to do a chat just like Franklin Roosevelt would have done, a fireside chat, and communicate with the American people about this, because otherwise you are going to have a real run on banks, and you will have nutty things done by nutty people that are trying to set the example of what they think is protection.

I looked at every single journal that came into my office the last 2 months, and slowly we are getting awareness that there is a problem in just the last 2 months. Finally, tomato growers and everybody else, their magazines are starting to talk about Y2K.

Senator Moynihan wrote the President many years ago and didn't get an answer. It took him about a year to answer me, and they finally appointed Mr. Koskinen in February 1998. We started our hearings in April 1996, and if we had been in the executive branch, we would have done it in 1989 when the Social Security Administration did it on their own. And I have cited the case many times, the Federal Highway Administration within the Department of Transportation, a very able woman programmer laid it all out for them in either 1987—in 1989, and they just laughed it off. And to show you how screwed up the Department of Transportation was

and maybe still is, that idea and that problem never went up the hierarchy so that the Secretary could deal with it. And obviously in any room of the top administrators within Transportation, one of them is the Federal Aviation Agency, and that is what should have been done. It hasn't been.

There has been very little leadership in the executive branch. Mr. Koskinen is doing the best he can, but the President of the United States any time he wants can get airtime, TV time, radio time, you call it. When he finally held his first meeting, he asked me to send him a few words and paragraphs, which I did. It was before the National Academy of Sciences. Well, they are the last people in the country you need to reach to because they know all about it, and they are scientists, and they are experts on computing and all the rest.

It was a good speech. Then when was the next one? The next one he got, oh, just 2 months ago maybe he declared that Social Security was OK. Well, we declared that from the beginning. We were giving them As, A-pluses, so forth. And our report cards did show that Social Security was the first to clear the decks, if you will, in their computers so that they would function, and there would be—of the 43 million customers and perhaps 50 million checks that pour out, there would be no problem with Social Security.

Then we found the Financial Management Service of the Department of the Treasury, they were not conforming, so we worked with people, goading them on. The legislative branch is simply an oversight branch. Our Majority Leader will be preparing kits for every Member of Congress so that when they go home, they will be able to understand these issues, and, of course, if 435 Members can at least hold one town meeting somewhere in their district, some of that word will be out.

But you are absolutely right. This is an executive branch problem. They have never run with it. They sort of—I call them the Perils of Pauline. You know, Pauline—you would have to be my age to understand that.

Ms. MANN. I may not be your age, but I like television.

Mr. HORN. She is strapped on the tracks with ropes, and the train is coming and all of that at the Saturday flicks in Hollister, CA. The next thing somehow she would escape from the ropes, and she is OK. But that is what it was, tremendous procrastination in the executive branch. They should have taken this from day one and educated people.

Without question, the FEMA operation, which is basically very well run, and your local emergency manager counterparts, that is where the information is going to have to come. And there is no magic bullet out of money from the Federal Treasury. We cannot even fund anything around here because of the caps that have been placed on it. And with the demagoguery going on by the administration and the Democratic leader in the Senate on what you have to do with the surplus, there is no money for anything else. It will all go into Social Security. And we will do just what they want, only we are going to do it better. If they want 62 percent in Social Security, we are going to put 100 percent in, et cetera. So there is not any loose change around here. But the communication can be done by your counterparts.

Ms. MANN. And I think that was one of the things that decided—made the decision for me to be here today is that at the end of these 2 days, at the very least what we should do is decide on a national consistent message that we keep pushing out and we don't deter from that message. This is why people and the Red Cross, when they teamed up many years ago and came out with one citizen message, how to prepare a citizen for any emergency or disaster, the 3-day kits, et cetera, that is what we are going to do.

I would like to comment on the Social Security because I work very closely with our local Social Security. When he said he got an A on his report card, and I naively asked him what did the Post Office get? Despite everything else, I think that—you think that everybody is going to wire transfer? But a few people still get their Social Security checks—that are delivered by the Post Office. What kind of grade did they get?

Mr. HORN. They didn't get a very good one. If it wasn't so sad, it would be laughable. But when we were grading all the 24 Cabinets and independent agencies, one of the questions we asked from the beginning was what is your contingency plan? With many of them it was the Post Office, because if you couldn't get the checks cut and sent by electronic mail, which is our legislation, and we think it ought to be done that way, but you are right, there are a few people who say, I want to feel that check, well, it is too bad because people rob them of their checks, and if they went directly into their bank deposit, one, it would be there, and, two, several days you could use that money ahead—between getting the check in the Post Office, walking down to deposit the check and all of that.

But you can't change some people. And I understand that. I grew up in the Depression. I know what my mother would have wanted. She wanted to see that check, too, because we almost lost our house in the Depression, and we lost everything else, but our house was firm. So people that have gone through that experience don't trust banks, don't trust government, and you can understand why.

Ms. MANN. Absolutely.

Mr. HORN. So we have got to educate them. Everybody we have been in our six field hearings in August in Indianapolis and Cleveland and Chicago and New Orleans and Dallas and so forth, we made the point, look, it would be prudent to have a month or 2 months of supplies of food that are edible, and if you don't have the gas, you don't have the electricity, or whatever it is, you are going to have to get some way to cook, which there are ways as you know, sterno and others, and try to get the food warm. You will not have your refrigerator working and so forth.

So we have tried to be prudent, not getting headlines. We had one once in a while a few years ago where they talked about planes dropping from skies. That is nonsense. The fact is the administrator, who is a very able person, has had to play catch-up because, again, her staff let her down once she was confirmed, so they are playing catch-up. I think they will be OK. The administrator of FAA has the authority under the law to ground planes any time of night or day for safety. As you know, most of us do not take off in the East and land in the West unless they are very sure we have got a spot to come right in and not go circling around the cities,

which we have done around Chicago for years, and you shoot right into Los Angeles. If you leave Dulles, you know you will be there X hours and minutes and seconds away.

So it is an executive job, and we are going to bring in a proposal for an Office of Management, which is what the President needs. This is a management problem, not a technical problem. I mean, techies can work on it, but somebody has got to lay it out and say, "hey, this is what we have to do in this time period." And what we finally did, just by a series of hearings, is shock them into a little action. But, again, the President has to communicate it, and he hasn't done a very good job at it.

Ms. MANN. Well, then I think we are here in Washington, DC, this week to help him. Because one of the things that we can do, which would be so simple nationwide since you already do a report card, we can do a monthly preparedness checklist that every citizen gets, nationwide. It is printed in the paper, just like you do your report card, and it becomes part of the press release packet.

Mr. HORN. Right. And we have urged—when we went to these various cities, we urged city managers and others, if you have a public utility—in the case of Long Beach, they have their own water company and gas company and so forth within the city government, on the bill, just—but a whole list of things you ought to be prepared to do. That communicates with a lot of people. Ballots that go out, the registrars could put these things in at the county level, in our case, in California.

So there is a lot of ways to reach people. And, of course, you are going to get tired of reaching them and think they know, but when you are tired is when you start over again.

Ms. MANN. Exactly.

Mr. HORN. And you are just getting there, and I think your counterparts can do a lot of good here to make up for the vacuum on the executive side of the Federal Government, and we will be glad to give you all the help we can.

Mr. Humphrey, I do want to put that "Y2K and You" in this hearing record, if it is not a problem for your people, and we ought to have cross-references on the websites of where people can download it and all the rest of it, which would be worthwhile.

[The information referred to follows:]

A Guide to



ACKNOWLEDGMENTS

On a date certain in the future (January 1, 2000), many computers and their embedded chips, at the heart of a community's infrastructure, will be unable to recognize the actual date. As a consequence, data transmissions, public safety operations and financial transactions that normally occur in communities may be at risk of performing irrationally, or not performing at all. This paper describes how local officials can demonstrate leadership to mitigate the potential negative impacts of this issue in their communities.

This paper was made possible through the contributions of many who conducted research and participated in discussion groups. A special thanks to Clint Page, who authored the book for PTI, to PTI's Urban Consortium Telecommunications and Information Task Force (UCTITF) for its vigilance and work in identifying critical issues of importance to local governments, and to PTI's internal Y2K Team.

Public Technology, Inc., is the non-profit technology research, development, and commercialization organization of the National League of Cities (NLC), the National Association of Counties (NACo), and the International City/County Management Association (ICMA). PTI's mission is to advance the development and use of technology in local and state government.

PTI's Urban Consortium (UC) is a special network of the nation's largest cities and counties that focuses on new solutions to common concerns. The UC provides a creative forum for elected and appointed officials to identify practical ways to improve the provision of public services while generating new revenue opportunities. The UC addresses the critical needs of large local governments through five technology task forces: Energy, Environment, Information and Telecommunications, Transportation, and Public Safety. The task forces are staffed by representatives of the UC member cities and counties who are experts in these arenas and have extensive experience managing related practical challenges in their jurisdictions.

UC members act as urban laboratories to develop and test solutions and share new technologies and management approaches with other local governments, both large and small, across the U.S.

TABLE OF CONTENTS

Year 2000 Problem	01
A Mandate for Leadership	02
Public Safety	02
Effect on the Local Economy	03
The Local Economy and Local Government Revenues	04
Legal Liabilities	04
On the Technical Side	05
The Cost of Coping	07
In Conclusion	07
Coping With the Year 2000 Problem: A Checklist	08
Y2K Internet Resources	10
Glossary	14



INTRODUCTION

The Y2K challenge is real: Unless we take action now, our communities may be severely weakened on Saturday, January 1, 2000. The local economy may falter, public safety and health may be compromised, and our citizens may become frustrated and begin to look for places to lay the blame. The Y2K challenge will stretch and test the mettle of local government leadership as no other challenge has in recent years.

For these reasons, Public Technology, Inc. and its sponsoring organizations, the National Association of Counties (NACo), the National League of Cities (NLC), and the International City/County Management Association (ICMA) have launched "Y2K & YOU," a campaign designed to increase awareness of the problem and to provide, through this tool kit, dependable resources that local governments can utilize as they develop their remediation strategies.

It is our hope that Public Technology, Inc. can be the premier partner with local government in facing the Y2K challenge.



Costis Toregas
President,
Public Technology, Inc.

YEAR 2000' PROBLEM

Call it the Year 2000 problem or the Y2K problem and it sounds like a technical problem; call it the Millennium Bug and it sounds like an end-of-the-world science fiction thriller. Whatever the name, however, the problem is real.

Nobody is sure what computers -- or for that matter, any of the countless devices and systems controlled by microchips -- are going to do at the stroke of midnight when December 31, 1999 rolls over to January 1, 2000. Some computers and systems will make the change smoothly; while others may behave erratically or even stop working.

Why? During the early days of computing, when processing power and storage capacity were puny compared to what we're accustomed to today, programmers and engineers decided to reduce the space needed to store a date by recording only the last two digits of the year: Valentine's Day 1980, for example, was stored as 021480 (they also saw no reason to store the slashes between the month, day, and year). When this century ends and the new one begins, however, that will become a problem. Computers won't know the difference between Valentine's day, 1901, and Valentine's Day, 2001; they will both be stored as 021401.

Traditional mainframe computers, which are dominated by older programming languages -- COBOL, FORTRAN, and others -- will certainly be affected. These programming languages are where the problem has its roots.

But virtually anything and everything that relies on embedded process controllers (microchips) will be affected. The first thing that comes to mind is the personal computer. Many older IBM compatible PCs won't be compliant, but machines sold after 1997 generally are compliant. Macintosh computers don't have a Year 2000 problem, because they store the date as a long number based on the number of seconds since January 1, 1904. This system handles the 2000 just fine, but apparently has its own problem at 6:28:16 a.m., February 6, 2040 when the total number of seconds since January 1, 1904 will be too long a number for the allotted storage space.

Computers and systems will make the change smoothly; some will stop working; others will behave erratically.

Microchips also control security elevators and doors, telephone switches, traffic lights, and electric utility substations, as well as small household and office appliances. Industry experts predict that of the 25 billion chips in electronic components, only about 2 percent will fail, because most of these devices lose track of their timing functions. But there's no way to know which 2 percent. In many (perhaps most) cases, the device will just stop working. Elevators will descend to the basement or go into security mode; VCRs will work but you won't be able to program them.

The problem is not just one of hardware and chips. Any software that stores and uses dates -- spreadsheets, databases, financial management software of all kinds, human resources software, and a host of other programs -- is vulnerable to the Year 2000 problem. By extension, so are all the data files used by those programs.

In short, anything electronic that depends on dates or on calculations involving dates is vulnerable.



[E E E E E E]

YEAR 2000 PROBLEM***You're susceptible if:***

- You have any central or mainframe computer that stores data vital or important to your local government.
- You have a local area network (LAN) over which data and files are shared, thus allowing dates to be entered in a variety of ways.
- You use personal computers. The device inside the PC that retains date and time when the system is turned off often cannot store a four digit year. It will give your operating system an invalid date after January 31, 1999 (perhaps something like 1/1/00).
- You electronically store any data with a two-digit year.
- Your telephone system has programmable switches. Phone systems are almost all controlled exclusively by software, and if the date clocks are not Y2K compliant, the whole system is not Y2K compliant.
- You have automated security systems with computers that automatically lock and unlock doors and elevators at night, open them in the morning, and keep them locked on holidays and weekends.
- You use global positioning systems (GPS) to locate emergency vehicles. GPS devices determine distance by measuring how long it takes to get a signal from several satellites in stationary orbit. On August 22, 1999, many will fail to calculate time correctly.
- You use automatic data collection systems, found, for example, on city-owned electric meters.

A Mandate for Leadership

The mandate for leadership by local officials is compelling. Should systems fail, the frustrations and ire of citizens will be directed at city and county leaders. Unfortunately, the liability will extend beyond the walls of city hall. To ensure that the public is as prepared as it can be, local officials need to enlist support from and galvanize the community at large: business, industry, civic organizations, schools, and neighboring jurisdictions. It is not just a local government challenge: It is a problem that may negatively affect everyone if not properly managed. Local elected officials are well positioned to capture the attention of and form strategic partnerships with stakeholders whose contributions help make communities work. Community forums, business roundtables, media strategies, and even personalized contacts will all be needed to ensure that the community is informed and prepared to respond to Year 2000 problems.

Public Safety

The first thing you may notice on January 1, 2000, is that the computer on your desk may tell you that the date is January 1, 1980. Or it may give no date at all. Looking beyond the computer on your desk, and even beyond those on desks throughout local government offices, there are some far-reaching ways that the Year

2000 problem will affect your city or county. Two of the broadest, but closest to home for local elected officials, are public safety and health and the local economy. Local governments are directly responsible for the former and play an important role in the latter.

Today's criminal justice system -- from the police to the courts -- is heavily dependent on electronic technology. Police departments use microwave communications systems, criminal records systems, offender information (including fingerprint identification) systems, computers, and telecommunications equipment in police vehicles. All are vulnerable. In the courts, systems for tracking pardons and paroles, scheduling court action, and documenting evidence are vulnerable, along with the normal data processing systems. Corrections records are vulnerable, as are the electronic systems that provide security and environmental control in police stations, courthouses, and prisons.

Emergency response systems are vulnerable through their reliance on telecommunications and data processing, of course, but they also have a less widely known problem related to the global positioning system (GPS) used to keep track of the whereabouts of police, fire, and other emergency vehicles. The GPS system may fail in August 1999 because of a date-related processing problem of its own.

Transportation control systems for streets, highways, mass transit systems, and railroads, to say nothing of air traffic control systems, are another vulnerable area. Traffic lights, freeway on-ramp controls, traffic monitoring, and rail switching systems are all based on chips that could fail entirely or become dangerously confused.

Utilities are particularly vulnerable. Water and waste treatment systems are controlled by automated systems that rely on computers and by flow control devices that rely on chips; problems with hardware, software, or chips could lead to system shutdown, or groundwater contamination. Power companies use computer systems to control operations and manage the distribution of power. Y2K problems with the hardware and software could lead to system failures. And of course, like any business, they depend heavily on computers for billing, personnel, payroll, and other general operations.

Effect on the Local Economy

Any local business could have Y2K problems; many of them will. In many cases the effects on one business or organization could cascade throughout an entire community. Banks, credit unions, and other financial institutions might not be able to record the date of deposits and withdrawals or correctly calculate interest on loans or savings accounts. Payrolls could be hopelessly snafued if human resources departments could not calculate wages and salaries, withholding, vacation time, and the like. Accounting departments would be unable to process accounts payable and accounts receivable. Inventory would become unmanageable. Local telephone systems could shut down because their chip-driven switches went into some kind of silicon limbo, their billing procedures could be confused, and automated voice mail systems could handle calls incorrectly.

The infrastructure of computers in communities is such that each depends on the operation of others. If cities and counties are concerned only with fixing their own computers, they need to begin taking a proac-

YEAR 2000 PROBLEM

tive leadership role in helping their communities prepare as well. Payment to one entity is dependent on revenue to another. If electric companies cannot produce electricity, many parts of the community will shut down; if they cannot generate revenues, they will be unable to make transactions with other businesses. There could be an avalanche of negative impacts from merchants' inability to charge for services, including the dire prospect of economic downturns, business shutdowns, and layoffs.

The potential effects of the Year 2000 problem seem likely to create an environment in which legal action will thrive.

At the same time, security systems in private as well as public buildings, including alarm systems, automatic door locking and opening systems, and identification systems could operate erratically or not at all, putting people and goods at risk and disabling authorized access to important functions.

Programable elevator systems could go into weekend mode on weekdays, or into weekday mode at night or on weekends, leaving buildings open; or could go into emergency or maintenance modes at the wrong times and leave buildings inaccessible.

Programable elevator systems could go into weekend mode on weekdays, or into weekday mode at night or on weekends, leaving buildings open; or could go into emergency or maintenance modes at the wrong times and leave buildings inaccessible.

The Local Economy and Local Government Revenues

Local government and local businesses are linked by a two-way exchange of information. Taxes, licenses, real estate information, development programs, and other city or county programs depend on the flow of information, and so do businesses. Ignoring the Y2K problem threatens that flow of information, and thus the health of the local economy and the fiscal health of the local government.

Local governments whose computer systems are vulnerable to Y2K problems face potential loss of revenues if they do nothing. Dayton, Ohio, for example, saw the Y2K problem as a threat to \$210 million a year in revenues from water fees, income taxes, and accounts receivable. The city plans to have systems installed sometime this year to keep its revenue streams flowing.

Tax bills could be overdue or not due at all, licenses could expire and not be renewed, building permits could go unissued, and so on -- and the link between local business and local government could become hopelessly tangled.

And beyond those are still other effects that local government and local businesses, too, need to consider, including legal liability.

Legal Liabilities

The potential effects of the Year 2000 problem seem likely to create an environment in which legal action will thrive. So far, with no lawsuits filed, there are no court decisions and no case law. But there will be.

Warren Reid, Encino, Calif., legal consultant specializing in Y2K issues, told clients in a recent white paper, "Failing to fix your upcoming Year 2000 problems can not only cause disruption and loss of market share,

productivity, and profitability in your company, but will expose the company and you to class-action lawsuits, possible loss of coverage from insurance companies, malpractice for professionals, and director and officer liability -- a grand slam!"

Several states have passed laws to protect private business and state agencies from just that kind of legal action related to the Y2K problem. Despite those efforts, and despite the fact that the Year 2000 problem is a technical problem with a technical solution, your city or county attorney should be aware of legal risks.

On the Technical Side

Solving the Year 2000 problem is not technically difficult, even for embedded microchips.

There are five recognized solutions to the Year 2000 problem:

- ① **Conversion:** The only fix that is a complete and permanent solution is also the most obvious: convert every date to a four-digit year, following International Standard Organization ISO 8601, adopted by the American National Standards Institute (ANSI), which calls for all dates to be entered as "yyyy mmdd." March 31, 1998 would be entered and stored as 1998-03-31. This approach offers a complete, permanent fix that will change all data records and every application using them. It is also the most intuitive fix. But it requires extensive program and file conversions. Every program in an application must be checked for significant data use and converted; then the entire application has to be converted from its previous form to its new form all at once. Existing data must also be converted all at once. This includes all active, archived, and security files. *Even a medium-sized local government or business could have millions of lines of program code, nearly any of which could use dates.* This approach will also demand a significant amount of new storage space, roughly a 7-percent increase. It will take the most time and is the most costly.
- ② **Fixed Windowing:** Creating a 100-year window such as 1936 and 2036 can give computers and software a way to decide which century is appropriate for a date. If the two-digit year is greater than 36, say 47 or 99, then the program assumes the century digits to be 19; if the two-digit year is less than or equal to 36, the century digits are assumed to be 20. This approach requires no change in data, but it provides only a temporary fix. At best, it buys some time. It works only until its appointed time runs out, and at that point it will require reprogramming.
- ③ **Sliding Windowing:** This is like fixed windowing, with one significant difference. The 100-year window is calculated from the current date. Each year the software using sliding windows will adjust (slide) the 100-year window one year forward. This approach requires no changes in data, only in date processing routines, and the same code can be used for many years. Production programs, for most applications, can be gradually converted, and they can adapt year after year without reprogramming. If the 100-year window is well-selected, it may be permanent and cheaper than ISO 8601. Thus, sliding windowing offers many local governments the fastest, most reliable, and least costly way of dealing with the Y2K problem.



[12 13 14 15]

YEAR 2000 PROBLEM

- ④ **Encryption:** It is possible to use binary arithmetic to compress dates expressed with four-digit years to occupy the same storage space as those with two-digit years. This approach gives the permanence of full date conversion without the need for more storage capacity, but it requires extensive reprogramming and is not intuitive.
- ⑤ **Encapsulation:** The Gregorian calendar has an interesting quirk -- it repeats every 28 years. Since the Y2K problem can be seen as a problem related to six-digit dates at the turn of the century, encapsulation simply resets to 28 years earlier. The computer and its programs do calculations based on a 20th century date and then add the 28 years back in for display purposes. This approach gives a quick fix for situations where source code is lost or time has run out. But it does not account for religious holidays that don't follow the Gregorian calendar. In the end, it may be useful only in embedded process controllers in which the actual year is not important but day of the week is very important.

A strategy for putting the appropriate technical fixes in place might look like this:

- inventory all automated systems and equipment;
- test to determine which will be compliant, and which will not;
- prioritize the results;
- find out what remedies to apply;
- determine which applications can be fixed on time; and
- develop contingency plans for those that can't be fixed on time.

But doing that is complicated by two factors.

One is that there are many related areas to find and fix. In numerous cases, application software was developed on a custom basis, or at least heavily customized, to handle local government business practices. These custom applications can be difficult to maintain, and some are too old to change. Even a medium-sized local government or business could have millions of lines of program code, nearly any of which could use dates. Invalid date comparisons could crop up in programs, training, embedded processors, and data. Beyond the computer hardware and software, too, there are all those other systems and devices that are controlled by microchips.

The other complicating factor is time. It will take time to make all the necessary changes. The inventory alone could take six to nine months for a medium-size organization and longer, up to twice as long, for a large one, according to some experts. And that's only the computers and software. Figure another three months to inventory all equipment that uses embedded chips. Once the code that needs fixing is identified, maybe 70 to 80 percent can be updated automatically. The rest will have to be read, a line of code at a time, by programmers, and manually changed. At an average rate of 3,000 lines of code a day, that is no quick job either.

But time is running out. With the Year 2000 right around the corner, we are all facing a deadline that can't be extended.

The Cost of Coping

Both the time and the money that it will take to solve Y2K problems in your local government or in your community will very likely be available only at the expense of other improvements and other projects.

It will require reprogramming, replacing, or retiring older "legacy" computing systems -- the mainframes and minicomputers that were the mainstay of computing before the advent of the personal computer. But it will also require that newer systems be checked as well as systems that aren't computer systems but use microchips -- elevator controls and security systems, for example.

The exact cost of doing that will depend on the size of the city or county and the extent of its use of information technology. Seattle estimates that it will spend more than \$50 million to reprogram major applications affected by the problem and replace the city's accounting system. Some cities and counties are fortunate to have recently launched major IT plans that will replace old systems with new ones in time to avoid the Year 2000 problem. In these cases, many of the Y2K compliance costs are covered by funds budgeted for system improvements in the overall city or county budget.

In Conclusion

The Year 2000 problem is a real problem, with serious impacts on local governments, local businesses, and local economies. Fixing the problem is not difficult technically; computer experts have been developing the solutions for some time and many of them are being implemented. But it will take time and money to make all the necessary changes in the computer hardware, software, data, and automated systems that are becoming essential parts of the modern city or county. It is essential, then, that local officials be aware of the problem and that they take the lead, not only in city hall but in the wider community, to make sure that the year 2000 will begin as free of problems as possible. The checklist that follows is, at best, an outline for action for local officials, local business owners, and the community. Above all, make sure that the operating mode for whatever you do is urgency, not panic.



COPING WITH THE YEAR 2000 PROBLEM: A CHECKLIST

TECHNICAL RESPONSES

- ☐ **Inventory systems.**
- ☐ **Test for compliance.**
 - Hardware
 - Operating systems
 - Custom code
 - Applications
 - Data interfaces
- ☐ **Analyze results.**
- ☐ **Prioritize.**
 - Critical systems that don't involve traditional data processing: traffic control, water-systems controls, etc.
 - Critical data processing systems: accounting, human resources, etc.
 - Systems whose loss would disrupt operations.
 - Systems whose loss would create minor inconvenience.
 - Systems that are extraneous and/or candidates for replacement.
- ☐ **Fix or replace hardware.**
 - Fix: requires appropriate technical skill.
 - Replace with compliant hardware: replacement is an expensive option, but it may be the only realistic one for many systems. It also becomes riskier as we get closer to 1/1/2000.
- ☐ **Fix or replace software.**
 - Fix the code: requires access to code and appropriate technical skills.
 - Replace with compliant custom or off-the-shelf software.
 - Outsource (at least temporarily) the process to a service bureau whose system is compliant.
 - Live with cosmetic problems or minor inconveniences until they can be finally fixed.
- ☐ **Fix or replace embedded systems and interfaces.**
 - Make sure that the same efforts to identify problems, prioritize them, and then fix or replace systems as appropriate are directed to automated systems in elevators, water systems, and building security systems.
 - Don't overlook interfaces with outside business partners.

What is a Y2K-Compliant Community?

A Y2K-compliant community is one in which all functions, both privately and publicly operated, within a local community will be operating and interacting normally into the year 2000 and beyond.

An automated system is Y2K-compliant when it will process normally, as it was designed, (i.e. without any extra processing, procedures, or other manual intervention) before, during and after January 1, 2000.

MANAGEMENT RESPONSES

- ☐ **Make the Y2K problem a priority for all city/county offices.**
 - Put someone in charge.
 - Make sure that IT professionals work with city/county department heads and business managers to help them bring their systems into compliance.
 - Larger cities and counties might create Y2K offices or task forces or other bodies.
 - Budget for solving the problem.
 - Have the city/county attorney research legal ramifications of the Y2K problem for your city/county.
- ☐ **Spread the word.**
 - Provide a central source of information on the Y2K problem and monitoring of progress for the whole city or county; a Web site, or a page on the city/county Web site, is a good way to do this. Make sure that all employees are aware of how it affects them.
 - Make sure that local businesses and organizations know that the city or county government is working on its Y2K problems.
 - Make sure that local businesses and organizations are aware of the Y2K problem and the need to become compliant.
 - Make sure that local businesses understand that they must be Y2K compliant in order to work with other businesses' computers and data as well as with local government computers and local government data.
 - Share information, through means ranging from brochures to a page on the city or county Web site.
- ☐ **Make operational changes within your offices.**
 - Use four-digit dates. Some software can handle the year 2000 if it's entered as four digits, and consistent use of four-digit dates will avoid confusion later.
 - Train staff to know where Y2K problems can arise and to spot them when they do.
 - Be prepared to replace what can't be fixed.
- ☐ **Make contingency plans for systems, processes, and data that can't be compliant in time; consider outsourcing (temporarily, at least) to compliant service providers.**

A WAY TO ORGANIZE YOUR Y2K EFFORTS			
	Programs/data Systems	Embedded Charts	Data
Awareness			
Solution			
Interface			
Contingency planning			



Y2K Internet Resources



Y2K INTERNET RESOURCES

ASSOCIATION SITES

Access Local Government. <http://www.al.gov.org/login/> - A private service for members of the International City/County Management Association (ICMA), the National League of Cities (NLC), and Public Technology, Inc. (PTI).

CPSR. <http://www.cpsr.org/program/y2k> - Computer Professionals for Social Responsibility (CPSR) Y2K Working Group.

DISA. http://www.mitre.org/research/cots/COMPLIANCE_CAT.html - Defense Information Systems Agency Year 2000 Product Compliance Catalog.

Federal Financial Institutions Examination Council. <http://www.ffiec.gov/y2k/impact.htm> - Gives guidance concerning Y2K impact on customers.

NIST. <http://www.nist.gov/y2k> - National Institute of Standards and Technology Y2K Web site.

Public Technology, Inc. <http://pti.nw.dc.us> - Keep up with latest news for local government by visiting this site frequently.

Reengineering Domain. <http://www.stsc.hill.af.mil> - An Internet site run by The Software Technology Support Center (STSC) from within the U.S. Air Force.

Standard for Year 2000 Test Certification. <http://www.software.org/y2k/index.html> - From The Software Productivity Consortium.

U. S. Federal Government Gateway for Year 2000 Information Directories.
<http://www.itpolicy.gsa.gov/mks/yr2000/y2khome.htm> - U.S. Federal Government gateway.

STATE SITES

Alabama. <http://agencies.state.al.us/y2k/index.html>

Alaska. <http://www.state.ak.us/foca/ekpages/ADMIN/info/yr2000.htm>

Arkansas. <http://www.dis.state.ar.us/y2k/y2kintro.htm>

California. <http://www.year2000.ca.gov>

Connecticut. <http://www.doit.state.ct.us/y2k>

Florida. <http://y2k.state.fl.us>

Idaho. <http://www2.state.id.us/itrmc/2k/default.htm>

Iowa. <http://www.state.ia.us/government/its/century>

Massachusetts. <http://www.state.ma.us/dls/year2k.htm>

Minnesota. <http://www.state.mn.us/ebranch/admin/ipo/2000/2000.html>

Nebraska. http://www.das.state.ne.us/das_cdp/rfp/rfp.htm

New Jersey. <http://www.state.nj.us/cio/nj2000.htm>

New York. <http://www.irm.state.ny.us/yr2000/yr2000.htm>

Ohio. <http://www.state.oh.us/y2k/> - What the State of Ohio is doing about the problem



Y2K INTERNET RESOURCES

Oregon. <http://www.state.or.us/IRMD/y2k/year2k.htm>
Pennsylvania. http://www.state.pa.us/Technology_initiatives/year2000/index.html
Tennessee. <http://www.state.tn.us/finance/oir/y2k/webindex.html>
Texas. <http://www.state.tx.us/Standards/>
Utah. <http://www.gvinfo.state.ut.us/sitc/yr2000.htm>
Virginia. <http://www.cim.state.va.us/cdc/INDEX.htm>
Washington. <http://www.wa.gov/dis2000>
Wisconsin. <http://badger.state.wi.us>

LOCAL GOVERNMENT SITES

Access Local Government. <http://www.algov.org/login/> - A private service for members of the International City/County Management Association (ICMA), the National League of Cities (NLC), and Public Technology, Inc. (PTI).
Albuquerque, NM. <http://www.cabq.gov/y2k/index.html>
Arlington County, VA. <http://www.co.arlington.va.us/ariccy/budget/thmtech.htm>
Indianapolis, IN. <http://www.indygov.org/cio/express/Jan97/yr2000.htm>
Montgomery County, MD. <http://www.co.md.us/year2000/>
Orlando, FL. <http://www.ci.orlando.fl.us/departments/y2kinter/y2k.html>
Portland, OR. <http://www.ci.portland.or.us/y2k/>
Riverside, CA. <http://www.ci.riverside.ca.us/riverside/year2000.html>
Roanoke, VA. <http://www.ci.roanoke.va.us/depts/cia/y2k.html>
San Bernardino County, CA. <http://www.co.san-bernardino.ca.us/y2k/>
Tallahassee, FL. http://www.ci.tallahassee.fl.us/citydh/info_systems/alt2k1.html

PRIVATE SITES

2000 Legal.Com: Year 2000 Legal Resources for Avoiding Y2K. <http://www.2000legal.com/index.htm>
 - A law firm providing "Legal resources for avoiding year 2000 business disruptions and reducing litigation exposure."
Audit Serve, Inc. <http://www.auditserve.com> - The Worldwide Connection for Audit, Security, Control, and Y2K Conversion Professionals.
BIOS Setup Information. <http://www.sysopt.com/bios.html> - A site devoted to technical information useful to Personal computer technicians.
Challenge 2000: Assessment. <http://boris.nfftd.co.uk/year2000/> - A UK vendor site.
CUNA Mutual Insurance Society: Credit Union Staff Pages. <http://CUNAMUTUAL.COM/custaff.asp> - A credit union resource.
Dell Year 2000. <http://www.dell.com/year2000/index.htm> - Dell Computer Corporation's Y2K site.

Dover Elevators. <http://www.doverelevators.com/whatsnew/y2k.html> - Year 2000 and Dover Elevators.

GT Beckec. <http://www.RightTime.com> - The RightTime Company, Miami, offering a test and solution for most non-compliant personal computers.

IBM. <http://www.ibm.com/IBM/year2000> - IBM's Year 2000 site.

IEE. <http://www.iee.org.uk/2000risk> - The UK-based Institution of Electrical Engineers' Y2K site.

Matridigm Corporation. <http://www.matridigmusa.com> - Matridigm Corporation, a privately-held software technology company.

Microsoft. <http://www.microsoft.com/year2000> - Microsoft's Year 2000 Resource Center.

NRF. <http://www.nrf.com/hot/t/sur2000> - National Retail Federation Survival 2000 Project.

Paritas Software Services. <http://www.paritas.com> - A software company with a Year 2000 product.

Princeton Softtech. <http://www.princetonsofttech.com/year2000/index.htm> - A software vendor with a suite of Year 2000 tools.

Team C4EWS. <http://www.monmouth.army.mil/y2k/y2khome.htm> - Combined Army, Navy, Air Force, and Marines Y2K Resources.

The Year 2000 Information Center. <http://year2000.com/> - Peter de Jager's Internet site. Mr. de Jager has been active in trying to make people aware of the Year 2000 problem for several years. This site contains a useful and easy-to-use archive and a list of vendors who have paid to advertise on his site. He also maintains one of the most active and useful Internet listserves available.

VIASOFT. <http://www.viasoft.com> - A private company offering several Y2K products.

Washington D.C. Year 2000 Group. <http://www.monumental.com/bwebster/y2k> - The Washington D.C. Year 2000 Group is the largest and most active Y2K group in the world. Members actively work on or deal with Year 2000 issues on a daily basis, in business, government, the military, or other organizations.

Westergaard Year 2000. <http://www.y2ktimebomb.com> - A news forum offering "strategic analysis of the Y2K problem."

Yahoo! Full Coverage - Year 2000. http://headlines.yahoo.com/Full_Coverage/Tech/Year_2000_Problem - An Internet-based news clipping service of Yahoo.

Year 2000 Embedded Systems Vendors, Associations and Manufacturers. http://ourworld.compuserve.com/homepages/roleigh_martin/y2k_com.htm - A private page maintained by Roleigh Martin covering Y2K embedded systems firms.

Year 2000 Information Network. <http://www.mbs-program.com> - Year 2000 Information. A Canadian multimedia publication.

Year 2000 Working Group Online conference. <http://www.year2000.unt.edu/> - Society for Information Management (SIM) International's Y2k Working Group site.

OTHER

Cassandra Project. <http://millennia-bcs.com> - 'A doom and gloom' view of the Year 2000 problem, offered by a grassroots non-profit organization.



Y2K INTERNET RESOURCES

Impact of the Year 2000 Problem. http://www.erols.com/stove451/main_y2k.htm -This site is dedicated to minimizing of the impact of the Year 2000 problem and contains information, opinions, findings, and links that will help you understand the year 2000 problem and how it will impact governments, companies, and individuals.

The Year 2000 in Jersey. <http://www.jersey.gov.uk/frames/year2000.html> -A UK site, the States of Jersey, offers Y2K concerns and solutions.

Y2K- Small Business. <http://www.sba.gov/y2k> -Small Business Administration's assistance for small businesses.

This list of resources is not intended as a comprehensive list of all Y2K sites.

A Glossary for



GLOSSARY

Acceptance Testing

A means by which software is verified to be "Year 2000 compliant" before it is put into use. This is usually accomplished by placing the software on an isolated system and performing tests that are intended to mimic everyday use. Specific methods are used to ensure the system is ready to be implemented and satisfies all documented requirements. The methods include definition of test strategies and procedures, design of test cases and scenarios, execution of the tests, and utilization of the results to verify system readiness.

Aging Report

A report showing the effect of time on a series of data or events.

Alias

A "data" data-element that has been given a convenient name. Data element names are often solely assigned by the computer programmer and may have no significance to anyone else. Typically, such aliases are difficult to find without a thorough understanding of the program computer logic.

Analysis (also Impact Analysis)

Detailed investigation into the location and nature of data uses.

Annotating

To make or furnish critical or explanatory notes or comments, generally within the program source code.

Application

A combination of statements, organized into one or more programs, so that when executed the statements will accomplish a specific set of things. For example, an "ad valorem tax application" may consist of several computer programs, that when executed as an application, will order records, match to existing records and either add or change them.

Auditable

A system or application that has sufficient documentation to support a methodical examination and review.

Assessment Phase

In this period, efforts are focused on an analysis of the Year 2000 inventory and the modification strategies suggested so that cost estimates for remediation can be developed.

Availability Management

Some changes include modifications to the application or system availability schedules, rather than hardware or software changes. When the installation of a change requires exclusive control of a resource and its related products, change control procedures must compare the scheduled date/time to the appropriate



GLOSSARY

availability schedules to prevent unscheduled outages. This includes the means to relate schedules to service-level agreements, such as availability commitments. During parts of the testing, ordinary systems will be unavailable for normal use.

Awareness Phase

In this period efforts are focused on promoting Year 2000 awareness at all levels within the local jurisdiction. Most observers believe this process requires establishing a project office, identifying liaisons, gathering information, and establishing communication channels and processes to be used throughout the Year 2000 resolution efforts. Smaller jurisdictions may wish to combine the Year 2000 awareness and coordination efforts into the existing responsibilities of a staff member, but clear attention to and coordination of this issue is vital to local government jurisdictions.

Batch Programs

Programs that are executed at an isolated time when interactive processes against affected files are not operating. Generally, batch programs are executed after the interactive or "online" systems are stopped.

Baseline Generation

Creation of a record of output from the production systems for comparison against a converted or changed application.

BIOS

Basic Input/Output System. A program or set of programs permanently stored in Read Only Memory (ROM) computer integrated chips installed on a personal computer's system board. The BIOS is the most elemental set of programs used to communicate with the computer chip. If the BIOS cannot update the Real Time Clock (RTC), which keeps the actual date and time, even when the computer is turned off, it will have to be replaced before that personal computer can become Year 2000 Compliant. The BIOS contains functions that enable the CPU to communicate with the outside world.

Binary format

Data stored by using binary arithmetic to represent each character. This is the typical way in which data is compared and processed by a computer. Before comparisons are made, data is converted into its binary equivalent.

Bridging (also Bridge, Bridging Routine)

A process of temporarily or permanently assigning a century value to a non-compliant date, so that the expanded date will be processed correctly by the program. Bridging routines may help local governments to process external inputs or create external outputs to other entities.

Business Rules (also Business Parameters, Business Logic, Data Logic)

Business rules determine how a company or local government will process a given input. For instance, whether the date on which an *ad valorem* tax payment is received is used in the calculations of interest or penalty is a business rule. Business rules dictate how automated systems are to operate.

BIOS Setup Screen

The computer screen of a basic utility program called the BIOS. It enables the user to control such things as the location and type of computer drives contained on a personal computer.

CYY

A date format in which only one digit is used to designate the correct century. An example, 078 might mean 1978, 178 might mean 2078, etc. In order to understand this formatting scheme the analyst must know all possible values of C.

CCYYMMDD

A fully expanded date format. For example, 19781112 represents 11/12/1978. Note that in this format the year is a four-digit number. It is the same format as YYYYMMDD.

Calls

Transfer of control from one software module to another, usually with the implication that control will be returned to the calling module. Historically COBOL "called" the operating system to get the current date. Historically a non-compliant date was returned - MMDDYY - which caused some of the reasons for writing non-compliant programming code.

Central Processing Unit (CPU)

The part of a computer that controls all the other parts. It actually performs all of the computer execution - all other parts exist to feed data or instructions to the CPU and to receive output from it.

Century Windowing (also Windowing)

See Windowing

Change Control

The tracking and management of changes to the production version of an application. A Year 2000 conversion project may introduce numerous changes and there is a potential for the introduction of invalid or improper changes causing the application to fail or return wrong answers.

CICS (Customer Information Control System)

An IBM-licensed teleprocessing subsystem that accepts online input from terminals, executes programs to fulfill user requests, and manages buffers, storage, and file input/output. Many traditional, first-generation, online systems were written on mainframe computers using either CICS or a competitive equivalent.



GLOSSARY**Client/Server Model**

A popular way to utilize the power of personal computers, network servers and the jurisdiction central or mainframe computer. In this model an application may be distributed over all three processors. But the customer uses a graphical user interface of the personal computer to access data and/or applications that reside either on a Network server or the mainframe computer. This computing model requires a sophisticated network infrastructure.

CLIST

A series of command and statements constructed to perform a specific function. Often used in a TSO environment (or SPF) by technological knowledge workers.

Code

Source code is in a specific computer language and must be "compiled" into machine code before use. Machine code is in a suitable format for the computer to execute and is the result of successfully compiling source code.

Code Analysis

The use of sophisticated computer tools to reveal non-compliant source code. Many private firms specialize in this field by providing code analysis tools ("code scanners") to speed a jurisdiction's efforts in locating all potential non-compliant references to date.

Code Conversion (also see Remediation, Code Analysis)

Repairing source code to make it Year 2000 compliant. Conversion can be done through field expansion, fixed windowing, sliding windowing, encryption, and encapsulation. Field expansion, while the most intuitive (all date fields are converted to have full, four digits to describe the century), is also the most expensive since it requires "Flash Cut" implementation and larger fields in existing databases (which often results in the need to buy additional permanent storage Direct Access Storage Device or DASD).

Compiled

Generally, programs are written using an "English-like" computer language, which makes it easier for humans to understand and write. Before these "source" computer programs can be used, however, they must be "compiled" - a process which expands source code into machine language that can be executed by a computer - and tested.

Compliance

Year 2000 compliance means that neither performance nor functionality is affected by dates prior to, during and after the Year 2000. In particular:

Rule 1. No value for current date will cause any interruption in operation.

Rule 2. Date-based functionality must behave consistently for dates prior to, during and after Year 2000.

Rule 3. In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.

Rule 4. Year 2000 must be recognized as a leap year.

Each jurisdiction should define what it means when using the word compliance; then that definition should be used whenever the jurisdiction purchases goods or services that might use automated processes requiring compliance of the vendor.

Complexity Rating (also Difficulty Rating, Program Metrics)

A quantitative measure of the relative difficulty to write or maintain a given program. Different variables are analyzed to determine the rating, such as the average and maximum levels of nesting, total lines of code, the number of data definitions, etc.. Complexity ratings are important as they affect time and cost outcomes.

Configuration Management

The tracking and control of multiple versions of applications that begin to coexist once multiple stages appear in a software life cycle. Because a Year 2000 project contains several phases including assessment, conversion, and testing, configuration management is critical to ensuring compliance.

Connectivity

The capability to connect a computer to other computers. The Internet makes it easy to connect one computer to another and thus promotes connectivity.

Contingency Plan

A documented approach for handling processes, done today by or with the aid of computers, in a manual way in the event those automated processes either do not work or become unreliable as a result of the date advancing into the next century.

Copybook

A record structure pre-defined and referenced by a computer program. It becomes easier to remediate programs when extensive use of copybook standards is employed.

DASD - (Direct Access Storage Device)

A device that permanently stores programs and data. DASD devices have various indexing schemes that allow programs to read or write other programs or data on the device in a very rapid way. These devices are generally thought of as mainframe devices but a personal computer has one or more DASD devices, generally - they are called "hard disks" in that case.

Date Aging

A process of modifying the value of a date so that it will represent a point in the future. For example, if the date is January 1, 1997 and you want to see what will happen at the turn of the century, you can age it by three years, run the program using the modified date, and see what happens.



GLOSSARY**Data Set**

A collection of things that can be electronically stored and retrieved as a unit. Local governments often collect and store electronically a citizen's name and address, which can become a "data set".

Database

An organized collection of "data sets". Elements in the database are related and can be retrieved using those relationships. For instance, a property record logically includes the citizen's name and address. But so does a zoning record. The citizen's name and address, kept only once, may be located elsewhere in the database and retrieved only when needed by an application. A relational database (RDBMS) holds data sets as a collection of tables and index spaces.

Data Defaults

The default date used by an application, usually retrieved from the computer.

Date Field (also Date Element)

Actual location that represents a date, can be represented or stored in many different formats and named by an application in many different ways.

Date Routine

Standardized date module that embeds the useful date logic in a "called routine". Very useful way to alter date logic, format, or calculations without extensive code revision. It is also an easy way to build interface programs whose function is solely to convert dates from one form to another.

Date Simulation

The temporary change of the date and/or time of a system clock, performed by intercepting the date from the system clock and changing it to a different value (e.g., January 1, 2000) before sending it back to the requesting application program. There are useful tools on the market that can help jurisdictions with this effort. Jurisdictions should be careful with date simulation since some software licenses may expire causing still more problems.

Dead Code (also Unreferenced Code)

Any part of a program that can never be accessed because all calls to it have been removed, or because it is guarded by a control structure that probably must always transfer control somewhere else. The presence of dead code may reveal either logical errors due to alterations in the program or significant changes in the assumptions and environment of the program.

Dial-up

A temporary, as opposed to dedicated, connection between machines using a device called "modems" over a telephone line.

Display Format

Data stored in a format that can be viewed by the human eye, i.e., 1978 is said to be in "display format".
(see Binary Data)

Display Only

Data which is printed and viewed on a report or screen, but data that is not used in calculating routines.
Since display only data is not used for comparison by a computer, it might be excluded from the Year 2000 work effort.

Download

To transfer data or programs from one computer to another.

Embedded Century Code

(see CYY)

Embedded Chips

Everything from personal computers to security elevator integrated circuits contain "embedded chips". When computer chips were originally designed some were unable to read or record the century information in part of their permanent memory called the Real Time Clock (RTC). This device keeps the date and time even when the chip is "turned off" and not processing. If these chips control an important process AND if they use their internal clock (RTC) as a trigger for doing something (e.g., open a valve, close an electrical switch, etc.) there is a chance these devices will fail after January 1, 2000. No one really knows how many of these chips use invalid, or non-compliant, RTC information to do important work. The responsibility for maintaining these devices generally falls outside of the normal activities of the information technology function of local government and is another reason top management must direct the remediation effort.

Encapsulation Technique

A remediation technique that depends upon the natural 28-year cycle of the Gregorian calendar. Every 28 years the Gregorian calendar, used predominately in the Western World, repeats itself. That is to say that July 2, 1998 was a Thursday just like July 2, 1970 was - a date 28 years before. For systems that do not need to know what year it is but do need to know what day of the week it is, the Encapsulation Technique may be very useful. The dates of some embedded process logic controllers (PLCs), which control many things, can be set back 28 years. Those processes can safely regulate gates, lights, etc. thinking it is 28 years before and not be adversely affected by January 1, 2000.

Encryption (also called encoding or compressing techniques)

One of the five ways in which remediation can occur. This technique uses binary arithmetic to compress a fully expanded date into almost half of its display size. In this technique, the date represented as YYYY-MM-DD requires 8 bytes (or positions) in display mode but only 5 bytes if compressed using binary arithmetic.



GLOSSARY

Event Horizon

An information resource's "event horizon" is the latest future date that will be processed or handled by the resource. For example, if an application calculates expiration dates two years into the future, its "event horizon" is always a date two years from the present date.

Expansion Technique

Perhaps the most intuitive remediation technique. The international standards setting body has defined ISO 8601, and many organizations have recommended this technique be used, as a way to make dates compliant. ISO8601 requires that dates are placed in the following format: YYYYMMDDhhmmssk where YYYY is the four-digit century; MM is the numeric number for the Month; DD is the day of the month; hh is the hour, using the 24-hour clock; mm is the minutes; ss is the seconds and k is the thousandths of seconds. This technique may also be the most expensive way to solve the Year 2000 problem since it will require that all changed applications be implemented at once after all existing data has been converted to the new format. Since the data will expand as a result, additional DASD may be required.

Failure Horizon

A point in time when an application is expected to fail due to non-compliant date comparisons. For instance, budget systems Failure Horizons might be when they project the future if they use non-compliant date structures.

File Integrity

All applications must treat the data in a file or database in a consistent, documented, and understood way in order to have file integrity.

Files

Logical storage units used to store data and programs.

Fixed Window

A technique of remediation that determines the century (specifically only the two high-order century digits) of a year which has been represented by only two digits (e.g., an automated record may have carried the code "78" for the year "1978"). The two-digit year is compared against a pair of hard-coded pivot points representing the low and high points of a 100-year span. Any two-digit century field is considered to be in the 20th century (19xx) if it is greater than the lower pivot point number (e.g., assume the lower pivot point is 60, a century designation of 71 would be interpreted as 1971). Likewise a century designation less than or equal to the higher pivot number is considered to be in the 21st century (20xx) (e.g., in our example the higher pivot point has to be 40, therefore a century designation of 31 would be interpreted as 2031). There are two flaws in the Fixed Window solution. First, it is limited to applications where 100 years will cover all cases. Secondly, as the years go by this "solution" becomes more constricting and less viable until it is no longer useful. To combat this problem, see the Sliding Window definition.

Flash Cut

Changes to an existing application (which may have many computer programs and many run sequences) must be implemented all at once rather than one computer program at a time. This form of implementation is required when the remediation technique called "Expansion" is used. This technique may be used in other circumstances as well, e.g., the replacement of an old application with a new one may necessitate the use of a "flash cut" process.

Gregorian Calendar

Today's general-use calendar of 12 months and 365 days that employs the current leap year algorithm. The Gregorian calendar repeats itself every 28 years which leads to the possibility of using the "Encapsulation Technique" on some embedded chip processes.

High-Impact

The failure of a mission critical application (because it was not compliant with January 1, 2000) would be considered "high-impact". Generally, whenever dates used as keys are compared, or used in calculation, those applications are considered "high-impact" exposures.

High-Order Truncation

Occurs when the variables defined to hold a certain result of a calculation are exceeded at run time. As a result, the first digit, the most significant digit in the number, is truncated and the incorrect number is stored in the variable. Some applications may have this problem when the application adds one year to the current year and the current year is "99" for instance.

Impact Analysis Report

A report that shows the relative severity of failures in applications.

Impact Analysis

To analyze the Year 2000 impact to applications, the impact analysis includes:

- *Analyzing Complexity*: determines the complexity of a software design or code using a metric, such as degree of nesting, or other characteristics.
- *Analyzing Impact*: analyze the application's program modules and related data to determine what is impacted and related.
- *Analyzing Metrics*: collects, analyzes, and reports the results of analysis activities.
- *Analyzing Database*: investigates the structure and flow within a database to observe the characteristics of the database and determine if certain measurements/requirements can be realized.

Integrate

Merging data from separate sources to create one unified database is a form of integration. Today most



GLOSSARY

applications receive input from many sources - some within an entity, some from outside the entity. Local governments must be certain that automated system inputs use compatible date formats and that they are compliant - regardless of their source i.e., inside or outside.

Integration Testing

A process whereby a related group of program modules are tested to determine if they work properly together.

Interface

A shared boundary across which information is passed. A hardware or software component that connects two or more other components for the purpose of passing information from one to another. Local governments must insure that automated interfaces handle dates in the same way as the internal application.

Interfacing

Computer applications often depend upon the output from other computer applications. Some of these applications are "owned" by the jurisdiction - others are not. However, for all computer applications to interface properly after the turn of the century, each entity must know how dates are processed in the other's application. Thus interface integrity must be maintained or segments of the society will not function, or will not function well, after January 1, 2000.

Inventory

The process of collecting and reporting all automated systems. It is the first, and perhaps the most important, step of a sound remediation effort. Without a good list of all potentially affected systems, management will not exercise those supervisory techniques necessary to get critical systems remediated. Inventories are critical to providing cost estimates, system status, interface, and certification information to the Year 2000 effort, and to the agency's general information protection program.

IMS (IBM's Information Management System)

A hierarchical database and data communication system that runs on large mainframe style systems such as IBM's MVS operating system.

JCL (Job Control Language)

A language used on large mainframe computers that identifies one job from another, assigns various devices and controls input and output media.

Julian Date

Formally, Julian Date is defined as the contiguous count of days from January 1, 4713 BC, Greenwich Mean Noon (equal to zero hours Universal Time). The fraction of each day is represented as a decimal number. Hence noon (GMT) on January 2, 4713 BC, would have the Julian Date 1.00000, 6.00 p.m. GMT on the same day would have the Julian Date 1.25000 and 6.00 hours Universal Time would have Julian Date 2443509.75.

However, in most local governments the Modified Julian Date is used. It is the last two digits of the year followed by the number of days expended since the last January 1. Thus February 1, 1998 would be expressed as 98032, and January 23, 1998 would be 98023, etc.

Key

A value used to identify a record in a database, derived by applying some fixed function to the record. The key is often simply one of the fields (a column if the database is considered as a table with records being rows). Alternatively, the key may be obtained by applying some function, e.g., a hash function, to one or more of the fields. The set of keys for all records forms an index. Multiple indexes may be built for one database depending on how it is to be searched.

Language Upgrades

Implementing a more recent release of language software.

Leap Year

Leap years are corrections to the Gregorian calendar. The Year 2000 will be a leap year. Century years (like 1900 and 2000) are only considered leap years if they are evenly divisible by 400. Therefore, 1700, 1800 and 1900 were not leap years, but the Year 2000 will be a leap year.

LOC (Lines of Code)

Common measure for stating size of an application or program. Gives indication of how much code must be analyzed and/or converted.

Logical Files

Contain data that is indexed.

Logical Data Model

The purpose of the logical data model is to show the data that the application must store in order to satisfy business requirements. It also shows how data is related. It is created without any specific computer environment in mind. No optimization for performance, data storage, or even application development is done. The intent is to produce a purely logical view of the data required by the business area.

Low-Impact

Year 2000 failures that occur to applications that are not critical to the jurisdiction are considered to be low-impact failures. If the jurisdiction has time they should be remediated

Mask

A pattern of characters used to represent another character or set of characters. For example, the mask TH* could represent all data set names beginning with the letters TH. This is used to filter out expected differences when running a baseline comparison.



GLOSSARY**Methodology**

A particular procedure or set of procedures or a particular way of doing things.

Metrics - (see Complexity Rating)**Mission-Critical Applications**

Applications which are needed in order to maintain the success of the business.

Modem

A physical device necessary to convert computer signals into waves that will travel over a telephone line. At the other end of the telephone line another modem must be used to convert those same signals back into useful information to the computer.

Naming Conventions

Programmers define data by naming its position and describing its characteristics. A data naming convention is a formal method of naming data that is given to the programmers. Naming conventions provide more structure to data and probably make it easier to locate and remediate Year 2000 problems.

Network

Hardware and software necessary to connect computers and resources into one communication system.

Network Adapter

An expansion card that connects a computer to the cables of a network and transmits the type of signals used throughout the network. On personal computers, the adapter (often referred to as a "NIC") is inserted into an expansion slot inside the computer. On portable computers, a "NIC" may be a PCMCIA card device (like a card modem).

Network Operating System

An operating system able to handle the many tasks associated with a network, such as file locking, resource allocation, and error control.

Network Server or File Server

A computer on a network that has the main hard disk storage for the other stations on the network. The file server usually also runs the network operating system.

Nonstandard Date Logic

Date logic found in the date routines, which does not adhere to the standard practice established in the computer organization.

Nonstandard Date Storage

Date represented in a nonstandard format.

Object Delivery

These are processes and tools used to take updated modules, procedure, and control information for an application, package them, and deliver them to production environments. They include mechanisms to prevent "back-leveling" or other improper installation.

Object-Oriented Change Management Packages

These packages manage the differences in how developers program in an object-oriented fashion. They enable programmers to use class libraries and reuse code.

One-Digit Century Code

A renovation technique in which one digit is added to the two-digit year to define the century. Perhaps no credible organization will use this technique. It begs the question, "Why not insert all four digits while those changes are being made?" (see Expansion Technique)

Parsing

Reading the pre-compiled source in the same manner as its compiler. Instead, however, of producing compiled code, parsers produce analytical output, in this case appropriate to the Year 2000 conversion. Parsing has many benefits over scanning, including identification of relationships between code components, summarization of attribute information, identification of aliases, and calculation of complexity ratings.

PDS (Partitioned Data Set)

A data set consisting of one directory containing one or more members.

Physical Files

Any single collection of stored information, typically on floppy or hard disks. A file may be a part of the operating system, an application, or data (such as word processing, graphics, or spreadsheet documents). Anything on a disk that has a filename.

Physical Model Names

Names used to describe physical models.

Platform

The hardware or operating system (or both) on which a program runs.



GLOSSARY**Printer File**

Stores the various pre-printed formats required by the application for printing reports, documents, etc.

Procedural Logic Change (also Procedural Modification, Logic Change)

In Year 2000 projects, the manipulation of program logic to achieve compliance.

Process and Project Management

The tracking and control of all of the activities, tasks, deliverables, roles, and techniques necessary to plan, estimate, and schedule an IS project. It may include customizable methodologies; project scheduling, control, and reporting; time and resource tracking; process and methods management; budget and cost analysis modeling, planning, and estimating; and experience management. Process and project management would utilize programmer skill levels, estimates of task difficulty and times, available calendars, dependencies, load leveling, resource availability, and all other planning elements to tactically plan a project.

Problem Tracking

Since problems frequently result in changes that fix them, problem-tracking tools must integrate/relate to change control. Since change is the nature of IS, changes that result in problems must be identified and their recurrence prevented.

Procurement

The process a local government goes through to purchase goods or services.

Program

A sequence of precisely coded instructions that, when assembled, describe an automated function performed by a computer. Several programs may be used in an application.

Program Files

Contain the programs that make up the application.

Program Modification Bridge

A bridge that performs spot renovation; it changes the spot that accesses the file.

Project Design Phase

It is a period in which examination, evaluation, and definition of an in-depth solution is made and documented for a Year 2000 project including standards, staffing, facilities, guidelines, and tools.

Project Management

This tool assesses a change request and evaluates return on investment for major change development. Pre-change planning tools that provide input to the change control process are also included.

Remediate

The process of making an application, system or computerized component compliant to the Year 2000 and beyond. To remediate is to "fix" an application or process for the Year 2000 problem.

Renovation

A Year 2000 conversion strategy in which resources that are not Year 2000 compliant are located, modified, and verified to ensure Year 2000 compliance.

Replacement

A Year 2000 conversion strategy in which resources that are not Year 2000 compliant are replaced with compliant, purchased solutions or solutions that are developed using the existing system's design.

Repository

A data repository is a specific location where data is stored.

Retirement

A Year 2000 conversion strategy in which resources that are not Year 2000 compliant and are deemed no longer necessary are systematically and permanently removed from the production environment. It might be determined, after a thorough impact analysis, that a given application is no longer needed and that it can be successfully retired.

Scanning

Searching for a character string within a given text. This manual analytical approach is generally performed by a parsing program.

Scoping

A high-level analysis of an enterprise to determine the magnitude or impact of the Year 2000 problem. It usually results in preliminary estimates of the time, resources, and costs that would be needed to achieve compliance. Determining the "scope" of the problem is generally followed by an "impact analysis".

Serial Date formats

A number value based on a set starting date. For example, January 1, 1980 is often considered a base date for personal computer Real Time Clocks with a serial value of "000001" and all dates subsequently assigned the exact number of days since that base date.

Service Levels

Assurance that response time in an on-line system is within the time-span tolerance and that the application workload can be completed in accordance with the application schedule.



GLOSSARY**Sliding Window**

This is a special case of the Fixed Window technique. It is a way of automatically advancing the selected 100-year window, thus making this technique, theoretically at least, a permanent solution. A 100-year window is selected so that the sum of the two must add up to 100. For example, a sliding window of 80 (lower pivot point) and 20 (higher pivot point) means that for 1997, the effective range is 1917 through 2016, so that a year value of 17 through 99 has a century value of 19, and a year value of 00 through 16 has a century value of 20. In 1998, the 80 and 20 pivot points means that the new effective range is 1918 through 2017, so that a year value of 18 through 99 has a century value of 19, and a year value of 00 through 17 has a century value of 20. By the same reasoning, a sliding window of 60/40 means that for 1997 the effective range is 1937 through 2036, so that a year value of 37 through 99 would have a century value of 19, and a year value of 00 through 36 would have a century value of 20.

SMF

System Management Facilities within MVS.

Software Conversion Factory

An off-site (often "off-shore") location where non-compliant code is shipped to be installed on hardware for processing and conversion by Year 2000 consultants. Utilization of a software conversion factory frees up an organization's system resources, so that daily business and mission-critical activities are not adversely affected by the Year 2000 project. Having the work done off-shore may be cheaper as well but has its own political liabilities.

Source Code (also Source or Code)

The form in which computer program is written by the programmer. Source code is written in some formal program language that can be compiled automatically into object code or machine code or executed by an interpreter.

Source Control

The process of managing multiple versions of source code, during development, maintenance, testing, and production. This includes library management, versioning, and relationships to other source code elements. Several software products can help with this process. Careful source control is vital during the Year 2000 remediation process.

SQL (Structured Query Language)

A database language used to query, modify, and manage relational databases. Whereas each commercially purchased database has its own language, generally SQL statements are recognized by most of those systems available.

String Testing

The Year 2000 testing of a series of programs that make up a logical portion of the entire system. Generally, string testing is a sub-set of System Testing.

System

The IEEE Standard Glossary of Software Engineering Terminology defines system as a collection of components organized to accomplish a specific function or set of functions. It also defines a subsystem as "as secondary or subordinate system within a larger system."

MIL-STD-498 (5 December 1994) tries to deal with the potential ambiguity as follows: The term "system," as used in this standard, may mean: a hardware-software system (i.e., a radar system) for which this standard covers only the software portion, or a software system (i.e., a payroll system) for which this standard governs overall development. If a system consists of subsystems, all requirements in this standard concerning systems apply to the subsystems as well. If a contract is based on alternatives to systems and subsystems, such as complex items, the requirements in this standard concerning the system and its specification apply to these alternatives and their specifications.

System Date Simulators

Tools that allow information systems to pass user-specified system dates to batch jobs and other program components without destroying the validity of date dependent license agreements.

System Testing

Testing that demonstrates the adherence of a complete system to functional specifications, usability requirements, system integrity requirements, and integration with external systems and procedures.

Technology

A manner of automation techniques used to accomplish a task.

Testing

As related to Year 2000 projects, verification that changes are functioning properly. This can be done at the unit level (ideally, by tools actually making the changes) and at the system level. Proper testing requires methodology, management, test data that has been aged to appropriately "exercise" the application in question, a playback testing tool, and a date simulation tool. (Note: date simulation tools are suggested even when a separate CPU is available for testing. This protects against damaging SMF dates.)

Tools

There are a wide variety of tools that can be used throughout each of the phases of the Year 2000 remediation process. The following categories are provided as examples:

Software Inventory Tools - Help determine all code, control scripts, databases, etc., that constitute a system. Essential to complete impact analysis.

Configuration Management Tools - Turns software into configurations. This is important during modification and elimination of bugs in code prior to systematically recording what software is fixed and what still needs to be fixed.



GLOSSARY

Change Tracking Tools - Logs request for changes and tracks them to resolution. The change tracking database can be a useful place to look for changes regarding dates or bugs concerning dates.

Cost of Work Estimating Tools - This tool, spreadsheet, or methodology predicts how much work will be needed to remove Year 2000 problems. Check how the model you intend to use has been validated. That is, its predictions compared with actual human performance in removing the Year 2000 problem. Because carefully measured empirical data on finding and removing Year 2000 problems is currently hard to find, the cost model may not have been separately calibrated with the valid data collected from real Year 2000 problem removal projects.

Problem Code Finding Tools (Clock Simulators) - These change system clocks, unknown to programs. They are an easy way to quickly check if code has Year 2000 problems.

Problem Code Finding Tools (Data Finders) - Help locate date-oriented data, variables, or information in the code.

Problem Code Finding Tools (Browsers) - Scans code and inspects. Scanning can be speeded by looking at structure charts, selecting code, and immediately jumping to the code. They can save a lot of time over just using a text editor. Browsers can include some reverse engineering tools or maintenance workbenches.

Impact Determining Tools (Impact Analyzers) - These essential tools do the hard work of finding what is related to what. However, just because an item is estimated to be affected does not mean that item will need to be changed to fix a specific Year 2000 problem. They tend to overshoot their estimates to be on the safe side.

Impact Determining Tools (Cross-references) - Identify variables, procedures, or other items are in the code. Provide a limited form of impact analysis.

Impact Determining Tools (Program Slicers) - Help identify all the code affecting a given variable or statement. These tools do not replace the need for regression testing.

Change Makers (Data Cleanup) - Extract and convert data from a non-relational to a relational DBMS.

Change Makers (Field Expansion) - Expand two-digit year fields to four-digit year fields.

Change Makers (Data Name Rationalization) - Introduce standard or more uniform names to date-oriented fields.

Change Makers (Code Modularization) - Help identify chunks of code and may wrap an interface around them, making them into procedures or modules. Fall-throughs into this code are replaced by calls to it. This is helpful because certain changes in the module can be hidden without fear that other parts will be affected.

Change Makers (Date Subroutines) - Reusable code modules that have correctly implemented the handling of dates.

Testing and Regression Testing Tools - Essential for checking whether software changes introduced unwanted problems. Since automatic impact analyzers do not check impacts in all possible inter-code relationships (e.g., timing), testing is nearly always a necessary part of the software change.

Unit Testing

The separate testing of the individual modules that comprise a production system. (see String Testing)

User-Acceptance Criteria

Criteria defined early in the system development process by the customers, which determines the acceptance of the system.

VSAM (Virtual Storage Access Method)

An IBM-licensed program used for indexed or sequential processing of fixed-or variable-length records on direct access devices. VSAM is frequently used on the MVS operating system.

VTAM (Virtual Telecommunications Access Method)

An IBM-licensed program used for controlling communication between terminals, CPUs, and various other devices.

Windowing

Defining a continuous 100-year period over two consecutive centuries so as to allow years to be defined by only two positions or "pivot points". For example, a business parameter can be added to the code, saying "If year is equal to or less than 68, then a century of '20' is assumed; otherwise, the Century is assumed to be '19.'" This rule would mean that the century window would run from 1969 through 2068, inclusive. See "Fixed Window" and "Sliding Window".

Workstation

A PC (personal computer) or RISC (reduced instruction set computing) box or terminal connected to the network.

Year 2000 Compliant

(see compliance)

Year 2000 Event Horizon

For purposes of these standards, the "Year 2000 event horizon" is the date by which a resource must be compliant before its date process fails. (see Event Horizon). Most observers believe that complex applications should be compliant one year before their Year 2000 event horizon occurs.

Year 2000 Ready

(see Compliance)

YY-Format

The YY-format is a two-digit year format (e.g., 99).

**This glossary is not presented as a comprehensive list of Y2K-related terms.*



Mr. HORN. I am sorry to take more than a minute, so go ahead.

Mrs. BIGGERT. You are yielding back to me now?

Mr. HORN. Yes, yes. Go to it.

Mrs. BIGGERT. Thank you, Ms. Mann. I think that your enthusiasm and what you have to say will really carry this forward, too, so we appreciate you being here. With the enthusiasm and the dedication that you have for this problem, I think that it will move forward.

Just, Dr. Morentz, is the emergency management community taking advantage of the products and services that you have talked about, the technological products that will move us forward in this?

Mr. MORENTZ. Yes, I would say, by and large, there has been good movement over the last decade in emergency management organization embracing technology. The Federal Emergency Management Agency has been good—although they were prodded by about 30 of the States that had adopted automated systems before FEMA actually made the embrace of technology as broadly as they have. But since then, a couple of years ago, they have done a very good job as has the Army National Guard; and the Air National Guard and the Air Force at the Federal level have done very good jobs in starting to establish an infrastructure.

The point of this confluence between that incremental movement that has been taking place to improve emergency management and the Y2K opportunity is one that really deserves attention to be able to get everyone to focus on the Y2K, thus moving Y2K from a potential disaster into a routine emergency. Whatever happens, at the same time, we will have created an infrastructure that will survive January 1, 2000, and for many years.

Mrs. BIGGERT. Do you see that there is really a difference in the type of emergency that could be created by the Y2K and other emergencies?

Mr. MORENTZ. You know, I really don't see it as distinctive. I think, as you have heard from local government representatives and others, we have done—particularly in the United States, we are an infrastructure-rich country, and when a hospital experiences a problem, there are other hospitals generally within an area to take critical patients. But the idea is that if the organization doesn't know the plan and have procedures in order to get accident victims to an alternate hospital, then it becomes a disaster. So, truly, it is the application of the technology to drive the contingency planning and put in place a command and control system for alternatives that is really the potential missing link here.

Mrs. BIGGERT. So you would say that the existing information systems and data bases can be used to better prepare the citizens and the public sectors for emergencies, or do we need something beyond that?

Mr. MORENTZ. No. Really, the standard things that are being done to plan for any type of a disaster are exactly what you need for contingency planning for emergency management for Y2K. It is a matter of applying them, focusing on them and making certain that they are, in fact, widely available, rather than more narrowly available, as is the case today.

Mrs. BIGGERT. OK. What would be, do you think, the most difficult technological challenge for emergency management in the 21st century?

Mr. MORENTZ. Well, clearly, the advantages that we are seeing in technology with small telecommunicating devices provide such an abundance of opportunity for the emergency management community. I think the biggest thing that is going to take place is the implementation of that inside a consistent—both policy, program and infrastructure, to drive the technologies out to the places where they are needed. You have heard about Kitsap County over here.

The key is to be able to make those technologies available. The private sector is doing its part by creating the technologies, driving the prices down to where they become incredibly affordable, but what still is missing is an ability within the State, Federal and local governments to actually make these part and parcel of what every emergency program does.

Mrs. BIGGERT. Thank you very much.

Thank you, Mr. Chairman.

Mr. HUMPHREY. Mr. Chairman, just one quick point I wanted to make, and that was the need for resources and assets at the local level. I will give you some quick examples of that.

Aircraft carriers that normally dock in the Norfolk area generate enormous amounts of electricity. They have great capacity. Now is the time to see if, in fact, they can support those seven communities of that area in some way or another. Maybe there is some ways in which they could provide warming facilities should it be needed; maybe they could provide food stores.

I mean, there are lots of different ideas. I certainly don't have a lock on them. But I think we have to think out of the box, and we have to come up with ideas that, in the case of disaster, we have a plan to deal with them. This, in deference a little bit to my colleague, this is really different in the sense that it is going to look normal. Everything is going to look fine. It just may not work or it may not work correctly. And so it is going to be a different psychological response. It is going to be a different kind of need. We have to prepare; but the question is, how should we prepare and what kinds of contingencies and can they make commitments to do that? That is why I say, I bring up the Navy, that example, the National Guard in Albuquerque. There are resources and assets which can help citizens of this country in specific ways.

My colleague was pointing out traffic lights. We don't think about traffic lights, but being many traffic lights are controlled by the timing mechanisms of embedded chips and all of them, some of them, have mechanical wheels that turn but others are controlled by embedded chips, and local governments have to figure out which is which and what to do with them. I mean, there are little things like that, that this is going to be a, really, a different issue.

Thank you.

Mr. HORN. Well, you are absolutely correct. We have stressed that every hearing we have had in the field when we have had city managers and mayors with us on fire equipment, traffic lights, all the rest.

Ms. HECKLER. Mr. Chairman, I wondered if you would be willing to allow my colleague, Dr. Gerschel, to say something.

Mr. HORN. I was going to ask him, yes.

Ms. HECKLER. Because this medical problem is unique.

Mr. GERSCHEL. Mr. Chairman, my level of expertise is perhaps not as great and as long as the others, but I come from a somewhat different perspective. We spoke just now of issues of traffic lights. In conversation, candid conversations, with some city managers in the area in which I live, they have basically come to the conclusion there is not enough time. There is time to take care perhaps, and I say perhaps of waste management because we are not going to know until the end, perhaps of water supply. Certainly they are concerned about the electrical supply and the electrical grid, but they have come to the conclusion there is not enough time and not enough money to take care of traffic lights in the time that remains.

Now, in terms of medical situations, well, traffic lights aren't part of the hospital, but the accidents that take place thereafter probably will be or, hopefully, won't be. But in terms of specific medical issues, and perhaps in addressing Congressman Biggert's question, what we have found in major institutions in the testing that we have seen and done and reported and what we have put on these websites is that we will get a notification that a piece of equipment or a piece of hardware is, in fact, compliant. Well, that is only partly true. It is compliant, if it has been built, let's say, past 1997, but something, bearing the same model number but a different set of chips, will not be compliant, and we are testing a lot of materials that way, and we are posting that on these sites.

The suggestion that Ambassador Heckler has made is to take that data of specific testing where it is not only just a model number but a serial number as well in a production run of material so that county hospitals, municipal hospitals that don't have really the wherewithall and the time to test it, collecting that data into this super site, medical health care super site.

We know that is a problem, we know it is an issue, we know that it takes a little time and effort, but that could save a lot of time, effort and energy on the local level, make expertise available to them that they might not be able to get initially or easily.

Mr. HORN. That is well said, Dr. Gerschel, and I want to thank you for all you are doing in helping this matter.

I thank all of the panelists. I would like to ask now for those that are in the audience on the emergency management workshop participants, why don't you just stand so we can see how many of you are out there, just stand, who is going to participate this afternoon and tomorrow.

Good. Thank you for coming. We are honored to have you here as experts on emergency management, and I am gratified that you would give your time and your resources to be in Washington today. I know that among you are emergency management experts from my own home State of California, as well as Florida, Massachusetts, Georgia, Colorado, New York, Montgomery County, MD, Virginia, and the State of Washington, of course. And those from the National Defense University, they are also interested in this subject. We thank all of you.

With so much attention that is being given to the year 2000 computer problem, it is a remarkable coincidence that altogether you have about 2,000 years of experience in hundreds of natural and man-caused disasters among all of you. This includes floods and hurricanes and wildfires and earthquakes and toxic spills, snow, ice storms, all the rest, cyber attacks—thank heaven, we haven't had too many of those—and chemical and biological terrorism. We have had some fake ones now, and let's hope that we don't have the real ones. We are looking forward to meeting all of you in the workshop group as you discuss and formulate these things.

I also want to recognize a longtime friend of mine, if he is in the room, Dr. Robert Chartrand. Do you want to stand up? Oh, there you are, OK.

Bob and I have worked together for 3½ decades. When I brought together the senior staff in the Senate in the mid-1960's to computerize the Senate with the major offices, as I was assistant to the Republican whip, Mr. Kuchel in California, and then we had the New York senators and we had the Illinois senators, where Senator Dirksen was from, and we believed in the concept of, I think the Washington Post called it Dial-A-Bill, because we were just tired of our staff having to pick up the phone every day, find the status on this, who has testified. It was obvious it was something we could computerize.

When I went to Brookings I had a dinner of about 100 from the Hill and staff and Members and one rather crusty chairman, which will go unnamed, but many of you might know, sat listening and said, "well," and chomped on his cigar, "all I can say is you are going to do that over my dead body." And it took a long time to get computing anywhere around here that would help. But Bob Chartrand has certainly been in the forefront of that; and we thank you, Bob, and all of your associates here.

As I understand it, you are divided into four groups, each one of us has chosen a group to work with, and the full particulars are found in the material you were given as you entered the hearing room. My charge to you is very simple. Within the scope of your workshop group, evaluate current emergency management efforts, propose solutions, products and systems that will meet the challenges of the 21st century. You are all visionaries just by being in this business, but you are also practical people, and that is where it is very important to bring both of those values together. I look forward to receiving your recommendations tomorrow when we reconvene, and we plan to feature these in the upcoming committee print. Your group leaders will meet with you at their designated places in the hearing room. I hear there are signs with workshop group names being posted at four locations in this hearing room. So thank you all for coming.

I would like to thank the following people for the record: J. Russell George, staff director and chief counsel for the subcommittee; Bonnie Heald, director of communications of the subcommittee; Harrison Fox, professional staff member for the subcommittee;

Mason Alinger, our clerk; and interns Kacey Baker and Richard Lukas. Also, Faith Weiss, minority counsel; Jean Gosa, minority clerk; and our court reporters today, Cindy Sebo, Joe Strickland, and Julie Bryan.

With that, the subcommittee is adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

