AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 105–895

EMERGENCY PLANNING FOR THE YEAR 2000: PREPARATION OR PANIC?

HEARING

BEFORE THE

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

ON

THE PREPAREDNESS OF EMERGENCY SERVICE AGENCIES AT THE STATE, COUNTY, AND LOCAL GOVERNMENT LEVELS

OCTOBER 2, 1998

Printed for the use of the Committee

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

51-565 CC WASHINGTON : 1999

For sale by the Superintendent of Documents, U.S. Government Printing Office
Washington, DC 20402

SPECIAL COMMITTEE ON THE
YEAR 2000 TECHNOLOGY PROBLEM

[Created by S. Res. 208, 105th Cong., 2d Sess. (1998)]

ROBERT F. BENNETT, Utah, *Chairman*

JON KYL, Arizona
GORDON SMITH, Oregon
SUSAN M. COLLINS, Maine
TED STEVENS, Alaska, *Ex Officio*

CHRISTOPHER J. DODD, Connecticut, *Vice Chairman*
JEFF BINGAMAN, New Mexico
DANIEL PATRICK MOYNIHAN, New York
ROBERT C. BYRD, West Virginia, *Ex Officio*

ROBERT CRESANTI, *Staff Director*
T.M. (WILKE) GREEN, *Minority Staff Director*

CONTENTS

OPENING STATEMENT BY COMMITTEE MEMBER

Robert F. Bennett, a U.S. Senator from Utah, Chairman, Special Committee on the Year 2000 Technology Problem 18
Christopher J. Dodd, a U.S. Senator from Connecticut, Vice Chairman, Special Committee on the Year 2000 Technology Problem 20

CHRONOLOGICAL ORDER OF WITNESSES

John A. Koskinen, Chairman, President's Council on Year 2000 Conversion 2
Lacy Suiter, Executive Associate Director for Response and Recovery Directorate, Federal Emergency Management Agency 5
Hon. Michael O. Leavitt, Governor of the State of Utah 25
Ellen Gordon, president, National Emergency Management Association 27
Maj. Gen. Edward J. Philbin, USAF [Ret], Executive Director, National Guard Association of the United States 30
John Thomas Flynn, President, National Association of State Information Resource Executives 33
Bruce Romer, Chief Administrative Officer, Montgomery County, MD, on behalf of the National Association of Counties 40
Bob Cass, City Manager, Lubbock, TX 42
John S. Powell, University of California Police Department, on behalf of the Association of Public Safety Communications Officers 44

APPENDIX

Alphabetical Listing and Material Submitted

Bennett, Hon. Robert F.:
- Opening statement 18
- Prepared statement 53

Cass, Bob:
- Statement 42
- Prepared statement 58
- Responses to questions submitted by Chairman Bennett 60

Collins, Hon. Susan M.: Prepared statement 61

Dodd, Christopher J.:
- Statement 20
- Prepared statement 62

Flynn, John Thomas:
- Statement 33
- Prepared statement 63
- Responses to questions submitted by Chairman Bennett 86

Gordon, Ellen:
- Statement 27
- Prepared statement 87
- Responses to questions submitted by Chairman Bennett 89

Koskinen, John A.:
- Statement 2
- Prepared statement 90
- Responses to questions submitted by Chairman Bennett 92

Kyl, Hon. Jon: Prepared statement 94

Leavitt, Hon. Michael O.:
- Statement 25
- Prepared statement 95
- Responses to questions submitted by Chairman Bennett 97

Page

Moynihan, Hon. Daniel Patrick: Prepared statement 98
Philbin, Maj. Gen. Edward J.:
Statement 30
Prepared statement 99
Responses to questions submitted by Chairman Bennett 100
Powell, John S.:
Statement 44
Prepared statement 102
Romer, Bruce:
Statement 40
Prepared statement 122
Smith, Hon. Gordon: Prepared statement 132
Suiter, Lacy:
Statement 5
Prepared statement 133
Responses to questions submitted by Chairman Bennett 136

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Statement of R. Michael Amyx, Executive Director, Virginia Municipal League, on behalf of the National League of Cities 140

Note: Responses to questions submitted by Chairman Bennett to Mr. John S. Powell and Mr. Bruce Romer were not received at the time the hearing was published.

EMERGENCY PLANNING FOR THE YEAR 2000: PREPARATION OR PANIC?

FRIDAY, OCTOBER 2, 1998

U.S. SENATE,
SPECIAL COMMITTEE ON THE YEAR 2000
TECHNOLOGY PROBLEM,
Washington, DC.

The committee met, pursuant to notice, at 9:30 a.m., in room 192, Dirksen Senate Office Building, Hon. Robert F. Bennett (chairman of the committee), presiding.

Present: Senators Bennett, Collins, Smith of Oregon, and Dodd.

Chairman BENNETT. The committee will come to order.

We are very pleased this morning to have John Koskinen and Lacy Suiter with us as our first panel. I have an opening statement, copies of which are available to members of the press, which I will not read, out of deference to the fact that Mr. Koskinen has an airplane to catch a little later in the morning and I think the committee would be better off hearing from him than from me. That's usually the case with every committee chairman, but usually not observed on Capitol Hill. So I will delay making comment about some of the issues in my opening statement until after we have heard from Mr. Koskinen.

I will make this general introduction. Those who have followed the committee know that we set out in the beginning a series of priorities, listing them in the order in which we thought failure because of Y2K problems would cause the greatest impact. The first priority was the power grid, utilities, and then we talked about telecommunications. We have talked about transportation—we had a full hearing on that—the financial system, and now we come to general government.

We have divided the responsibilities in the committee among the seven members, because we ended up with seven priorities. Senator Collins has the lead on the committee for today's priority, which is general government activities. We're delighted with the line up of witnesses that we have.

We will start with the Federal Government, with Mr. Koskinen and Mr. Suiter, and then we'll have State governments—the lead witness will be Governor Leavitt, the Governor of Utah, and the potential, incoming, prospective, whatever the appropriate adjective is, chairman of the National Governors Conference, and then we will go to local government, county, and city. So that's the outline for today's hearing.

While Mr. Koskinen has appeared before the committee before, we wanted to give him this opportunity to describe to us where we

are at the Federal Government level, and then interact on the panel with Mr. Suiter, who will have much of the responsibility of dealing with Federal Government coordination with State and local governments in those areas where any kind of emergency may arise. So that's the format for today's hearing.

Senator Collins, we appreciate your leadership on this portion of the committee's work, and you're willingness to accept this assignment. I will recognize you for any opening comments you may have. Senator Collins. Thank you very much, Mr. Chairman. I do have a fairly lengthy opening statement. It's my understanding that one of our witnesses is under a time constraint. If you would like to hear from the witness first, I could then do my opening statement afterwards.

Chairman BENNETT. Yes. I said just before you came in that I'm going to postpone my opening statement for the same reason, so I'm grateful to you for your willingness to do that.

Mr. Koskinen, we will go directly to you, then. We welcome you.

I must make this comment. John Koskinen's responsibility is in the executive branch, but he has been called as far away as Japan to talk to the people about their Y2K problems. He's just getting over jet lag.

Mr. Suiter is just recovering from coming back from dealing with immediate emergency problems relating to the current hurricane and got in very late last night. So we're grateful to both of you for your willingness to appear before the committee.

Mr. Koskinen.

STATEMENT OF JOHN A. KOSKINEN, CHAIRMAN, PRESIDENT'S COUNCIL ON YEAR 2000 CONVERSION

Mr. KOSKINEN. Good morning, Mr. Chairman, and thank you for the kind comments. I am pleased to appear again before the committee to discuss the role of the President's Council on Year 2000 Conversion in dealing with this problem. With your permission, I will submit for the record my full statement and summarize it here.

In the past, as you have noted, I have described our general approach to this issue, including the formation of the Council, with representatives from 35 agencies across the Government, including the regulatory agencies.

As you know, we have divided the world into 34 sectors that we are concerned about. We are dealing with a review of the Federal Government's operations as it attempts to remediate its systems. We're focused on the interfaces between the Federal Government and State governments which administer many of our most important programs. Most importantly, in each of the 34 sectors, we're involved in reaching out to public and private entities in the United States, as well as countries around the world, both to increase the level of awareness, and promote activity on the Year 2000 problem.

This morning I would like to discuss the Council's role in the development of contingency plans and appropriate emergency responses to any difficulties that may arise as we make the transition to the Year 2000.

Before I discuss this issue though, let me express the administration's appreciation for the strong support this committee has provided in the development and passage of the Year 2000 Information and Readiness Disclosure Act. In particular, the assistance you, Mr. Chairman, Senator Dodd, and Senator Kyl have provided has been an indispensable part of the success we have achieved. As the President has said, this bipartisan legislation provides us with an important opportunity to help our Nation prepare its computer systems for the new century.

I would also note that this committee has made a major contribution in promoting awareness of, and action on, the Y2K problem with hearings that have examined, as the chairman noted, public and private sector progress in important economic sectors that range from electric power to transportation to telecommunications.

But even with the best efforts of all of us, we need to understand and expect that not every system and embedded chip will be found and fixed. To minimize disruptions caused by these failures, businesses and government agencies must focus on contingency planning in addition to their remediation efforts.

Federal agencies are developing continuity of business plans for their core business functions. OMB, in its quarterly reports, has asked the agencies to report on their progress in this area, and is looking closely at their planning activities as it develops the President's fiscal Year 2000 budget.

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. 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.

Federal agencies have had to confront the second type of contingency planning in their relationships with the States. As I said, States help to carry out several important Federal programs, such as Medicaid and unemployment insurance. These programs depend upon Federal-State data exchange points, and agencies have been working with their State counterparts to ensure that these exchange points are compliant. But even if the exchange points are ready for the Year 2000, service delivery could still be jeopardized if the State systems behind the data exchanges fail. Federal agencies like the Labor Department, for the unemployment insurance program, are now working with States to ensure that backup plans are ready to support continued service delivery should State systems or other non-Federal systems fail.

One of the Council'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. This information will be important to organizations as they develop and refine their contingency plans. For example, everyone is concerned about having electric power, but that doesn't mean that they should all immediately buy their own generators without having a

better sense of where outages are possible and what their likely duration will be.

The Council has established cooperative working relationships with umbrella groups in electric power and other important sectors. The focus initially has been on increasing awareness and the level of activity by those operating in each sector. We are also, however, developing assessment processes whereby the umbrella groups will be surveying their members on a regular basis to determine their state of readiness. Summary reports will then be provided to the Council and the public. Over time, such information will allow everyone to adjust their contingency plans appropriately.

I might note that the Year 2000 Information and Readiness Disclosure Act will increase our ability to obtain such assessments, since it provides protection to the information provided by individual companies to their umbrella groups, thereby increasing the likelihood of candid responses.

As you know, the Federal Government, in coordination with State and local governments, plays a key role in responding to disasters and other emergencies, and is looked to for leadership at those times. I will let Mr. Suiter of FEMA describe in more detail the Federal Government's role, but I would point out that the Year 2000 problem provides a unique emergency response challenge.

With most major emergencies, such as hurricanes or blizzards, authorities are dealing with one localized problem in a town, county, State or region. With the Y2K problem, however, it is possible that emergency response systems could face multiple system failures occurring at roughly the same time and in different places.

For example, in a worst case scenario for a city or a town, authorities could face the failure of the power plant, water treatment plant, and transportation systems. While no one of them alone may be a major problem, simultaneous failures will test the capacity of our emergency response systems, and I am pleased that FEMA has agreed to chair the Council's Emergency Services Working Group.

The Federal Government has separate response systems related to specific types of emergencies. Internationally, we have an apparatus for responding to emergencies such as famine and refugee assistance, as well as military threats. Domestically, we have the systems and relationships that FEMA will discuss with you. We are presently reviewing our inventory of emergency response mechanisms and authorities to ensure there is no confusion across organizational lines on January 1, 2000, and that we can handle the possibility of multiple requests for the same resources.

In addition to FEMA, the Council is working with the National Security Council, the Departments of State, Defense, and Justice, and others who are responsible for meeting the challenges we may face, internationally as well as domestically, as we try to coordinate Federal emergency response efforts.

In particular, we are beginning to look at scenarios that may involve disruptions in key foreign countries, as well as difficulties at home, so that we can map out plans for appropriate Federal action. In foreign countries, we are concerned about how Y2K-related disruptions may affect the operation of our embassies, American citizens living abroad, and American businesses. At home, we antici-

pate that multiple burdens placed upon State and local disaster authorities may result in an increased demand for Federal assistance.

The American people have confidence in our ability to respond in the wake of natural disasters. Our objective is to ensure that the American people have the same level of confidence in the Federal Government's ability, and that of our State and local officials as well, to respond to any Year 2000-related disruptions.

We all want to ensure a smooth transition to the Year 2000. For most organizations, including Federal agencies, the primary Year 2000 focus up to this point has been on fixing or replacing noncompliant systems and embedded chips. But as we enter 1999, that will change.

The Council is committed to encouraging businesses and helping Government agencies to prepare for likely problems and develop viable contingency plans. We have to expect some problems on January 1, 2000. If we share information and plans, however, we can generate public confidence in our preparedness and minimize the impact of those problems on everyone.

Thank you, Mr. Chairman. I am delighted to respond to inquires, either now or after Mr. Suiter presents his testimony.

[The prepared statement of Mr. Koskinen can be found in the appendix.]

Chairman BENNETT. Thank you. Let's hear from Mr. Suiter and then we can get the two of you going back and forth.

STATEMENT OF LACY SUITER, EXECUTIVE ASSOCIATE DIRECTOR FOR RESPONSE AND RECOVERY DIRECTORATE, FEDERAL EMERGENCY MANAGEMENT AGENCY

Mr. SUITER. Thank you, sir. I appreciate the opportunity to be here, and it's good to see you again, Senators, under more pleasant circumstances than the last time we met on the battlefields of Maine.

I am Lacy Suiter. I represent FEMA's Emergency Response and Recovery Directorate. My directorate coordinates the Federal family's emergency response, as well as its disaster recovery, and to specific and identifiable emergencies and disasters when requested to do so by a State's governor, or in those very rare instances—this has only occurred once—when directed to do so by the President until a governor can concur.

In any event, with or without a Presidential determination, a Governor must both request and concur with any Federal disaster assistance to be provided within their State. If one views governmental relationships as vertical, then, indeed, FEMA's programs represent a bottoms up approach as opposed to a top down activities.

Y2K assessments, preparedness and emergency response begins at home, in the community and with local governments, and with the governor. Federal consequence management response and recovery essentially is by invitation only, and that invitation must be issued through the governor. It is requested by and coordinated through the governor and never independently by the Federal family.

FEMA's Y2K efforts for fire and emergency services include the following. We are one of 34 sectors, coordinated by John Koskinen.

We chair the emergency services sector. We're in the process now of assessing that sector's awareness, its preparedness and readiness to respond, were there to be catastrophic failures of systems at the State or local government level. We're developing an outreach plan for the States and for the States to use with the locals, if they so choose, and a monitoring process. We are preparing for disruptions as they are identified to us. In other words, FEMA's outreach includes awareness, assessment and preparedness.

We will provide reports in the coming weeks that, when combined with the reports of the other Federal agencies, should give us our best indication of the extent of total governmental emergency preparedness.

Y2K presents a couple of sets of response needs. First, obviously, is the technical support to operators of disrupted systems and business continuity planning. FEMA's systems critical to interagency response are ready. We have 49 mission-critical systems, 34 are compliant. There are 15 left to do. We are replacing seven of those systems and we're coming up with work around options on the other eight. All of our classified programs are all operational at this time as far as the continuity of government is concerned.

The second set of response needs is emergency assistance to State and local governments. FEMA manages the Federal response through the President's Federal Response Plan with supplements which are tailored specifically for certain types of disasters. Y2K will be one of those plans.

The regional interagency steering committees meet periodically, and they are about to get instructions to begin meeting more frequently, with the State agencies, at the regional level. These committees support the bottoms up approach of intelligence, of warning, of assessment, of preparedness, all leading to whatever the appropriate response and recovery effort might be for a particular event. We intend to exercise and do some evaluations of those activities later this winter or in early spring.

While it is difficult to define the truth on the nature and extent of the Y2K threat, planning must be based on credible assessments of specific vulnerabilities that describe the areas at highest risk and consequences. The Council's report will help us prioritize those risks and describe a plausible, worst case scenario. I meet monthly with the Federal response community to prepare our response to the Y2K problem and other disasters that occur in the country. However, the efforts of the emergency management community and fire services cannot be viewed as a substitute for personal responsibility and community preparedness. We will continue to keep you informed, sir, as we meet with your committee, on our progress as we march towards the millennium.

Thank you.

[The prepared statement of Mr. Suiter can be found in the appendix.]

Chairman BENNETT. Thank you both very much.

Mr. Koskinen, you made reference to the passage of the bill in the House, and naturally we take credit for all of the passage here in the Senate. But we will be happy to congratulate you for your leadership in getting it done in the House.

Seriously, this is a significant piece of legislation. Everyone involved in working on it I think deserves congratulations. As Mr. Koskinen and I were talking about this the day before yesterday, when we started on this, everybody told us it couldn't possibly happen. We didn't have time, it was too complicated, there are too many competing interests, everybody would stand up and say, "Well, I can't accept this, I can't accept that."

Now it has happened. It has been an incredibly interesting exercise in the present atmosphere of Washington, which might be described as somewhat polarized, where both parties, both branches of Government, the Legislative and Executive branches, both Houses, got together and said, "We are facing a genuine emergency. We must put our parochial interests completely aside to do the right thing." And while there's much that I might want that's not in the bill, that is not there, the fact that we have as much as we have and that we have accomplished what we have is, I think, a demonstration that our system still will rally to a challenge of an emergency.

I would be derelict, Mr. Koskinen, if I did not acknowledge your leadership in this, and your dogged determination to see to it that it did not die. You can take great satisfaction in the fact that this bill has now passed both houses and is on its way to the President, and I think it will make a significant difference.

Mr. KOSKINEN. Thank you, Mr. Chairman.

Chairman BENNETT. One of the things we hear so often in this committee—we've had 70 witnesses now—a common refrain from the witnesses is that it's very difficult to plan while so much is unknown. We need better information. The passage of the bill, I think, will help us get better information from people who have been hiding behind the threat of their lawyers, that they might get sued if they're forthcoming with information. But I would hope today, and if not today, at some time soon, we can begin to get some specific information out of your Council, Mr. Koskinen.

Can you give us some idea of when we will see sector assessments from the President's Council, and if anything can be done to accelerate the release of these assessments?

Mr. KOSKINEN. As I noted in my written testimony, we already have two significant assessments that have been provided to us and are available to the public. One is from our electric power working group, is working with the North American Electric Reliability Council, and the other is from our oil and gas working group, which is working with a broad number of industry umbrella and trade associations.

Approximately 2 weeks ago, they provided their first assessment of the status of both of those industries. We expect these industry umbrella and trade associations will continue to provide us that information, which we will continue to make available to the public. We have been most aggressive with these areas at the outset, because, as I noted in my testimony, everybody is very concerned about the availability of power and fuel.

We hope to have a similar process, especially now that the bill passed, for the telecommunications industry and other areas. In health care, for example, the American Hospital Association has been surveying its members about the status of hospitals so we

know that other industry organizations have begun these assessments. Now with the bill's special provisions protecting information provided for special data requests, I think that we should be able to accelerate the process.

Our plan all along has been to have at least initial assessments from the sectors by the end of this year. We chose that time because most industries have plans where by they are now completing their remediation and are beginning the testing phase. The information that all of us are most concerned about is where they are once they have completed their testing.

During the summer, the major issue was: Were people paying attention to the problem? Were they working on it? But ultimately, for emergency and contingency planning purposes, we must have the clearest possible idea as to how many people are actually going to complete the process in a timely manner. So our goal is to have, by the end of this year, as many working groups as possible produce their first preliminary assessments. But we expect to continue to receive their initial assessments as we move into early 1999.

Chairman BENNETT. For those who are watching television or who are listening and don't want to wade through your prepared testimony, will you summarize where you think we are with respect to the power grid and the availability of fuel?

Mr. KOSKINEN. Anybody who has access to the web can find them on our web site, which is www.y2k.gov. The assessments are provided in our groupings for industry sectors. And we will continue to make assessments available to the public as we receive them.

As a general matter, the NERC report for electric power was a balanced document. NERC was pleased to note that there appeared to be less of a challenge than originally thought with regard to embedded chips in electric power, both in generation and distribution processes.

On the other hand, NERC said that significant portions of the industry needed to accelerate their rate of progress to meet their goals of finishing work by the spring of next year, and they issued guidelines to help facilitate greater progress.

The oil and gas assessment report shows that half the industry is well into remediation and compliance, and the other half is still working through planning and assessment. the industry groups that produced that report also noted that there is an urgent need for the members of those industries to increase their rate of progress.

What we have asked these working groups to do, and we will ask this of all the working groups, is to prepare an analysis that divides those responses by the size of companies reporting, because both reports indicate that the concern we've all had about smaller organizations still holds true. In these industries and others, the large organizations, almost by definition, have built-in capacity to deal with this problem. So whether you're looking at financial services or telecommunications or power, you find that large companies tend to be working on the problem aggressively, and are deploying substantial financial and personnel resources toward solving it.

The concern we all have—and these reports mirror that concern—is with the status of small and medium-sized enterprises. In

telecommunications, we have 1,400 small telephone companies that deliver services to small towns and rural areas. In fact, as a general matter, the Rural Utility Service advises me that 20 percent of all utility services are actually provided in rural areas of this country, generally by small and medium-sized organizations. So we are focused, and have been for some time, on trying to increase the level awareness and activity in smaller organizations. I think the advantage of these assessments is that we will be able to quantify the magnitude of the challenge and hopefully increase the level of activity in smaller organizations.

I should put a plug in here for National Year 2000 Action Week. The SBA had started a program that designated the week of October 19 as Year 2000 Action Week, with SBA field offices holding educational events across the country. We have expanded upon that, focusing on both small and medium-sized businesses, by inviting local offices from other agencies to hold Y2K events during the week as well.

The Department of Commerce will be participating. The Department of Transportation's regional offices will be participating. The Social Security Administration's offices will be participating. The goal is to make a full court press in local communities across the country, to get small and medium-sized organizations to understand that it's critical for them to solve this problem.

Chairman BENNETT. That assessment will be very valuable.

The Small Business Committee on which I sit, in the next Congress, is going to have to address the question of whether or not a new category of SBA loan needs to be created for the purpose of helping smaller enterprises deal with the financial challenge here.

One of the reasons that the bigger enterprises, as you indicate, are in better shape is that they have the financial muscle to tackle this. I say to people, you know you're dealing with the CEO who understands the problem, when he or she tells you that it's costing far more than was originally anticipated. Many small businesses that are on the edge of profitability all the time simply don't think they have the resources to deal with this. They're going to have to borrow somewhere, and many, many banks will say we won't accept Y2K as collateral for an SBA loan. It may be an emergency, but how are you going to pay it back.

So the quicker we can get this kind of information from you, the better off we, the Congress, will be in fashioning some kind of emergency loan program through SBA or elsewhere, to help small businesses that simply cannot solve their problem for financial reasons with some financial emergency money.

I know FEMA doesn't normally deal in that kind of issue. You come along, or the Federal Government comes along, with loans after the fact, when there's an earthquake and something has to be rebuilt. But here's one where we know the earthquake is coming, we know exactly when it will hit, and maybe we had better deal with the financial services before the fact, to try to shore up the structure so they don't collapse with the earthquake.

I had better get away from that analogy in a hurry.

Senator Collins, I would appreciate your questions.

Senator COLLINS. Thank you, Mr. Chairman. Again, I want to commend you, Mr. Chairman, for your leadership on this very im-

portant issue. Good morning, gentlemen. I want to take this opportunity to thank Mr. Suiter for all of the assistance that FEMA gave to the State of Maine during our ice storm in January, which was the biggest natural disaster in Maine's history.

In many ways, State, Federal and local disaster authorities worked very well together to cope with the ice storm's aftermath in Maine. But the ice storm also pointed out vulnerabilities in our emergency response system.

One of those vulnerabilities, to me, is very similar to the kinds of problems that a Y2K failure could create. For example, because the electric grid in Maine was essentially knocked out for many days for much of the State, the State's emergency broadcasting system was also inoperative for at least a week. That system is maintained by Maine Public Radio, which lost its transmission facilities completely for several days. Some Republicans thought that was a good thing, that Maine Public Radio was off the air. [Laughter.]

I am not one of those who did. But on a serious note, it really was a problem, that the State lost completely its capacity to have an emergency broadcasting system during that time.

Has FEMA taken the experience in Maine and other areas of the Northeast, where there was a widespread failure of the electrical system, and drawn any lessons from that experience as far as emergency response systems and the need for a coordinated response at all levels of government?

Mr. SUITER. Of course. Most of the missions that we deal with following earthquakes, major floods, or hurricanes, which I've just been down on the Gulf Coast reviewing, deals with what happens when major systems fail. They usually fail because of some natural cause. Y2K happens to be something else. So, yes, we always evaluate what we did, how we it, and what do we have to do to improve in the next disaster, and then try to apply those lessons to our long-term planning.

In this particular instance on the Gulf Coast, we discovered that we didn't have the right size generators, and the prime power assets that we needed to get them hooked up as quickly as we possibly could.

Obviously, we're leaning forward in the foxhole for Y2K so to speak, in terms of our readiness to inform the public about what's going on, which systems have failed, and certainly using the media to get the word to the people, is one of our most important efforts. Senator Collins. I'm going to talk later in my opening statement about the 911 system, and the potential vulnerabilities that have been identified in the 911 system.

Has FEMA done any work in this area yet, to assess the 911 systems that are so important in our States and local communities?

Mr. SUITER. We haven't finished it yet, but we're in the process. There are three or four different agencies who are working on that. The United States Fire Administration, a part of FEMA, is working directly with the fire service organizations, the fire chiefs and so forth, as well as the suppliers of these particular groups. Second is the Department of Justice, which is working with the law enforcement side of the 911 system, and third is the Department of Transportation, which has responsibility for the emergency medical services.

FEMA is reviewing all of this and coming out with a report, which is not complete, and we will be advising back to those districts in the country about the 911 system and what we need to do to fix it, or be ready if it fails.

Senator COLLINS. When do you expect your assessment to be completed?

Mr. SUITER. We're working with the Federal agencies right now, on a monthly basis. We were supposed to have met this past Wednesday, but unfortunately I was on the Gulf Coast dealing with the hurricane so we had to postpone that a couple of weeks.

We expect to finish our initial assessment, of the Federal Government's capability to respond, in the next few weeks.

We plan to have our evaluations ready for John's Council by December: Federal response planning should be based on what we know at that point in time.

The Director of our agency, James Lee Witt, plans to make a report specifically to the governors at the NGA meeting here in Washington in February of 1999. FEMA will be conducting, in cooperation with John Koskinen, some exercises and evaluations in April 1999, followed then with specific corrective actions—such as pre-deployment, if that's what it takes, a warning system to monitor Y2K as it works around the world so that we see what's happening and could get as much advance warning to our local governments, through our State governments, as we can.

So yes, I think we're doing quite a bit. We're going as rapidly as we can. Given all the rest of the disasters going on—there are 31 open disasters as we speak right now in the United States that we're dealing with—we're stretched kind of thin. But we think we're making good progress and I don't think Mr. Koskinen is too unhappy with me yet.

Senator COLLINS. Thank you, Mr. Suiter.

Mr. Koskinen, in the Federal response plan, Executive branch agencies play an important role in the emergency support systems, such as transportation, health and medical services, public works, et cetera. Yet it's my understanding that the agencies that are responsible for some of these emergency support systems—the Department of Transportation, for example, Health and Human Services, Defense—are listed as Tier 1 agencies. It is my further understanding that Tier 1 agencies are those that face the greatest challenges in becoming Y2K compliant.

That troubles me because, if we're relying on those departments in an emergency situation to provide emergency support services, and if they are having the greatest difficulty, what does that suggest for our ability to respond to an emergency?

Mr. KOSKINEN. It's an important question and I am happy to answer it.

While the OMB Tier 1 agencies face challenges, it's because of particular aspects of their operations. In no case is the ranking reflective of their emergency response capabilities. In fact, as Mr. Suiter noted, one of the first things our emergency services working group did was pull the Federal response agencies and others together to review the status of their own systems as they relate to the Government's ability to provide emergency response.

Lacy knows the details better than I—but as a general matter, agencies, particularly Transportation and HHS, are in good shape with their emergency response capabilities. They're either up to speed or will be by the end of this year, so there will be no problem with emergency response capacity.

But you're right. Agencies like HHS, with the Health Care Financing Administration, and the Department of Transportation, with the FAA, face significant challenges and are focused on overcoming them.

Senator COLLINS. Thank you, Mr. Chairman.

[The prepared statement of Senator Collins can be found in the appendix.]

Chairman BENNETT. Thank you very much.

Vice Chairman Dodd.

Vice Chairman DODD. Thank you very much, Mr. Chairman. I thank our witnesses.

It may have already been said, Mr. Suiter, but I'm sure all of us express our tremendous appreciation on how well FEMA has been responding over the years.

Lower New England has not been faced with the problems of my colleague from Maine, but I know an awful lot of people in my State went up to Maine during the ice storms and I think there's a general sense that your agency is doing a tremendous job across our country in responding to these natural disasters that have occurred.

I'm really very grateful. I hear it all the time. We don't hear a lot about Federal agencies, but we do hear it about FEMA today. I want to commend you and the people who work for you for the tremendous job you're doing.

Mr. SUITER. Thank you, sir. We have a great Director in James Lee Witt in providing that leadership.

Vice Chairman DODD. I know you do. He's very vocal and outspoken, and I have referred to that on numerous occasions.

I guess I find myself again in that sense of—maybe I'm the frustrated member up here, I guess. We have 15 months, five quarters, 455 days to December 31st. I'm very uneasy about the fact we don't have assessments. Generally, we've had 70 witnesses before this committee. The chairman has done a terrific job in trying to expedite a lot of hearings. Generally what we hear from witness on this, their response is that it's very difficult to plan while so much is unknown. We need better information.

We hear from Federal agencies and are frequently told that they're waiting for guidance from the President's Council. We hear this all the time from people that come up, that we're going to wait for the President's Council to get back and so forth on these assessments. I'm just very uneasy that time is moving along here and we're not getting these assessments laid out so that we have a much clearer plan as to how to respond to potential problems.

You said you were hoping by the end of the year to have these, but could we get a better feeling? You know, that's going to shorten up that calendar even more, about whether or not we can get these assessments, so that these agencies can start making very specific plans to minimize the potential impact of this. It might seem like I'm hounding on this, but you understand my frustration here. It

seems vague, and I watch this calendar go by day after day. I'm just uneasy about it, to put it mildly.

Mr. KOSKINEN. On behalf of those of us who have clocks on their desks that count down the days, I'm uneasy as well.

Vice Chairman DODD. I know that.

Mr. KOSKINEN. And it's a critical issue.

As I mentioned earlier, we already have two significant assessments that are provided to the Council and are now in the public domain, one for electric power and the other for oil and gas. These are two critical parts of our infrastructure and we're pleased to have assessments on progress in these areas.

We continue to encourage umbrella groups to provide us assessments for other areas as well. As you know, we have no authority to require those assessments by industry, but the legislation is a critical lynch pin in making them possible, because it provides specific protection to companies and umbrella groups who collect this information for us. We think it will improve the ability of those groups to gather candid information from individual companies, and to ultimately provide us accurate assessment information.

Part of the difficulty—and we're all frustrated by this—is that everyone, both in the Federal Government and in the private sector, is now moving through the remediation phase and into the testing phase. Virtually no industry will have compiled significant testing results until the end of this calendar year.

Right now, our assessments give us a picture of the level of activity. But what we really are looking for, and we hope to begin receiving this in hard terms, are assessments of actual readiness. Who has completed their tests? What is the level of compliance? Our ultimate goal across all of the working groups, through voluntary working relationships with umbrella groups and industry associations, is to get detailed assessments that will tell us the state of preparedness.

Even without detailed assessments we do now know of several areas of concern, and we are focused on them accordingly. One is international, in terms of the lack of preparedness in many countries. Domestically, as I said, we are very concerned about small and medium-sized organizations, both in the public sector as well as in the private sector. So we are mounting a full court press, to increase the level of activity in those areas, to the extent we can. At the same time, we are also continually trying to refine our assessment of the severity of the problem in these areas.

I think, when we get to the end of next year, our difficulties are going to come not from the major companies but from small and medium-sized organizations, which have the capacity to create substantial disruptions on the local level. While they may not bring down the entire country, if you're living in an area that suddenly finds that its local power company or telecommunications company or water treatment plant doesn't work, you have the equivalent of a major disaster on your hands. That's what we're trying to isolate as best we can.

Vice Chairman DODD. I appreciate that, and I understand you don't have legislative authority. Maybe it's something we should have thought about. But aside from that——

Chairman BENNETT. If we get past S. 2000, we would have. We tried, but we ended up with what we could get.

Vice Chairman DODD. Yes.

You know, there is the power and authority that we sort of extended, if not de jure, de facto, to you, as sort of our "Tsar" of this. I don't know if other members of the committee feel this way, but you certainly would not hear any complaints from me if you were to set dates. There's nothing like having a mark out there, saying to people, "Look, I expect by December 15, or January 10—" and I realize there might be different dates for different agencies, depending upon the complexity. It's not a one size fits all.

You know, I'm expecting that back. When it's a little vague out there as to when it comes—I suspect it's not a whole lot different when you're dealing in these agencies than it is with sort of the reaction we get from colleagues and others when we bring up this matter. We get a bemused look on faces of people.

I don't know if that's something you feel comfortable in doing, and if anyone complained about it, I would be more prepared to go to your defense and suggested that we do need time tables here, and to let agencies know we're expecting them to get back so that those assessments can be made by certain dates.

For instance, I don't know—Mr. Suiter, can you plan effectively without an assessment?

Mr. SUITER. Well, we have to respond to the unknown at all times. We need the assessment. It would focus what we're doing, but in the things we do, we deal with the unknown, the unexpected.

I'm sitting here right now, but very well, by this afternoon at 6:00 o'clock, I could be in San Francisco dealing with a catastrophic earthquake. We know the parameters of what a major earthquake would do in San Francisco, so we plan backwards from there. Yes, we need the assessment.

Vice Chairman DODD. I understand that. My point is that here you need to assessments in order to——

Mr. SUITER. Yes, we do.

Vice Chairman DODD. That's what we're talking about here. That's what we have got to get if we're going to move effectively on this.

It may have been asked by the Chairman or someone else already, but do you have any plans to preposition core reserves of personnel, equipment, in anticipation, for instance, on December 31, where you may have power outages and shortages, not because of an act of God but because of this very predictable problem? You don't have to worry tomorrow on whether or not January 1, 2000 is coming. I promise you, it's going to come. We know there's a potential here for some serious problems. We all hope it doesn't happen, but we know—we're sitting here today, with 455 days to go, and we know that there's a real potential for serious disruption in this country and elsewhere. You don't have your assessments so you really can't plan that effectively, but there are some things that can be done.

Are such things such as the prepositioning of personnel and equipment to deal with this potential problem in place?

Mr. SUITER. Yes, sir.

Vice Chairman Dodd. Thank you, sir.

We have a vote coming up, so I would yield to my colleagues. I do have more questions.

Chairman BENNETT. Senator Smith.

[The prepared statement of Senator Smith can be found in the appendix.]

Senator SMITH. Thank you, Mr. Chairman. Gentlemen, thank you for being here.

Last evening on ABC national news there was a story that caught my attention about Lubbock, TX, who prepared to simulate as many Y2K tests as possible. When the city moved the calendar ahead to December 31, 1999, the story indicated that the fire departments, radio communications, and gas to homes just shut down. The story also indicated that 80 percent of American communities are not even doing anything about Y2K at this point, or at least working on solving the problem.

Is Lubbock unique in that they actually tried to simulate a test and demonstrate what would happen?

Mr. KOSKINEN. They are unique in the sense that they're the most visible community that has done it, and we applaud them for it. As I noted earlier, the Federal Government doesn't even have direct lines of communication with many local communities, but we are working with national organizations representing city executives, county executives, the National Governors Association, to urge them to, in effect, replicate what Lubbock is doing. We need to have people at the local level, at the grassroots level, ask the questions that Lubbock is asking itself.

What does happen if these failures occur? What are we doing to avoid them and, if we can't, how are we going to respond? One of my great concerns is—and whether it's 80 percent or not, I don't know—that a lot of small and medium-sized cities and counties at this stage have not yet understood that this problem could have an immediate and important impact on their citizens as we move into the Year 2000.

Senator SMITH. If Lubbock is any indication, then we'll have a serious problem. You know, I've been saying in Oregon that we should be prepared, we shouldn't panic, but if Lubbock's experience is any indication of what can happen, maybe it's time to panic.

Are there any States, any regions of the country, where you are particularly alarmed, that would suggest this 80 percent may be accurate?

Mr. KOSKINEN. I think the 80 percent is probably on the high side, based on the anecdotal information and surveys I've seen. If you look at surveys done on small businesses, they generally show that about 40 percent of those surveyed aren't planning on doing much, which I have said is rolling the dice on whether or not they're going to stay in business. My expectation is we're at a similar level with small and medium-sized cities and counties.

But clearly, our dealings with States, counties, and cities have demonstrated that they too are concerned about the difference in preparations among larger entities compared to their smaller counterparts.

Large, industrialized cities and States understand the problem and are dealing with it. They haven't solved it necessarily, but

they're dealing with it. But when you start to get to smaller organizations, the initial problem has been the perception of applicability. People think, if they're not running a major mainframe operation, processing millions of transactions, that somehow it's not their problem. But they haven't understood the impact of integrated circuits, microprocessors that affect virtually everything that runs in this country. So we are trying to encourage more communities and community action groups to focus on the issue at that level.

As I have said—and the chairman and I have talked about this—the Federal government faces substantial challenges, and we need to focus on them. But this story is more than just a Washington story. We have to expand it. It has to be a question of what's going on in cities and counties across the country, and those issues have to be raised by public citizens as well as political officials in those areas.

Senator SMITH. Thank you.

Can Y2K be declared a special event, those words of art, and if so, what will that allow us to do? Is there a category under FEMA called a special event.

Mr. SUITER. We don't have a category called special event, per se. The President could make that determination. That would allow us to respond, if requested to do so by the Governor.

If I might comment on Lubbock, TX, if I could for a moment, Lubbock, TX for years has been a leader in any number of emergency management and fire service responses and have set the mark for other cities and communities across the country to follow. They had a catastrophic tornado there many years ago, and they learned those lessons at that time and they haven't repeated those lessons. It's a model for the rest of the country to follow.

I don't know how many other cities are doing that to that extent now, but that will be a part of our report for you.

Senator SMITH. Thank you, Mr. Chairman.

Vice Chairman DODD. Coming up on the next panel, by the way, we have the city manager of Lubbock, so you may want to——

Mr. KOSKINEN. It's called a well-organized hearing.

Vice Chairman DODD. I'm sure his ears were perking up over there.

Chairman BENNETT. Mr. Suiter, when did FEMA begin the Y2K annex to the Federal response plan, and how are you ensuring agencies such as DOD, which will play critical roles in the plan, will be ready?

Mr. SUITER. We've been planning our part of this, as far as the supplement to the Federal response plan, about 4 months. The last report would have been September 30. But as I said, I had to postpone that for a couple of weeks here.

What we have asked all the Federal agencies to do, including the Department of Defense, is to report back to us in convincing terms that they will have the ability to communicate up, down and sideways with their resources when asked to provide some specific response to our governors' request and to the President. That's precisely where we're working.

All of this begins at the local government level, and how we communicate up and down and sideways with each other are the interdependencies, the critical part of it. So that's a part of the response

that we plan to have ready by the 1st of December here. We will have a better evaluation by that time.

The initial reports, sir, are not that bad, and they're in the very narrow focus of interoperability and how they move their resources to get our part of the mission done. I don't know about the rest of their agencies.

Chairman BENNETT. The more I hear about DOD, the more sympathetic I become, and at the same time, the more worried I become. DOD has so many internal problems of their own, and then here you come along and say we're going to draw on DOD resources to deal with emergencies.

We have had some testimony with respect to their readiness impact as well as the impact of Y2K on national security with respect to military readiness, and now we're aware that they play a role in other places. Being sympathetic with their problems doesn't mean that we can allow them to slide by, however. We're going to have to keep pressure on them.

Mr. SUITER. I think you would be very proud of the response of the Department of Defense in helping people of the Commonwealth of Puerto Rico right now. We have planes landing and taking off many times a day, and they're bringing in critical supplies such as water, ice, baby food and other products that we could not get in there without the resources of the Department of Defense. There are C–5A's, 141's, constantly responding around the clock. We know that part of it is going to work OK for us. I don't know about the other parts.

Vice Chairman DODD. As an aside to that, the northeast utilities in my State, one of the companies has volunteered to send personnel and equipment down. I called last night and they were told the trucks they want to send down has to be sent by barge, which takes about five days to get down there. Since you're here I'll make a pitch and appeal. I wonder if there's any way you could fly some of those vehicles in down there.

Mr. SUITER. I'll look into it for you, sir. I can't report off the top of my head.

Chairman BENNETT. Senator Collins, anything further?

Senator COLLINS. No, Mr. Chairman.

Chairman BENNETT. All right. We promised Mr. Koskinen we would get him out of here by 10:30, and we're 2 minutes in advance. I think we have a vote scheduled at 10:30, do we not?

Vice Chairman DODD. We do. We haven't scheduled——

Chairman BENNETT. I'm told it is 10:45.

Vice Chairman DODD. May we submit some additional questions? I know John has to be moving along, but some of this gets pretty technical in terms of follow up and so forth. Like the 17 hour rule—is it 17 days or 17 hours?

Chairman BENNETT. 17 hours. I didn't get into that; I thought I would now as we're waiting for the vote.

Mr. KOSKINEN. That sounds like a good question for Mr. Suiter to answer. [Laughter.]

Let me express my appreciation to the Chairman and the panel for accommodating my schedule which allowed me to appear with you this morning. I think it's another in a series of very critical issues that you're dealing with, and we look forward to continuing

this dialog and working together as we move through, as Senator Dodd noted, the remaining 455 days.

Than you all.

OPENING STATEMENT OF HON. ROBERT F. BENNETT, A U.S. SENATOR FROM UTAH, CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Chairman BENNETT. I had made reference to the First Alert system in my opening statement, which I deferred until now. Let me go through that so that everyone can understand what we're talking about.

We have noted a potentially serious oversight and at the same time unique opportunity with respect to the millennium change. We tune into the National Weather Service and say what's going to happen with the hurricane and hope that they can give us an advance alert. But with respect to Y2K, because of the way the world is organized, we will have an advance alert in the form of one hour at a time moving through the world's clocks.

With the vice-chairman, Senator Dodd, and Senator Collins, I am announcing the committee's pledge to establish a Y2K First Alert system that will enable citizens of the United States to have up to 17 hours of advance warning of the nature of the Year 2000 disruptions. Just think about the time zones around the world. Citizens living west of the Eastern Standard Time zone will have progressively more advanced notice. In Utah, we'll have 19 hours of advanced notice, and citizens in Hawaii and those in the farthest reaches of Alaska would have almost a full day advance warning.

Vice Chairman DODD. How much do Susan and I get?

Chairman BENNETT. You're stuck with 17 hours.

The new day begins at a spot in the middle of the Pacific Ocean, 17 time zones earlier than Eastern Standard Time. If the Y2K bug is potent enough to cause immediate problems in information systems and embedded chips, you will have a 17-hour description of what those problems are and it will move progressively around the world.

The stroke of midnight in Wellington, New Zealand won't occur in the United States until 17 hours later, and then in California 3 hours after that and so on.

We think it's foolish not to use this advance notice and we're going to do what we can to make sure that the implementation of a 17-hour advance watch system is created. Frankly, Mr. Suiter, we'll be working closely with FEMA to have you work with us within the context of your existing authority to achieve this goal.

Now, we've been talking about preparedness. I have had a chart prepared, over here to my right. I will just walk you through it so that everybody can understand why we are focusing on that here today.

Let's take a fire, as depicted in this picture, that occurs in a high-rise building. I will walk through the various places where we could have problems.

Vice Chairman DODD. Just let me say that I thoroughly endorse the Chairman's idea here on this. He has announced it for all of us, but I think it's really the kind of far-sightedness that I think is going to be tremendously helpful. So before you move your

charts, I just wanted the record to reflect that I think this is a very sound and wise suggestion. Hopefully we'll discover early on that there's not much to worry about, but if there is, it will be of some help to us. I commend you for it.

Chairman BENNETT. Thank you.

On this burning building, the alarm on the premises would have to operate correctly to warn that a fire had broken out. Has the alarm system been certified as Y2K compliant? Then it would automatically alert the fire department through a 911 call. Does the telecommunications system that handles the 911 call have Y2K problems, and has the 911 system that receives the call been remediated to be Y2K compliant?

Now, the computer aided dispatch. The call comes in from the building, everything is compliant, and now we dispatch the fire truck. That system has computers in it. Is it Y2K compliant in order to make the right kind of dispatch, or is there a contingency plan in place in case that fails?

The emergency vehicles start on their way. They have to be fueled. How about the city government fuel pumps, are they compliant, so that the emergency vehicle can get there? If not, again, is a contingency plan in place with alternative agreements struck between the city and local gas stations?

Now, there needs to be personnel on that truck, and the scheduling tool that sets shifts for people to come to work probably is computer operated and it needs to be checked so that the personnel are scheduled properly.

The traffic signals along the route to get there need to be compliant so that you don't have gridlock that the emergency vehicle can't get around. Has the local transportation department examined these?

So let's assume that all of those are proper and you get to the scene, the firefighters now need a reliable source of water. What about the local water supply, is it dependent on any kind of central pumping system and will there be water in the fire hydrant?

Medical equipment on the scene. This harks back to the hearing that Senator Dodd spearheaded for us, is all of the medical equipment in the paramedic's truck Y2K compliant and will it work? Of course, we have already gone through the very basic question of whether we have power overall. Was the fire department able to check its database to see if the hazardous inflammable equipment stored at this location was compliant? And so on and son on.

So here we have a single burning building, but it illustrates the complexity of the Y2K difficulty that could hit us everywhere.

[The prepared statement of Chairman Bennett can be found in the appendix.]

Chairman BENNETT. Now, the vote has been called.

Mr. Suiter, do you have a comment on this one example of a disaster out of your experience?

Mr. SUITER. Only that if you add the thousands of buildings all across the United States that might experience the same thing at the same time, you're exactly correct in your characterization of the problem.

The only thing to add is the additional unknown of what is the Y2K impact on that if these systems fail. If we were to take you

from Baton Rouge, LA all the way to Fort Walton Beach, FL right now, you would have seen that almost all of those systems failed in terms of what we depend upon for as single house fire or a single building fire, in terms of all the power outages. We had no traffic control system; water pumps were down to pump the water. So the whole system is dependent on manual back-up systems, that someone who knows that community, understands their responsibility, can operate even if some of these critical systems fail.

The part that we have to really be reporting back to you on, and soon, though, is what is the impact of Y2K if all these systems fail simultaneously and communities don't have a back-up plan for how they're going to respond to this.

We agree with you 100 percent. It was from your staffs that we got the idea of the advance warning program. That's why our people are working on it, and we plan to continue to work with you and to get suggestions from you, but also to offer to you what we plan to do in that area. We will be speeding it up. That's a very important characterization and I would like to use it.

Chairman BENNETT. It's not copyrighted.

Mr. SUITER. Thank you.

Chairman BENNETT. You can have the picture and the chart and, as far as I'm concerned, drop it out of B–29's over the local populace.

Mr. SUITER. We plan to do just about that, sir, in our outreach program.

Chairman BENNETT. OK. A vote has been called, so the committee will stand in recess until we can——

Vice Chairman DODD. Mr. Chairman, I have an opening set of remarks. Maybe I could do that while you go vote, instead of taking the time later, and then when we come back we can go right to the questions. All right.

Vice Chairman DODD. I would like to make some opening comments in support of what you're suggesting.

Chairman BENNETT. OK. Very good. We will turn the gavel over to you and we'll get back in time for you to go vote.

Vice Chairman DODD. And I promise not to pass any legislation in your absence. [Laughter.]

Chairman BENNETT. Since we don't have any legislative authority, that's probably a safe promise.

STATEMENT OF HON. CHRISTOPHER J. DODD, A U.S. SENATOR FROM CONNECTICUT, VICE CHAIRMAN, SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM

Vice Chairman DODD. Well, that has never stopped committees around here from trying anyway.

I thank you, Mr. Chairman. Again, I want to commend FEMA, and I know all of our colleagues have been doing just a great job. I wanted to begin and end my remarks with that and emphasize what I think is important in this area as well and sort of encourage you. I'm looking forward to hearing from Governor Leavitt and some of our local folks as well.

Getting people to think about this is really, about 80 percent of it is getting people to think this and asking each other the questions about how do we respond to this stuff, it really takes us a

good distance down the road of addressing the potential problems we face here.

Again, with the various sectors that we're all aware of here—in fact, we will be holding soon a general business hearing, with an emphasis on small business, just another aspect of this.

Today, of course, as we have heard already, we are going to review emergency preparedness and disaster relief at the national, State and local level. Indeed, few functions of government are more fundamental and important than our government's readiness to respond to the needs of its citizens in emergencies.

These emergencies, again as we've all noted today, can be on a grand scale, such as floods, tornadoes and earthquakes, or they can be personal emergencies, where one person may need the police, the fire department, or an ambulance. In all of these situations, there is a shared common denominator, and that is communication systems that receive the calls and direct the responses to those emergencies. Most importantly, these systems may be very vulnerable to Year 2000 problems.

Sophisticated information technology systems serve as important tools for law enforcement today. Systems such as the National Crime Information Center, or NCIC, the National Law Enforcement Telecommunications System, or NLETS, and individual criminal information data system operated by each State, enable officers to obtain the most updated information on wanted persons, stolen vehicles, criminal histories, and Department of Motor Vehicle records. The ability to dependably and quickly access such information is essential both to officer safety and to the speedy and effective administration of justice at all levels.

A recent survey—and I found these statistics interesting—conducted on the effectiveness of NCIC indicates that during a 1-year period, 81,750 "wanted" persons were found, 113,292 individuals were arrested, 39,268 missing juveniles and 8,549 missing adults were located, and 110,681 cars valued at over $570 million were recovered as a result of NCIC's use.

The good news is that we have been assured that this system will be fully able to meet its Year 2000 challenge, and that its links to the systems of all 50 States will remain fully operational. The challenge for local law enforcement agencies is to be sure that their own links to these vital information systems, and any similar systems which they might operate on a regional or agency wide level, are both compliant and compatible with the larger systems.

Also, at the local agency level, there often is a great deal of interconnectivity between some of the emergency service department's records systems and those of other city agencies, such as the court system, the corrections department, and even local utility companies, thus increasing the potential for Y2K related problems in this area.

As we have found to be true in so many other areas, Y2K's presence is insidious in the area of emergency services. One major police department related to our staff that its city government was required to remediate their gasoline pumps in order to assure that gasoline would continue to flow to its patrol cars on January 1, 2000. I wonder how many departments have made a similar assessment.

This problem had the potential effect of an entire fleet of city government-owned vehicles being shut down. In this particular case, the computerized gasoline pumps perform a time and date calculation based upon the last time a particular gas credit card was used to fuel a vehicle and, therefore, was vulnerable to the Y2K issue. In other case, the sheriff of a large western county related that his department was currently examining its computerized detention files which are used to track "time in" and "time out" of the county jail facility, as well as hearing date information for inmates.

According to the Bureau of Justice Statistics, there are over 17,000 police and sheriff departments in the United States. The International Association of Fire Chiefs estimates that there are 32,000 fire departments in this country. We also should not overlook the fact that approximately 65 percent of our country's Emergency Medical Service agencies reside within the organizational structure of our Nation's fire departments.

I think these statistics clearly indicate to all that the potential scope of the emergency service sector at the State, county and local levels of our Nation is enormous. The task of assuring that each of these agencies meets the challenge of providing uninterrupted and reliable service in the Year 2000 is an immense one. It is a task that must be tackled at each and every city, township, county and State government in the Nation.

In addition to the technical aspect of Y2K vulnerabilities, we must also consider the possibility that January 1, 2000 may bring with it an enormous increase in the demand for service from our emergency response agencies. Will there be an increase in the need for additional traffic control personnel in the event of certain Y2K failures in the transportation sector? How many additional elevator extrications will the fire departments be called upon to perform? None, we hope, but these are all things that we must consider as we plan.

While the preparedness of emergency service agencies is the most vital aspect of Y2K preparation for State, county and local governments, we must recognize that it surely is not the only Y2K problem that those governments will face. It is, in fact, only one aspect of the much larger Y2K challenge confronting the mayors, city and county executives, as we'll be hearing from shortly from around our Nation.

Again, I want to commend FEMA for what it has done in these other emergencies, the natural disasters. But there are a lot of these questions that I hope are being raised at the local level as they think through and examine—I wouldn't have thought that a gasoline pump or county vehicles would be an issue, but yet this smart town made that assessment and found out it was a problem, and had they not fixed it, would have faced a situation of those pumps shutting down. It might mean nothing if nothing else happened. If you had a major problem in your city, it could really be a serious, serious issue.

Again, I'm not an alarmist about this. We have time on our hands. But I think what Senator Bennett has been doing will raise the level of awareness, to get people to think about this. It doesn't take much time to think about it and take a good hard look at

what exists, what potential problems exist. I think it's just the wise thing to do.

Again, I appreciate the patience of the audience in listing to this, but I wanted to share those statistics, which I thought were fascinating, in terms of the numbers of interconnections that exist around the country.

With that, the committee will stand in recess for a few minutes until the Chairman comes back.

[Recess.]

[The prepared statement of Vice Chairman Dodd can be found in the appendix.]

Chairman BENNETT. The committee will come to order.

We apologize for the fact that the Senate has a way of intruding on our business. They require us to vote and that is, of course, what we're here for. So we appreciate the indulgence of the witnesses. The other Senators will be back, I'm sure, after they have voted.

We now turn our attention to governmental activity outside the Federal level. I would like to lead a discussion with those at the State and local levels who must respond to the challenge of the Year 2000.

I would like to refer to another chart in anticipation of our witness for the Governors, entitled "The Year 2000 Status of the 50 States". It's right next to the burning building over there. That's not a deliberate juxtaposition; that's just kind of the way it got placed.

It shows the state of readiness of the 50 States. The first blue block, for those of you who can't read the label, says "Uncertain". That is just under 10 percent. Level I means they're getting started, they have identified a champion or tsar, working on awareness, and beginning an inventory of the problem. Again, that's just under 10 percent.

At Level II, developed a detailed inventory of operational dependencies. That's the third block over from Uncertain and Level I.

Level III, or the fourth block over, has a project plan completed, resources assigned, made detailed risk assessment, they remediate and test 20 percent of the mission critical systems, reviewing their vendors, and they are completing contingency plans. That, of course, is up to almost half the States.

The next two levels, while there is a small blue square there, in fact, are at zero. Level IV would be completing remediation and testing of the remaining 80 percent of mission critical systems, with contingency strategies implemented for mission critical dependencies. In Level V, remaining systems and dependencies completed and policies in place to avoid noncompliant issues after compliance is reached.

Now, the source for this information is the Gartner Group. If Senator Dodd were here, he would point out that they are located in Connecticut. We don't know that these numbers are exactly precise, but that's the first cut that has been made by a group who have spent a great deal of time on this issue and that's their assessment of where we are.

[The referred chart can be found in the appendix.]

Chairman BENNETT. We will hear from Governor Leavitt. We understand the self-reported numbers from these States are different from the numbers from the Gartner Group, and we will explore that.

I am also happy to point out that the National League of Cities and the National Association of Counties is putting out this packet called "Y2K and You". It consists of a folder with some useful information in it, and this little bulge in the packet is a videotape that addresses it. Here is the folder. It has a "Guide to Y2K and You", and then in the other part of the folder an overview of frequently asked questions, hot buttons, Y2K dos and don'ts, and cooperating organizations. This is useful information from the National League of Cities and the National Association of Counties.

Then here is an example of a Metropolitan Washington Council of Governments publication, "Year 2000 Best Practices Manual." This shows the kind of effort that is being made, at least in the greater Washington area. The one question I keep getting asked and can't answer, which may be in this: "Is Metro going to work in the Year 2000?" We will try to find that out, and as soon as we do, we will report it.

I do not have a corresponding chart for cities and counties. This kind of information is very encouraging, but I do not know anyone who has attempted to assess the state of awareness in cities and counties the way the Gartner Group has done for the States. I share that with you to set the stage for the conversations that we are now going to have.

We welcome to the panel Gov. Michael Leavitt. He comes from a State that I consider enormously outstanding. He is the Governor of my home State of Utah. He and I share the distinction of both having finished second in the party conventions, where we sought our party's nomination in 1992. He was a close second; I was a very distant second. In the primary that was subsequently created by that, he won his primary very handily and I did it just by a hairs breadth. But close only counts in horseshoes and hand grenades. If you win, you win, in politics.

Governor Leavitt has been an outstanding chief executive of the State, and sometimes we get together and reminisce on our days in the political trenches. Governor, we're delighted to have you here. He will be the Chairman of the National Governors Conference during the year that the governors will be discussing and grappling with Y2K problems, so he is a logical spokesman for the governors.

Senator SMITH. Mr. Chairman, as one whose paternal ancestry is also from Utah, I would like to say that I think Utah is at least the second-best State in the Union. [Laughter.]

Chairman BENNETT. I think we had better move on before the other members of the committee get here. But we appreciate that.

Governor LEAVITT. That wasn't a logical follow up to Senator Bennett's suggestion that second was attractive, I guess. [Laughter.]

Chairman BENNETT. With the Governor on the panel we will have Maj. Gen. Edward Philbin, who is the Executive Director of the National Guard Association; John Thomas Flynn, who is the chief information officer of the State of California and president of

the National Association of State Information Resource Executives; and Miss Ellen Gordon, who is administrator of the State of Iowa's Division of Emergency Management, and she is president of the National Emergency Management Association.

Miss Gordon, I understand you have an airplane to catch, too, so if the other gentlemen will indulge us, we will hear first from the Governor and then go directly to Miss Gordon so that she can meet her schedule.

Governor Leavitt, again we're honored and delighted to have you here. If you have the wherewithal to argue with the Gartner Group, we'll be glad to hear that, too.

STATEMENT OF HON. MICHAEL O. LEAVITT, GOVERNOR OF THE STATE OF UTAH

Governor LEAVITT. Thank you, Senator.

I think, while there may be some variety in the numbers, I think the conclusion of the chart and the report of the Gartner Group is consistent with the testimony that I will present to you today.

Among the States there is substantial progress, but progress has varied. For some it is significant, advanced to the point where testing is already underway, including testing of law enforcement and emergency management systems; other States are just getting started.

There is also a variety of degrees of collaboration between State and local jurisdictions. Most States, I think, are entirely conscious of this dilemma, and they understand the need to work cooperatively with local jurisdictions. They are working very feverishly now, and I think the pace is increasing as we get closer to continue that function.

The National Governors Association, like many other organizations of its type, are doing what they can to help their members. We had a summit in July of this year, the "Year 2000 State Summit", attended by senior-level policy people from nearly every State. We have also provided a lot of written material and papers that are available.

We welcome, as an association, I might add, the passage of the "Good Samaritan" legislation that was authored and sponsored by members of this committee, as being an important step forward in our preparation.

It may be valuable for me to take a moment or two and talk about some of the things that are happening in Utah, simply because those are the ones that I know the best. And while in my judgment there is no State that stands head and shoulders above as a sterling example of its preparation, I think we are doing things that other States may share in and we're looking very anxiously to learn from them.

Utah is moving forward. In essence, we have concluded that we can cover the problems that we know about. As in every other case, it's the problems we don't know about that worry us.

In the realm of the known, while we are not yet compliant, it is measurable for us. We are measuring it on a month-to-month basis. Among those areas that we have identified as known problems, or known systems of potential problems, we deem ourselves at this point to be 51 percent compliant among those systems. We are cur-

rently testing 600 different information technology systems within our State.

One of the most important things that we have done—and it happened really in a way that was not intended simply to deal with the Year 2000 programs—we have developed an alternative site where we have literally duplicated all of our systems for the purpose of emergency management. We have developed that "alternative site" in a little town called Richfield, which is 130 miles south of Salt Lake City, as a testing center.

All of our major systems now are being taken to that testing center and we are rolling it forward to the Year 2000, to two/zero/zero/zero, and testing the system to see what occurs. We are finding that there are problems, some that would be anticipated and many that would not be. This has been a very helpful facility, one that as we finish our testing we're anxious and willing to make available to local government jurisdictions as well.

Half of the State's database and mainframe resources, as I mentioned, we have found to be compliant, and we're working on the others. We are going through a prioritization system, obviously to make certain that the systems we work on first are the most important. Those pertaining to public health and safety and so forth are being prioritized.

Obviously, the unknown component of Y2K is what we're the most worried about. We are developing contingency plans, what the State will do if information technology systems are not remedied in time, and then how we will deal with the systems during a breakdown in the infrastructure, if that were to occur.

Now, we have directed all of the State agencies to provide contingency plans. We have set a deadline of December 31, 1998. Again, I think this is consistent with what many other States are doing. My colleagues on the panel will be able to validate or tell about their suggestions.

One rule we have found is that, the more we look, the more we find, and the more we find, the more it costs. We have identified costs on Y2K in our relatively small State in excess of $50 million already.

Gratefully, we began some years ago working on the re-development of some of our major systems. As we have done that, we have made them Y2K compliant. We have not included the entire cost of that resystemization in that $50 million, so we and other States are developing a substantial amount of resources to go into this.

We are working very closely with every State agency dealing with Comprehensive Emergency Management. We are working closely with FEMA and others to make certain that we are there. I might just say—and my time is rapidly coming to a close—that perhaps one of the most important things we're doing is coordinating in our State the work of local governments, not just in terms of their own Y2K compliance, but their interaction with us and Federal agencies.

We have also called together all of the financial institutions in our State, all of the utilities in our State, all of the major public systems, and asked them to demonstrate to us their compliance—all on a voluntary basis. I must say that, for the most part, they have been very willing to do that. This is a problem that is so

broad in its scope that no government agency is able to solve it. We all have to do our share. I think it's safe to say, Mr. Chairman, that the States are doing that, to varying degrees, and hopefully they will be compliant by the Year 2000.

Thank you.

[The prepared statement of Governor Leavitt can be found in the appendix.]

Chairman BENNETT. Thank you very much, Governor. We appreciate that. We will be back to you with questions.

Miss Gordon.

STATEMENT OF ELLEN GORDON, PRESIDENT, NATIONAL EMERGENCY MANAGEMENT ASSOCIATION

Ms. GORDON. Thank you. Good morning, Mr. Chairman, and members of the committee.

My name is Ellen Gordon and I represent and appear before you today on behalf of the National Emergency Management Association, and Governor Branstad, as his emergency management director.

On behalf of the association, I thank you for this opportunity to provide input and to appear before you today to discuss this very serious issue as it relates to emergency preparedness, response and recovery. We commend you on the seriousness with which you're taking on this issue, because we understand and realize that there will be consequences that we potentially could be faced with in responding.

I will summarize my remarks in the interest of time.

NEMA represents the State directors, as you mentioned earlier, of all emergency management in the States and territories and we are responsible to our Governors for ensuring that the public's life and safety is taken very seriously and to protect it from disasters and emergencies. State emergency managers are well aware of the Year 2000 issue, particularly the possibility that we may be called upon to respond to those consequences of Y2K technology failure or disruption.

NEMA recently conducted a very quick survey, just asking some very basic questions of our State emergency management agencies on the overall awareness of Y2K issues. It yielded the following information. Again, I stress that it was very basic questions that we asked, in a very quick survey. This is just to get a feel for what's going on out there as it relates to emergency management.

All of our State emergency management directors reported that the Y2K programs for State agencies and the State Y2K programs differ in organization and implementation strategies, as Governor Leavitt just pointed out. Many of these agencies, however, are working with the emergency management agencies within each of the States and are coordinating, marrying each other up with information technology departments and emergency management, so that is occurring, which is good news.

All State emergency managers indicate their emergency operation centers will or are currently compliant for the Y2K technology issue. We find that to be a very serious issue for a State to be able to respond to any disruption, because if our State centers

are not operational, we will not be able to coordinate effectively the State resources.

All States believe that their emergency management systems that are owned and operated by the State will be Y2K compliant. At this time most States cannot assure that the emergency management systems being utilized by local governments will be Y2K compliant. For example, what you were discussing earlier this morning, the 911 centers, and all the critical infrastructure it takes to protect public health and safety.

NEMA believes that the Y2K issues in emergency management systems, especially at local government levels, needs some focused leadership from State government. We are going to be working closely with our local governments throughout our States, as Governor Leavitt stated, to provide some leadership and some coordination, and make sure the information flow is going to local governments.

Since all disasters typically involve local emergency management agencies first, NEMA believes it is important to determine the impact of Y2K on local emergency management systems which could produce deficiencies in providing for the public health and safety. As President of NEMA, I am urging all State emergency management directors to provide information and assistance, as appropriate, to their local emergency management agencies. It is imperative that capabilities be in place and ready to respond to the consequences of a potential Y2K technology disruption.

As we find significant problems in emergency management systems, I intend to immediately advise the Director of FEMA of any major shortfall in local government emergency management systems and seek assistance and solutions to preclude adverse impact on the public. Hopefully, the partnership of NEMA and FEMA can help local governments avoid significant adverse consequences of the Y2K dilemma—not that all the answers lie there, but that's at least one major step that we are working on and working very closely with FEMA.

As I stated, local government has the front line of authority and responsibility for events or emergencies. However, if the emergency overwhelms local resources or capabilities, the State then provides assistance and resources as determined in our State Emergency Operations Plan. The role of State emergency management is to coordinate and provide the State assistance as required during a disaster or emergency, regardless of whether the disaster is a tornado, hurricane, blizzard, civil riot, or a Y2K-related disaster.

These responsibilities are common to every State's emergency operations plan. Most State agencies, not only the emergency management agency, but most State agencies have disaster preparedness plans that include all hazards preparedness, response and recovery procedures. Almost all State and local government emergency management agencies have infrastructures in place to coordinate their agency's role in disaster response and recovery.

As I alluded to earlier, there are emergency operations centers throughout the country. However, the degree of that capability varies. Some States, some local governments, will have a better capability than others.

As such, NEMA anticipates the Y2K problem will be dealt with much the same as any other disaster, through an integrated and coordinated emergency response system. The resources and types of people needed may differ for a Y2K event, but the emergency response system itself will remain the same from the information that we know today.

Regarding interstate cooperation, NEMA administers the national Emergency Management Assistance Compact, EMAC, an interstate mutual aid agreement, a system for us to provide resources rapidly to supplement Federal assistance, when merited, or to replace Federal assistance when it is not. The EMAC agreement establishes our legal mechanism and operational procedures to facilitate the rapid disaster response, using personnel, equipment and materials from 23 States and 1 territory.

The compact has been tested extensively this year during the Florida wildfires and Hurricane Bonnie and has proven to be an efficient and effective system for States to help each other during disasters. As we speak, a number of our EMAC member States are providing assistance to the Gulf States impacted by Hurricane Georges.

Interstate mutual aid may prove extremely beneficial should the infrastructure fail in a Y2K scenario, particularly if only a few areas within a State or region are impacted. However, should all States be impacted in a significant manner, mutual aid between States may not be possible. Individual States would not be able to spare limited personnel or resources outside State boundaries. So these are some things that we're taking into consideration as we're working with FEMA on what we can expect the Federal emergency response plan will be able to deploy if a State needs Federal assistance.

In conclusion, NEMA, with the support of its member States and territories, and in partnership with FEMA, is working to determine that Statewide emergency management systems are Y2K compliant and, if not, what needs to be done to be responsive to disruption or failure. Many State emergency management agencies already have plans to activate their emergency operations centers on December 31st, and watching the reference to the 17-hour issue that you talked about earlier. Many of us will activate our EOC's on whatever the appropriate time is back from an event when we start being able to get information based on the alert information.

These Y2K preparedness activities are a part of our mission to coordinate and facilitate resources to minimize the impact of disasters and emergencies on people, property, the economy and the environment.

The most immediate need is for States to work with their local governments to identify potential system failures and make sure the contingency plans are there to manage the consequences of those failures. In addition, the States need more information and guidance from the Federal Government as to what assistance will be made available to State and local governments in a Y2K emergency, particularly if it becomes multi-state.

Thank you again for inviting NEMA to provide this testimony. I will be happy to answer questions. I don't have to leave for about a half an hour.

[The prepared statement of Ms. Gordon can be found in the appendix.]

Chairman BENNETT. Thank you very much.

General Philbin.

STATEMENT OF MAJ. GEN. EDWARD J. PHILBIN, USAF [RET], EXECUTIVE DIRECTOR, NATIONAL GUARD ASSOCIATION OF THE UNITED STATES

General PHILBIN. Thank you, Mr. Chairman, Senators. I am Ed Philbin, the executive director of the National Guard Association of the United States, based here in Washington. I am here today to offer opinions on the problems that may arise as a result of noncompliant computers and computer-dependent systems that are unable to transition through midnight, 31 December, 1999, and also to address the role the National Guard could and probably will play in managing emergencies arising from those problems.

My testimony generally reflects the opinions of the association and its members, who are the commissioned and warrant officers of the Army and Air National Guard. It should not be construed as representing the official positions of the Department of Defense or of the National Guard Bureau within the Department of Defense.

It is increasingly evident that an appreciable part of the Nation's infrastructure could be adversely affected in some way by what is commonly referred to as the Y2K problem. In general, the National Guard has the capacity to provide military support to civilian authorities, and can contribute a myriad of human and equipment resources to restore essential operations disrupted by Y2K generated incidents.

Considering the possibilities of a large-scale disruption of governmental, commercial and other routine daily activities, it is certain that the National Guard will be among the first organizations activated to assist in the revitalization of the Nation's computer dependent infrastructure. As with hurricanes, floods and other incidents requiring quick reaction by a well-trained and well-equipped on-site team, no other organization will be able to respond in support of police, fire fighting, and other civilian emergency responders to major crisis situations that may be caused by Y2K disruptions as well as the National Guard. The National Guard's practiced interaction with State and local organizations, and its connections to the National Command Authority, provide a unique emergency response capability not found in any other Federal or State organization.

The immediate need, as Senator Dodd pointed out, is to determine what responsibilities the Guard will be expected to assume in the management of the Y2K related problems, that many analysts have forecast, will have the potential to trigger the destabilization of societal functions. The National Guard needs to be prepared to assist in maintaining or reestablishing essential stability in the civil sector.

I suggest that the Department of Defense must develop a clear concept of how the National Guard will be required to respond to the spectrum of problems that could be created by a Y2K disruption. The DOD, through the Chief of the National Guard Bureau—

who by law is the channel of communication between the Federal Government and the States—must now coordinate with the Adjutants General and the Governors to determine the likely, locality specific scenarios that may arise in a Y2K situation.

The DOD should also assist the Governors and State emergency response coordinators to ensure that the National Guard itself will not be impaired by the effects of a Y2K incident at a time when it will be most needed.

I suspect that, to date, this has not been a priority effort on the part of the DOD, even though to properly prepare for possible Y2K disruptions, the Office of the Secretary of Defense must be cognizant of the necessity of ensuring that the National Guard is fully capable of responding to any such technical breakdown.

We must be certain that the National Guard will not itself be a victim of any Y2K disruption. All National Guard units in 3,200 locations throughout the Nation must possess computer dependent equipment that is Y2K compliant. Responding to the consequences of these disruptions will be futile if the National Guard's operations are plagued by the very consequences the Guard is attempting to manage.

It is critical that the Y2K response requirements of the National Guard be fully funded to ensure that it is able to respond quickly and effectively to the needs of the community. I respectfully request, Mr. Chairman, that this committee urge the Senate to provide full funding for Y2K compliance upgrading of National Guard equipment as one of the highest priorities for such funding, since the Guard will be among the first responders to a Y2K incident, together with police, fire fighting and other civilian emergency response personnel.

The critical first step in ensuring that the National Guard will be fully prepared for a possible Y2K calamity is the collection and sharing of information. When I was Commander of the New Jersey Air National Guard, the State Adjutant General for the first time requested all of his commanders to conduct a survey to identify all of the Army and Air Guard resources that could be made available in response to a State emergency.

My survey of the New Jersey Air National Guard identified what was to me a surprisingly long list of both mundane and sophisticated equipment which could be useful in responding to a State emergency. I strongly recommend that such a survey of the available resources of both the Army and Air National Guard of each State and territory be conducted prior to midnight on 31 December, 1999.

Equally important, we must determine how the National Guard will interact with the Federal Emergency Management Agency and the DOD in response to Y2K induced emergencies. Command and control of multiple agencies must result in mutual support rather than multiple collisions in addressing emergency situations. Therefore, a comprehensive study should be conducted on the potential roles of and the interaction between the FEMA, the DOD, and the National Guard of the various States and territories in response to Y2K induced problems.

I applaud the recent inclusion of the National Guard for the first time in the President's Y2K subcommittee on emergency response,

chaired by FEMA, and I believe that the subcommittee, with the DOD, National Guard Bureau and the Adjutants General, must develop a cohesive strategy that prepares this country for any event of mass effect leading up to and after midnight, 31 December, 1999.

Mr. Chairman, let me stress the need for the Adjutants General to play an important role in the development of this strategy. In most cases, it will be the Adjutants General who will integrate the planning efforts for their respective States with those to be developed by the National Command Authority.

As you are aware, the Quadrennial Defense Review highlighted the role of the National Guard in homeland defense of the United States. While the Guard stands ready to meet the needs of the citizenry during any Y2K incident, it is important that, in preparing for that eventuality, the National Guard's ability to respond to its Total Force mission of rapidly expanding our Army and Air Force in response to a national threat not be denigrated.

Funding for current combat readiness resources should not be the source of enhancing the Guard's ability to respond to a Y2K event. As an example, it is becoming increasingly evident that the current structure of the active duty Army cannot execute the current two Major Theater Wars strategy without the assistance of the Army National Guard combat divisions and brigades. This increased dependency on the National Guard requires increased, not decreased, combat readiness resourcing to enable the Guard to accomplish its historic combat mission. Mere reallocation of current funding to Y2K missions will have a negative effect upon the National Guard's ability to recruit, train and keep our soldiers and airmen combat ready to respond at a moments notice to a national threat.

The Year 2000 challenges present an emergency scenario unlike any other in our Nation's history. Our technological society has grown extremely dependent upon the continuity of computer driven systems and networks and, as a consequence, the Nation's vulnerability has increased appreciably. Any significant disruption of our computer dependent infrastructure could result in a significant societal disruption. However, with the cooperative interaction of Federal and State governments, the military, the private sector, and with serious advance preparation, the impact of such an event on the American people can be significantly reduced, if not totally eliminated.

Mr. Chairman, thank you very much for the opportunity to offer the opinion of the National Guard Association on the readiness of the Guard to deal with these potential emergencies. As we have for over 3½ centuries, the National Guard of the United States, both Army and Air, stands ready to protect the Nation against military threats and local disasters.

I would be happy to answer any questions you might have, sir.

[The prepared statement of General Philbin can be found in the appendix.]

Chairman BENNETT. Thank you very much.

Mr. Flynn, you represent the largest State in the country, and perhaps the one we're focusing on the most.

STATEMENT OF JOHN THOMAS FLYNN, PRESIDENT, NATIONAL ASSOCIATION OF STATE INFORMATION RESOURCE EXECUTIVES

Mr. FLYNN. Thank you. My name is John Thomas Flynn, and I speak before you today as President of the National Association of State Information Resource Executives, which represents the chief information officers of the States, and also as Governor Pete Wilson's chief information officer in California.

First of all, I want to express my appreciation for the opportunity to update this committee on Year 2000 readiness, and particularly as it affects emergency preparedness.

I'll get right to the point. As to the States overall remediation efforts, compliance among the 50 States with all aspects of mission critical systems ranged individually from below 10 percent to over 90 percent. I would point out that these figures are based upon NASIRE's self-reporting online survey, a hard copy of which I have provided to this committee.

This report, the latest results of the survey, which in many cases were done just in the last several weeks, just under half, 24 of the States, have completed remediation of at least 50 percent—that's 50 percent of their mission-critical systems. There is no State that I know of that has announced itself to be 100 percent complete, and in addition, due to the various interpretations surrounding this term "completeness", as well as the legal ramifications involved, we may not see total compliance claimed until after January 1 of the Year 2000.

I have also submitted a column that I wrote on this topic of completeness for Government Computer News for the committee.

Chairman BENNETT. That will be included in the record. Mr. Flynn. That's right.

As the remediation process has evolved from addressing software applications and interfaces, desktop systems and embedded technologies, a key focus of activity in the States has involved contingency planning, operational recovery and of particular importance to this hearing today, emergency preparedness.

As to the general condition of the States' emergency preparedness and the readiness of State emergency response agencies, I would offer the following. Disaster relief services are facets of a civilized society that citizens should be able to depend on. Obviously, we could imagine the residents of New Orleans or the Florida Keys managing without State emergency and disaster assistance as a result of the hurricane. Also, you may recall that earlier this year there was a total blackout, a power blackout, that occurred for weeks in the central business district of Auckland, New Zealand. Or you might recall the Galaxy 4 satellite that put 50 million pagers out of commission, with one satellite and 50 million customers affected. When you think about how many lives are touched by one action or, in this case, inaction, you understand the magnitude of the Year 2000 situation.

Regarding specific emergency preparedness issues, 11 States responded to a NASIRE survey, which I have also listed in my written report to this committee.

The NASIRE Chief Information Officers reported that close working relationships have been established with their emergency

management organizations, and their mission critical system remediation for those particular emergency agencies has been given the highest priority in the States.

I could give a few specifics. Governor Leavitt already mentioned some of the fine work that's going on in the State of Utah under his Chief Information Officer, David Moon. The State of Arizona, with John Kelly the CIO there, has biweekly meetings with their Y2K coordinators from the Public Utility Commission, the Attorney General's office, the Office of the Courts, and the Department of Emergency and Military Affairs. Staff representatives from both Senators McCain and Kyl were recently invited to these meetings.

The Colorado 2000 Council has asked the Colorado Office of Emergency Management and the Federal Emergency Management Association to participate in Colorado's Council. This council is a coalition of public and private industries representing critical service sectors such as telecommunications, public safety, and water, just to name a few.

I would also point out that New York's Governor Pataki, his Office of Technology and State Emergency Response Offices are working closely on a statewide Y2K emergency response plan, which they expect to have in place during the first quarter of 1999.

In California, the Governor's Office of Emergency Services, OES, is a stand-alone cabinet level agency, like the Department of Information Technology, which reports directly to the Governor.

Having this kind of authority naturally leads to quicker and more comprehensive responses. As you know, California, during this decade, has suffered through flood, fire, drought, riots, and other natural disasters with responses coordinated by this department.

As CIO for California, my office is partnering with California OES Director, Dr. Richard Andrews, along with our California Year 2000 Intergovernmental Task Force, which is comprised of State, county, and city CIO's, for a Western States Y2K Summit on Emergency Preparedness and contingency planning scheduled for this fall. Dr. Andrews and I have been in contact with the emergency directors, State CIO's and Y2K managers of these States who have all voiced unanimous enthusiasm for this endeavor. We believe that the model and subsequent action plan we develop for this summit will be of value to States, not only in our region but beyond.

In summary, the emergency management services, while they do not fall directly under the responsibility of our IT organizations, those who work in the IT environment are working very closely with their sister agencies who are directly tied to providing support and order during a disaster.

I thank you for the opportunity and look forward to your questions.

[The prepared statement of Mr. Flynn can be found in the appendix.]

Chairman BENNETT. Thank you very much. I appreciate the testimony of all of you.

Governor Leavitt, we are very interested in the Year 2000 State summit that you referred to in your testimony. Could you tell us a little bit more about that, and then prospectively, during your term as the head of the National Governors Association, is there

anything specific that you can see that the Federal Government ought to be doing to help the States, that we either are not doing or not doing well enough?

Governor LEAVITT. You can get your own systems compliant. I think the States recognize the need for us to do ours, that local governments ought to do theirs. But the national government systems we're all dependent upon in various ways. I would say the national government's highest priority ought to be getting its own house in order.

I don't say that in an accusatory way——

Chairman BENNETT. Oh, no.

Governor LEAVITT. I say it simply as a matter of fact.

With respect to the summit that was held, it was really a method of being able to share among senior policy staff the perspectives of other States. What's being done by the chief information officers I think is a corollary to that.

It has been my experience that there is no dearth of information about this. There is just simply a dearth of action. Everyone has to do their part in order to this not to have broad, social consequences.

Chairman BENNETT. Do you agree that the National Guard might well play a key role in terms of challenges with respect to civil disorder? I can imagine a metropolitan area where the welfare checks don't go out, turning into a really ugly situation rather quickly if the local computers that handle the welfare checks don't get remediated.

Governor LEAVITT. As I mentioned in my testimony, Senator, there are two levels of planning that we're going through. One is to find those systems where we know there's a problem and to deal with it. I think most States are going through that process. The piece that we don't now understand is what the implication could be for a system where we can't contemplate the impact.

Every State, I believe, is using whatever their emergency management method is. In our State, the National Guard has a different role than it would in another State. In some States, the National Guard actually handles the comprehensive emergency management function. In other States, it is basically an adjunct and participates. So clearly the National Guard will play some role in every State. The issue is the degree to which they will play a role will depend entirely on what role they play in their individual State.

Chairman BENNETT. Do you expect to have another summit?

Governor LEAVITT. We expect to have an ongoing discussion with—we are creating a network now with people who have responsibility and are in charge, as Mr. Flynn has suggested. One of the things that I believe has been most helpful in our State is the creation of a very sophisticated web site that is available not just to local governments and State agencies, but also the private sector. The creation of user groups within the State, our Economic Development Office, has begun to develop user groups among small business to give them access to information.

But the very technology that at this point imperils us also provides us the tools of disseminating the information for compliance. We are working mostly to create information availability.

We have had a summit with our—we have the benefit of having one of the great sponsors of this dilemma in our State. Senator Bennett, you have been a voice, a voice that started off as a voice in the wilderness, and you have come to the point where you are well known for your early warning. But we have had the benefit of that for some time.

So we're having meetings with our utilities, meetings with our banks, meetings with our police and public safety people, and we're in the process of completely redoing our system for communication.

Another challenge right now, which has also turned out to be an opportunity in our State, is the 2002 Winter Olympic Games. It is causing us all to work together. So I think every State has their own approach to it, and we will continue at the national level at the National Governors Association to provide information between States.

Chairman BENNETT. We passed the legislation that we were congratulating ourselves about all morning today, which will allow businesses to share information in ways that their legal departments may have counseled them not to do prior to the legislation.

Do you see any impediments to the sharing of information between States, or between the State and local government, that we might address on the Federal level, or are you in an atmosphere where the antitrust laws or the trial lawyers suing you for liability is not as big a problem as it is for some businesses?

Governor LEAVITT. They are a significant worry to us, because of the broad public responsibility we carry. For that reason, we joined in your applause for the "Good Samaritan" legislation that was passed.

There may be additional legislation that I am not able to articulate at this moment, but we will not hesitate, given the scope of that problem, to come back to you to ask, if that's the case. Perhaps the State CIO's would be able to respond to that better than I.

Chairman BENNETT.

Vice Chairman Dodd.

Vice Chairman DODD. Thank you, Mr. Chairman. Welcome to all of you. Governor, it's nice to have you with us.

Governor LEAVITT. Thank you, Senator.

Vice Chairman DODD. I appreciate the fine job you're doing.

I was just thinking, I suspect you've got to do a fine job with Bob Bennett watching over your shoulder here, watching what's going on.

Governor LEAVITT. We have no excuse.

Vice Chairman DODD. You're doing well.

I would point out that the national excitement over the 2000 Winter Olympics coming to Utah is obviously of great interest in your home State, but also the Nation. So I suppose that's an added incentive to get this all working.

You've maybe heard that Senator Bennett and I have been constantly pushing, with 70 witnesses—and I don't know how many hearings we've had with our Federal agencies, including this morning. I don't know if you were in the room at the time, but even with Mr. Koskinen and others—to try to get these assessments in earlier and push them on the date to complete it, so we can start dealing with agencies like FEMA, which is of critical importance, and the

National Guard. You have to have an assessment to determine what can be done in order for you to start making the determinations of what you are going to need and, of course, it trickles down here to local government.

So that chart prepared by the Gartner Group—and I appreciate the Chairman making note of the fact that it's a fine Connecticut company, the Gartner Group, and has been a great asset to all of us in this as they have done surveys here. But that is a pretty low performance rate by our States. I don't know where my own State fits into this scheme. We have had some hearings up there, and I know John Rowland has been interested in it. We ought to raise the profile of this a bit.

I don't know if they have a State-by-State assessment done, but maybe we will be reaching a point where we want to do a State-by-State assessment and let that be known. It would be an added incentive for people to kind of get "back on the horse".

Governor LEAVITT. Senator, I might defer some to Mr. Flynn, who indicated that the CIO's in the country are doing ongoing assessments. I have required my own CIO to report to me monthly. In all of the areas where we have identified potential problems, we have quantified our progress. In our State we are 51 percent, as of this month, but that started in the low teens and each month continues to increase. We believe we will be compliant in all major systems by the Year 2000.

But we are only one State. As the Gartner report indicates, there is a wide variety of progress. But it's important, I believe, to acknowledge that virtually every State now is moving forward and the trajectory is a good one.

Vice Chairman DODD. I'm glad to hear that. As you point out, others have as well.

There is an interconnectability here on this, with the transportation system beginning the long list of items, where the towns, counties and States and the national government are so interwoven here that the collapse of a system even in a county could have national reverberations. So I think it's important to cite that.

This is not an easy question to ask you, and I don't know if there is one. But if I asked you as a governor, and based on your conversations with your colleagues, what is the single largest concern? If there is a single large concern you have as a governor, in your own State, or what you hear from other governors, is there one particular item that sort of gathers more attention than any other item, or maybe two?

Governor LEAVITT. We have had some discussion about this. I think there is a sense of confidence among governors that, among the problems we know about, we will get them solved. I think it is the unknown problem that haunts us all.

Obviously, there's the cost that goes into this. One of the characteristics of the job of governor is that it takes a very broad spectrum of responsibility. It could be education, it could be law enforcement, all of those things. So I can't say there is one. But if there is one area that haunts us, I think it's maybe the problem we haven't thought of.

I would say a second might be the systems we don't control, which potentially could be a Federal system. It could be the IRS

not being prepared. Many of our tax systems are very interrelated with the Federal tax system. It could be anything. So I think the interrelationships is probably what worries me, and I think that would be consistent with my colleagues.

Vice Chairman DODD. I appreciate that.

Let me ask this of Miss Gordon. The prepositioning issue I raised very quickly with FEMA, about the prepositioning of personnel and equipment in areas around the country in anticipation of some more widespread problem we would like to think about. Is that a reasonable request, in your view, Miss Gordon?

Ms. GORDON. I cannot speak for all 50 States at this point because we do not have any solid information as to who is going to be doing what, but I can pretty much expect that the States will preposition equipment, perhaps personnel and equipment, in strategic locations throughout the State for response time, to cut down on response time. Of course, in January, in the winter, your travel time is prohibitive in some States. Iowa, for example, will be looking at that very thing.

Vice Chairman DODD. Mike, do you want to comment?

Governor LEAVITT. We intend to use the 19-hour advantage that was spoken of earlier with great care.

Vice Chairman DODD. You notice how he already started that clock, so I lose two on this.

Governor LEAVITT. We will be, in fact, as a part of our contingency planning, be prepositioning equipment. But 19 hours is a lot of time to see a problem starting to develop and be able to dispatch equipment, so we will be using that to the fullest extent possible.

Vice Chairman DODD. You may have heard me mention with the FEMA people that the northeast utilities in my State have really stepped up to the plate on the Puerto Rican problem, the disaster with Hurricane Georges. They have gone down there to help out.

One of the problems they had, they were told the only way to get it down there was by barge, by boat, which takes five days. One of the problems was, it's not that they wouldn't fly it; it's just they had a higher priority level of materials they wanted to get in by aircraft—I gather that was the case—because they said they didn't have the aircraft to get it down there. That is obviously the unanticipated disaster.

But if all of a sudden we find our ability to move equipment—and that is one place. Imagine you have multiple, as I presume you would here, there is a failure here that's going to be in multiple places. You're starting to marshal resources, and the capacity to deliver those resources is something we ought to be thinking about. So prepositioning to some extent, where you can, would be wise.

General, we thank you immensely. General Gay is a great friend of mine, the Adjutant General in Connecticut. He does a great job and comes down here with some frequency. Usually he's not bringing me money. He's usually asking for a little money——

General PHILBIN. Usually.

Vice Chairman DODD. I wonder if you have done any assessment—Senator Bennett and I thought we heard, we commented to each other, that we thought we heard a request. This would make you unique, General, coming to Washington with a request. [Laughter.]

Is there any assessment that the Guard has done in terms of potential additional cost factors? I know you have suggested resource allocation, which I think deserves to be repeated. The primary goal of our National Guard, having served in it, is to obviously be prepared to respond to military situations. Every State I know of is very grateful, by the way and, in addition to that, the resources that the Guard has provided, I'm certain in every single State, at one point or another, in recent years, during times of natural disaster or other crises.

Obviously, this cost factor is a major one. We're looking at it from the standpoint of how do you provide resources to Federal agencies, State governments and so forth, to try and become compliant. But I have a feeling here that you've already done some work on this, in terms of what may be requested from our National Guard in potentially dealing with this issue. I wonder if you have, and if so, what are the numbers?

General PHILBIN. To make the National Guard Y2K compliant, I don't think that anybody really knows what the actual number is. I have heard wags of $25 million for the Army Guard and $25 million for the Air Guard. In my viewpoint, that's probably a bare minimum.

I would point out that all of the equipment we would use, and have been using for local emergencies, comes out of the equipment we were given by the Federal Government from the combat structure, both the Army and Air Guard. That's what we use for local operations. There are some cost-sharing formulas that are used for that, but basically, it's combat-related equipment that will be used.

Vice Chairman DODD. Thank you all very much. Governor, it's a pleasure to have you here with us.

Mr. Flynn, if I have any additional questions, I will be certain to send them along.

Mr. FLYNN. Senator, if I could just point out to you, I did submit with my written testimony a survey of the 50 States.

Vice Chairman DODD. Great. We do have it, then, State-by-State.

Mr. FLYNN. And I think it will show a little bit better light than the Gartner Group did.

Vice Chairman DODD. Connecticut is 50 percent. I would announce here that Connecticut is just like Utah. We're getting right along on that. John Rowland will be happy to know I made reference to that.

Thanks very much. I appreciate that. Let's put that in the record.

Chairman BENNETT. It is in the record.

I should comment that, for the Gartner Group, they could not provide State-by-State data because they have State-level clients and have contractual agreements, which makes that difficult.

Thank you all.

We will now have the third panel. We have Bruce Romer, who is the chief administrative officer of Montgomery County—maybe he knows whether the Metro is going to work or not; Bob Cass, the city manager of Lubbock, TX, and we've heard a great deal about Lubbock so far; and John Powell, with the Association of Public Safety Communications Officers.

Gentlemen, we appreciate your patience. We hope it has been enlightening for you to sit through this morning's activities. We look forward to having you enlighten us in your areas of responsibility.

We will go in the order in which I introduced them. Mr. Romer, you can go first.

STATEMENT OF BRUCE ROMER, CHIEF ADMINISTRATIVE OFFICER, MONTGOMERY COUNTY, MD, ON BEHALF OF THE NATIONAL ASSOCIATION OF COUNTIES

Mr. ROMER. Thank you, and good morning, Chairman Bennett, and members of the committee.

I am Bruce Romer, chief administrative officer for Montgomery County, MD, and also representing the National Association of Counties.

I guess if there's one message that I would deliver today, at least from my fellow local government officials, it is that the Y2K issue is not a technology problem. In fact, it is a business management problem. It really should be addressed at the highest levels of any organization. It's a problem of large proportions competing for very precious resources. In our case, it may impact the delivery of local government service and public safety, health, human services and traffic management, just to name a few.

Now, while the Federal challenge for the Year 2000 is sizable, the local governments' Y2K challenge is even greater. Local governments, some 87,000 nationally, have more interdependent information technology systems than the Federal Government. We employ more individuals and we spend more for IT than the Federal Government by far.

Local governments are the direct providers of services that enable the rest of our government and business economy to function. IT systems at Federal installations in Washington, Denver or Chicago may be functioning perfectly—at least we hope they will—but if the Federal employees who run those systems can't get to work safely, or have no basic services when they get there, all of us will have failed in our responsibilities. We think that a Federal and local government partnership is required.

Montgomery County, MD has a population of approximately 840,000. We have an annual operating budget of over $2 billion. We maintain a AAA bond rating from all three credit rating agencies, who have indicated that our Y2K program is, in their opinion, a model for other jurisdictions.

In 1996, Montgomery County formulated a plan to resolve its Y2K problem by December 31, 1998, thereby reserving the entire 1999 calendar year for testing and contingency planning. Our program is very broad in its scope because it involves the coordination of all seven independent county agencies, including our public schools, the community college, and the water utility, all of which are managed through our Year 2000 project office.

Our compliance program has four phases: system compliance, business continuity, contingency planning, and community awareness. We think that our progress has been substantial, but obviously more work remains. We have identified 204 systems that are in need of attention, of which 36 are today certified as complete.

That would put us at about Level III, gaining pretty well on Level IV.

The county has appropriated to date $35 million. We have allocated significant staff resources. We have also passed special legislation to employ fast-track procurement and budgeting processes to help us. Some of our original estimates were in excess of $40 million, and we were roundly criticized as overstating the problem, and today we have appropriated and are spending $35 million.

The Y2K projects, I monitor them biweekly through the use of a high-level management team. A management tracking scorecard was developed to ensure accountability and to properly address impediments.

Our community outreach program was initiated when we hosted all of the county's municipal governments for an information session, and a meeting with our chambers of commerce is scheduled next.

We have also begun to apply our very strong regional role in emergency preparedness to the Y2K problem. We plan to conduct an emergency management training exercise in December of this year to test the entire community's readiness, Montgomery County's community readiness, for the next year. We plan to identify the resources, including personnel and equipment, that may be necessary as the calendar turns.

And then, under the auspices of our Metropolitan Washington Council of Governments, we are now committed to test our region's readiness, probably in the first quarter of 1999. We hope that the scenario planning that we do in the Washington Metropolitan Area will be useful to local governments around the country.

Finally, we have recommended some seven initiatives to Congress in our more complete testimony that we hope you will consider. Some highlights include: establishment of a FEMA-like national emergency fund that might assist local governments to provide perhaps seed funding for cities and counties to apply the best practices that have been developed here as a part of our emergency management exercise. NACo, through Public Technologies, Incorporated, could serve as the vehicle for rolling this information out.

Also, of course, as has been talked about, is the passage of the immunizing legislation that we have all celebrated here rightfully this morning, and perhaps the establishment of a national program office to complement the President's Advisory Council and, of course, continued congressional leadership to highlight the issues before us.

In summary, the nationwide extent of Y2K failure is still unknown, but certain things we know for sure. The deadline is immovable and that there is no apparent "silver bullet" solution. Many of our Nation's local governments have not started in their testing and remediation. For many local governments, local resources, both human and financial, are what's keeping us from getting further along. Hopefully, Federal assistance for this unique challenge can be applied.

Thank you very much for having us.

[The prepared statement of Mr. Romer can be found in the appendix.]

Chairman BENNETT. Thank you, sir. I appreciate the testimony and the suggestions of specific Federal steps that we can take.

Another vote has been called, so I am required to put the committee in recess. I will do my best to sprint over and sprint back. I apologize to our other two witnesses.

The committee will stand in recess.

[Recess.]

Chairman BENNETT. The committee will come to order.

I think that's the last interruption we will have, but one never knows around here. Again, my apologies to our witnesses.

Mr. Cass, we will now hear from you. You have been very patient and we are grateful.

STATEMENT OF BOB CASS, CITY MANAGER, LUBBOCK, TX

Mr. CASS. Thank you, Mr. Chairman. I am very glad to be here.

We have gone through a number of the processes that have already been described to you, so I will not reiterate those types of analyses we've already undergone. I believe the primary reason the Senate staff asked us to be present was the fact that we ran a simulation Wednesday night that anticipated various Y2K failures on December 31st, 1999, so if it pleases the committee, I will simply give you some of the results of that, some of the lessons that we learned.

I would also point out we're going through detailed debriefings today back in Lubbock and we'll certainly be able to provide you with more detailed debriefing documents later, if you so desire.

One of the first lessons that became readily apparent was that it's going to be extremely critical for us to pay close attention not only to our own processes and systems, but also to those business partners on whom we're hugely dependent.

We had small consolation in our simulation exercise when we found out that although our electric utility system, Lubbock Power & Light, which we control, was ready, the simulation assumed that the natural gas suppliers which fuel our boilers would fail. We had anticipated that problem and, in fact, have already begun meetings at not only the policymaking level but at the operating level with the key partners that will impact us, the area power suppliers on whom we are somewhat dependent, the natural gas suppliers on whom we are somewhat dependent.

I would certainly urge any other community to begin those discussions now. Again, it's important that it take place not only at the policymaking level, the senior management level, but probably more important, at the operational level. It is one thing for the city manager to know you're compliant; it is more important, I believe, on the night of December 31st, for the guy that's flipping the switches to know what his counterpart is thinking and what he's doing.

I would say we are also very concerned and very interested not only in what is going on at the FEMA level—and we certainly want to salute that agency; they've been tremendously helpful to us—but also other Federal agencies, such as the National Weather Service, the air traffic control system, those types of things which are going to heavily impact our operations.

Another lesson that we learned was that it is important that we not overlook and immediately discard the low-tech solution. We believe that most of our systems are already compliant and will be compliant. We are not going to assume that they will. I would offer as an example our traffic control system. I had been assured by our traffic control engineers that it will be compliant. I had been equally assured that, if it is not, there is not a single embedded chip in any stop sign in Lubbock, Texas, and that they will have the ability to spread additional signs to control our major signalized intersections.

We learned that in our Lubbock Power & Light, a highly sophisticated system which controls our boilers, which are natural gas fired, we do have on hand very inefficient, very low tech diesel generators which we do not use except in peaking capacity times. We also have a million gallons of storage capacity left in our diesel tanks. We intend to have those filled to the brim and will be, in the case of an emergency, able to utilize our old diesel generators to keep the basics of government going and the basics of our citizens' lives going, in the event we have problems either in the natural gas suppliers or our more high-tech equipment that is fueled by natural gas.

Our simulation pointed out what many of you already know, that the key systems which will impact us are going to be our emergency communications systems, not only those which enable us to communicate with the firefighter and the police officer in the street—and let me tell you, they are very concerned about our ability to do so—but also our ability to communicate with our water control system. It is small consolation to communicate with the firefighter if we can't get water to him.

We think that it's important—The fourth lesson we learned is that it's extremely important to take advantage of the one advantage this particular incident will offer us, and that is the ability to know when it will occur. I have been in this business for 22 years and I have handled numerous emergencies. Rarely have they had the courtesy to announce they're coming. In this situation, we were able to preplan and to deploy men and material in appropriate situations, as Senator Dodd so aptly pointed out, and that was extremely beneficial to us.

Finally, I would say a lesson we learned is that there is no substitute for an educated citizenry. As we were putting the simulation together, unfortunately some invalid information got out in the local media, and the local radio station broadcast some information indicating that major systems were being shut down, which prompted a series of very concerned calls on the part of a few citizens to city hall. It felt very much like "War of the Worlds," the sequel. We were able to scotch that, to scotch those rumors fairly quickly, but again it did point out to us the probable lack of knowledge in the general citizenry about this particular issue.

We have already made plans to begin a public education campaign that will take place over the course of the next year. I salute the committee for the work it's doing in that regard, too, and I would be happy to answer any questions.

[The prepared statement of Mr. Cass can be found in the appendix.]

Chairman BENNETT. Thank you very much. We appreciate the first-hand information. I think your observations are right on.

Mr. Powell, you get to be the clean up hitter.

STATEMENT OF JOHN S. POWELL, UNIVERSITY OF CALIFORNIA POLICE DEPARTMENT, ON BEHALF OF THE ASSOCIATION OF PUBLIC SAFETY COMMUNICATIONS OFFICERS

Mr. POWELL. Thank you and good morning. I guess it's not still morning yet. Good afternoon.

Chairman BENNETT. It's morning in Chicago. [Laughter.]

Mr. POWELL. And they have 1 further hour of warning.

My name is John Powell. I'm with the University of California Police Department at Berkeley. I'm a past president of the Association of Public Safety Communications Officials International. Your staff also directed some questions to me with regard to the International Association of Chiefs of Police, as I sit on their Communications and Technology Subcommittee.

I would like to thank you for this opportunity to provide information on the state of our Nation's local public safety agencies with respect to the Year 2000 technology problem.

The United States has nearly 19,000 State and local law enforcement agencies. Ninety percent of these have fewer than 24 sworn officers, and about 50 percent have less than 12 sworn officers. There are over 32,000 fire departments. Eighty percent of these are staffed entirely by volunteers. Yet nearly every agency has at least one system that needs to be checked.

Senator Dodd earlier mentioned the NCIC system. Virtually every law enforcement agency in this country has a terminal to access their State and Federal criminal justice information system. Senator, these police and fire departments are where Americans turn first for help.

We have heard horrific predictions being made by millennium fundamentalists. At the opposite end of the spectrum, it appears that the majority of Americans, if they are aware of the Y2K issue at all, consider it to be only a computer problem.

The state of local public safety agencies appears to spread across this entire range, with thousands of smaller agencies not yet aware of the potentially major problems they could face in less than 15 months.

Two wake-up calls this year highlight our dependence on telecommunications services. In April, AT&T's frame relay network failed. Twenty-four hour outage caused by a software glitch in a single card dropped service to major ATM and credit card systems across the country. Then, as mentioned earlier, on May 19 the Galaxy IV satellite failed, disrupting service to 50 million pagers, including critical alerting systems used by Federal, State, and local governments.

Let me highlight the major points in my written response to the questions you posed.

First you asked about the APCO and IACP role in assessing the vulnerability of emergency service agencies to your 2000 problems and our efforts to increase awareness. Such associations generally do not have specific roles in assessing vulnerability. Yet we often serve as a statistical resource to those responsible for such assess-

ments. Associations do play a major role in promoting awareness and providing education, and they are the keys, I believe, to dealing with Y2K.

APCO and the IACP annually host the world's largest public safety conferences in their respective fields. In August, APCO conducted a number of Y2K seminars in Albuquerque. IACP holds its annual conference in Salt Lake City later this month, and Y2K will be a topic in several venues. John Clark, Deputy Chief for Public Safety at the Federal Communications Commission, specifically will address the forum on issues regarding Y2K.

Second, you asked me to address ways that Y2K might impact local law enforcement. Agencies will be impacted in four ways, two internal and two external. First, internal systems must be made compliant. State and local radio communication systems, these [indicating] appear to be in excellent shape. Unfortunately, our computer-aided dispatch and records management systems don't fare so well. Many of these are Legacy systems that will be cheaper to replace than to make compliant.

Critical considerations for governments include long procurement lead times, coupled with potential overload on vendors, during the next 15 months.

The other internal problem—and this is one that's going to be hard to deal with—is preparing to meet the special needs of agency employees during the period of impact. All of us that have been involved in disasters know that people simply don't perform at 100 percent if they're worried about their families. Externally, agencies must deal with the potential disruption of services, primarily utilities providing electrical power and telephone services, especially 911. The critical 72 hours of self-reliance that disaster planners promote as the average time before help arrives does not apply if the problem is, indeed, nationwide.

Last, and clearly the most difficult to judge and plan for, is additional workload caused by impact of the Year 2000 problem on the public. If even minimal disruptions occur, the additional workload on law enforcement in particular could be significant.

With respect to a university campus environment, let me simply say that our issues are identical, except that, like military bases, campuses are cities unto themselves—in my case, a city of 50,000. We are responsible for all buildings, all housing, all operations, all services.

Finally, you asked for recommendations. As a Boy Scout, and later serving as the emergency preparedness officer at UC Berkeley during the Loma Prieta earthquake, the drought, the floods, and the Oakland Hills fire, I learned the critical meaning of two words: Be Prepared.

The most important issue facing us is clearly education for the American public in general, and those of us in government specifically. APCO and the National Institute of Justice are discussing a series of Y2K seminars targeted at public safety chief officers and upper level management to specifically address the four impact areas I just mentioned. To promote maximum attendance by small agencies, a number of these must be held quickly and at little or no cost to the attendee. To sponsor such critically needed seminars, the National Institute of Justice will need a budget augmentation.

Last, from these halls to the Oval Office, elected officials must make the Year 2000 problem a top public priority. The American people need to be aware and be involved. We must have ongoing and realistic assessments of the potential for problems across the plethora of impacted services. A public caught off guard by major failure on January 1, 2000 would result in devastating, long-term impact on this great Nation.

Thank you.

[The prepared statement of Mr. Powell can be found in the appendix.]

Chairman BENNETT. Thank you very much.

I should note that Sergeant Powell participated in the arrest of several armed robbers just a few nights ago. That's a low tech solution, but I'm sure you had high tech help. I congratulate you on your courage and hope that we can keep the high tech equipment that you used to track that particular incident working properly.

Now, I understand you have two radios here, one that works and one that doesn't. Can you give us an example of——

Mr. POWELL. This is a cell phone and I'm not going to count on it working. Our telephone industry across the country has embedded processors everywhere, be it land wire, and particular our cellular telephones.

You can talk to any public safety dispatch center around the country. We are getting tremendous numbers of our calls for service now coming via cellular or other wireless devices.

This one—indicating—this is our mainstay of communications between our dispatchers and our field officers, be they fire, law enforcement or medical. I am very confident that these are going to continue to work. Some of the new systems that have very fancy management software may not properly report statistics across the Year 2000 boundary, but it's not going to stop us from being able to dispatch our officers in the field, at least any place that I'm aware of.

Chairman BENNETT. As is often the case in these hearings, the final panel usually ends up with the most practical information. We've had a lot of theory at high levels, but I think the information we have gotten from the three of you has been extremely valuable.

Mr. Cass, do you know of any other city that's planning the kind of test that you have done? Has anybody been in touch with you to say "We would like to do it"?

Mr. CASS. We've had several indications of individuals that want to do one. After doing ours, several communities found out about it and asked to attend ours, and we allowed them to do so. But much to our surprise, we were apparently the first to do a simulation.

Chairman BENNETT. Do any of you know of any other cities that will——

Mr. ROMER. We're planning to do that in December, and we're going to share information with Bob. That would be very useful. We have our planning underway so we could probably benefit from each other.

Chairman BENNETT. We have talked about the legislation that allows businesses to share information. Governor Leavitt said it was useful in his situation as well.

Are any of you aware of any impediments to getting information that might be removed by Federal legislation or Federal action?

Mr. ROMER. We've experienced that very directly, and that's why we applaud what's been done with the legislation. We did our business continuity planning and challenged all of our departments to identify all the relationships up and down the supply chain.

We sent out 3,500 letters to those folks up and down the chain, and to date we have received about 500 responses. But they really run the gamut. Of course, they are pre-legislation. Some of them are simply not filled out at all, and some of them simply say "our attorneys told us not to answer this." And others have very useful information.

So I think, at least from Montgomery County's standpoint, one of the biggest impediments you have taken care of, or are one the way to taking care of, with the legislation that allows that information to be shared without fear of penalty. I think that's very important.

Chairman BENNETT. One of the other things I have discovered as we've held these hearings is that the people who come forward and are the witnesses are almost always the people who have done the best job and are in the best position, so we get a little bit of a distorted, overly optimistic attitude. I think it's inevitable that there will be cities that are not ready. I don't know where they are, and we're doing everything we can to deal with it.

Mr. Powell.

Mr. POWELL. One of the things I found, and my biggest concern with regard to failures, is the loss of our power grid for any length of time. For a period of time, we'll be OK. What I found is——

Chairman BENNETT. Mr. Cass has got a whole bunch of diesel fuel. [Laughter.]

Mr. POWELL. We do, too, but if you can't get power, you're not going to get more delivered.

One of the things I found from our utility in Northern California is that we're getting conflicting information. Their web site will tell us one thing. They'll be interviewed by a newspaper or they'll be quoted someplace else with different information. So I'm hoping that this legislation will allow them to standardize some of the answers that they're giving, so we'll get what the real answer is.

Chairman BENNETT. Let's assume that Y2K was this weekend, not 455 days away but this weekend. Where would you think the main failures would come, in your own system or——

Mr. ROMER. I guess the way I would look at that is there's a threshold question, at least for us in our contingency planning, and that is, is it a "no power, no dial tone" environment, versus the opposite——

Chairman BENNETT. Let's assume that it's not a "no power, no dial tone", that the national infrastructure works. What would be your problem if you didn't have the additional time that you do have, what would happen in your county, in your city?

Mr. ROMER. One of the things that we're concerned about is some systems that we are integrated with or depend upon over which right now we feel we have no control. A good example is the health care system in our county. We have multiple hospitals of various specialties, and we, of course, are part of that emergency care sys-

tem when we have to transport injured people or sick people. We want to deposit them at a competent place and then go on about our business.

We have a concern that we don't have enough information that gives us the comfort that we're going to be able to do our mission and pass it off to the other element of that chain. So that's one area that we're concerned about.

In a have power/have dial tone environment, we're reasonably confident that our emergency management systems are part of that compliance already, or will be. So we're really not that concerned about traffic management and E 911 dispatch and things like that.

What we are concerned about is some of the systems that we are responsible for. Let's take permitting, the whole construction permitting process, or business permitting process. While it may seem like a governmental function, it can have ripple effects throughout a local economy if we aren't prepared to discharge our duties, from the homeowner who wants to just do something on the weekend to the restaurant that was planning to open the day after New Years. So we had that concern about an internal permitting system.

That would be two examples I would give you there.

Mr. CASS. Senator, I would say that, accepting your premise, the two other concerns we would have would again be those areas in which our agency abuts up against other agencies. We simply need to be certain that the linkages will work out.

Second, we're very concerned about—for example, that fire truck you have on your graphic here. If my other systems work, I still lack certain assurances about the embedded chips to make sure that the ladder goes up, to make sure that the wand that my firefighters use that detects poisonous gases when they enter a dangerous scene, that the embedded chip in that is going to work.

We think we've hit the major systems. We think we've checked out the major systems. There are many other minor pieces of equipment that fill the air packs that my firefighters use, on which we are not able to receive the types of assurances we would like to have. We're going to be putting people into life-threatening situations and that's of great concern to us. Mr. Powell. The one system that I'm concerned about, which I think impacts all of us, is our fire alarm reporting systems. In recent years, we've had really complex systems going in, and the very minimum that all of them have is a clock on them. We had one system where the clock was almost for show, except that it was an integral function of the microprocessor that went around and scanned all the points. What happened when it hit 00 on the year, the accumulator overflowed and the micro stopped and it didn't go running around and around every so often to check all the points again. Those interface not necessarily with our system, but they may interface to a third party that then calls in the alarm.

In California, as I'm sure is true in many States, specifically in high-rise buildings, if you don't have a working fire alarm, it's against the law for there to be anyone working in that building.

Chairman BENNETT. Mr. Romer, will the Metro work? [Laughter.]

Mr. ROMER. Senator, I chair the COG/CAO committee for Washington COG. We were at the White House on Tuesday of this week,

kind of giving a "state of the region" report to some members of the President's Advisory Council. We did include a Metro report.

The answer is they have done their triage. They have established a hierarchy of concerns, not surprisingly customer/passenger safety being at the highest level, and they reported that they were confident that they could guarantee that. The other two levels they were still working through, that being customer convenience and the internal support mechanism of the system.

Of some concern to us locally is they reported about a $5 million gap in terms of their ability to meet their requirements. Now, that is of concern because, in Washington, like so many other regions, we as a regional agency support them. Montgomery County is a major contributor, as is the State of Maryland. So we were somewhat concerned to learn of that gap. I don't know what their plan is to meet it.

But to answer your question, they felt that they had the safety and operational end of a triage to the point where they felt they could get there on time.

Chairman BENNETT. So it wouldn't work if Y2K was this weekend, but they think it will work——

Mr. ROMER. At least in that meeting, everybody was counting on the 440 days yet to come.

Chairman BENNETT. What about mailing out welfare checks?

Mr. ROMER. We're concerned about that, from a variation of that. That is partially a State and county function in Maryland.

But similar to that, we're concerned about the fact that we have changed over our assistance recipients to using debit cards as a good, solid management move that made a tremendous amount of sense when we did it. But now we are concerned—and here again is a system that we don't control, but I know, if the debit cards don't work, where the complaints are initially going to be lodged. They'll be lodged at the county building and city halls across the country.

So yes, that is a concern, because we have not received the level of assurance from the people who take those debit cards from the local Giant supermarket through the bank system that supports that, that they're going to be able to deliver that yet.

Chairman BENNETT. You heard Governor Leavitt and the other officials talk about the level of readiness in the State arena. Do you feel you're getting the kind of appropriate support from State governments that you need?

Mr. ROMER. We've had a couple of good meetings with the Maryland Emergency Management Agency. We intend to draw them into our simulation that we're going to do in December. I want to learn from Bob about how they did that in Lubbock, because I think that's going to be our opportunity to so draw them into our process that we will then get the comfort level that we don't have yet. It may be simply a lack of information.

So I don't want to characterize it as being inadequate at this time, but we have developed that strategy to draw them into our process, to place certain demands on the State system and see how it performs for us.

Chairman BENNETT. Mr. Cass, how about Texas?

Mr. CASS. I would agree with that, Senator Bennett. As Mr. Romer has pointed out, I wouldn't want to characterize them as being unprepared. I would say we involved the National Weather Service in our simulation and they performed wonderfully, and I anticipate that other State and Federal agencies will be well-equipped. We simply need to establish the linkages now to be certain that that takes place at the operating level.

Chairman BENNETT. Sergeant Powell, the FBI database and other kinds of electronic connections between local law enforcement and the Feds, do you think that's going to work, or is that an area where we should put attention?

Mr. POWELL. I am confident—In fact, I'm going over to the FBI Headquarters later this afternoon. I'm confident that their systems are going to work. I'm confident that the linkages to the States will work, and that, for the most part, the States will continue to work.

My worry is at the local terminal level, where that small agency with three or four officers may not have the resources to get the corrections made, if they need to be made. Unfortunately, in recent years, we have all upgraded those terminals, and now almost every one of them is at least a personal computer, if not more. A lot of them are in the 5-to 7-year-old area and they're not going to be compliant, unless somebody touches them and fixes them.

Chairman BENNETT. I see a parallel here, and correct me if I'm wrong. The big businesses seem to have the financial muscle and the technological resources to, with brute force, work their way through this problem, so that we're getting information back that says General Motors will function, City Bank will function, and all the rest of it.

And then they say, now, the small community bank may have some trouble. NCUA told us flatly there will be credit unions—and they're talking primarily about smaller ones—that will fail.

The statistics you gave us about how many law enforcement areas have less than 12 officers—I think Montgomery County will probably be all right, and Lubbock, Texas will probably be all right. But a law enforcement activity with half-a-dozen officers is very much like a small business, where they're not paying any attention to it, don't plan to pay any attention to it, and just hope when it comes that everything will be OK.

Is that a fair characterization of what you see out there?

Mr. POWELL. Although I have to note that I drove through my local community bank window earlier this week, and they had a big sign on the front window that said "We're Y2K Compliant".

Chairman BENNETT. Without disclosing any names, I got a note from a bank saying "We are Y2K compliant", and at the same time one of the people working on the problem cornered me and said, "There's no way this bank is going to make it." So we'll just have to wait and see, I suppose.

Mr. POWELL. I found it refreshing just to see that they were aware of the issue.

Chairman BENNETT. Yes.

Mr. ROMER. Senator, one of the strategies that we had proposed in the seven suggestions was to fill that very gap, to provide some funding. We had provided two packages, a local package that would fund the regional readiness test, and a one or one point five billion

dollar fund nationally that could be used to address some of the smaller municipalities needs. I would just refer you to that proposal in our material.

Chairman BENNETT. Well, we thank you for that, and for the specificity of your proposals.

I will say now, in general terms, we have one more hearing scheduled for this committee prior to the adjournment of the Congress. Given today's model, we may be interrupted a great deal by votes because it is scheduled to take place as we get closer to the end of the session, that we're supposed to adjourn sine die on the 9th of October and we're scheduled on the 7th of October. So that does not auger well for our ability to go on uninterrupted.

Assuming my reelection and Vice Chairman Dodd's reelection, we will be back at this same stand in the next Congress. We will be addressing many of these same issues all over again, to try to get an update on how much progress there has been, and we will be talking about some of the specific challenges that you have raised in your testimony, Mr. Romer.

[The prepared statement of Mr. Amyx can be found in the appendix.]

Chairman BENNETT. We thank you and the other members of the panel. This has not disappointed or broken the tradition that says the last panel very often comes up with some of the most interesting material.

The committee will stand adjourned.

[Whereupon, at 12:43 p.m., the committee adjourned.]

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

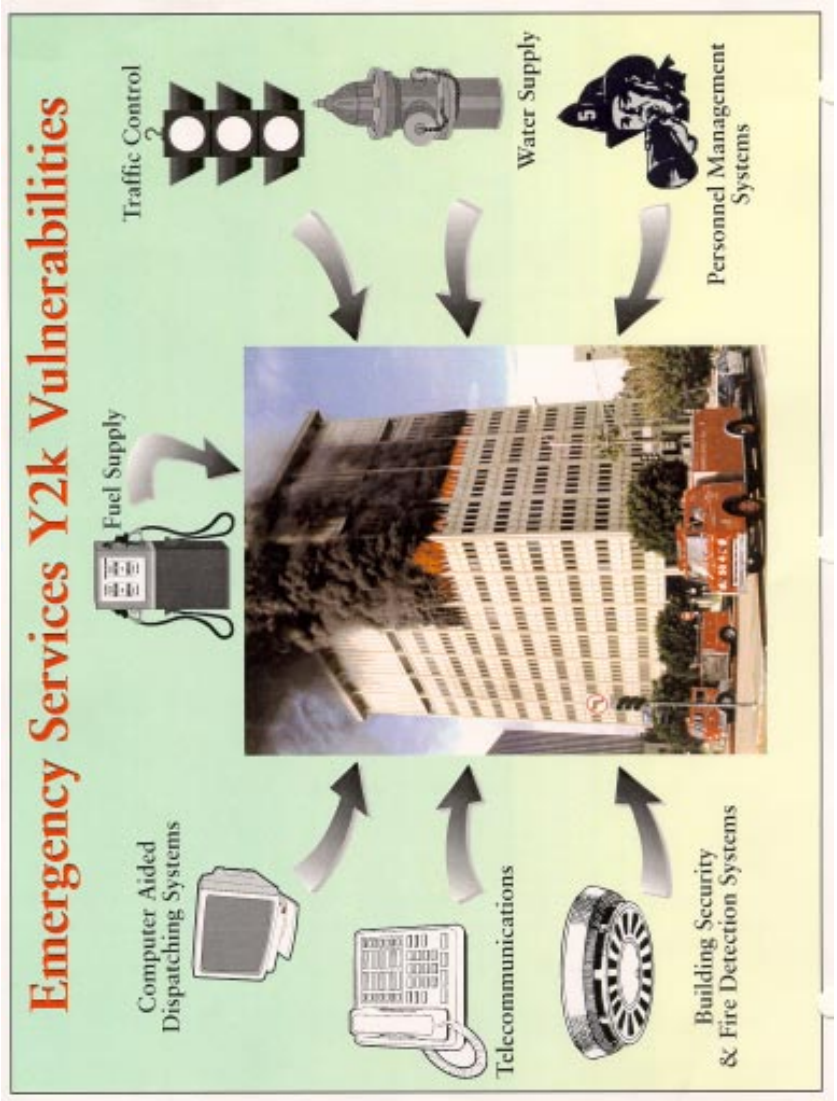
Before we proceed with our hearing today, I would like to make an important announcement. The committee has marked a potentially serious oversight in the national response to the millennium change. Just as we expect the National Weather Service to warn us about hurricanes, the Department of Defense to alert us of sneak attacks, and the Food and Drug Administration to guard against foreign pests and parasites, so should we expect the Federal Government to provide us with the earliest possible warning of Y2K events that may threaten our public safety or national infrastructure.

Therefore, today, with the vice-chairman, Senator Dodd, and Senator Collins, I am announcing the committee's pledge to establish a Y2K First Alert system that will enable citizens of the United States to have up to 17 hours of advance warning of possible Year 2000 disruptions. Citizens living west of the Eastern Standard Time zone will have progressively more advanced notice. Citizens in my home state of Utah will have up to 19 hours of advanced notice, while citizens of Hawaii and some citizens of Alaska could benefit from almost a full day's notice.

The new day begins at a spot in the middle of the Pacific Ocean 17 time zones earlier than Eastern Standard Time in the United States. If the Y2K bug is potent enough to cause immediate problems in information systems and embedded chips, the effect will not occur all at once. Rather, the problems will happen repeatedly in one time zone after another for one full day. For example, Y2K problems that occur at the stroke of midnight, December 31, 1999, in Wellington, New Zealand, won't occur in the U.S. until 17 hours later, when our own clock strikes 12:00 a.m. here on the east coast. Similarly, Y2K disruptions occurring in Tokyo, Japan at "zero hundred hours" on January 1, 2000, occur at that location while it is still only seven o'clock in the morning on December 31, in New York City. This provides us with a full 17 hours of advance notice regarding what we might expect to happen when our own clocks strike midnight later that night.

My colleagues and I feel it is absolutely foolish not to use this advance notice for the good of the nation. Wouldn't it be useful to know that utility and transportation problems are likely to occur, based on information we received as a result of our Y2K First Alert System, before everyone is already out and about celebrating on New Year's Eve? The committee is prepared, if necessary, to introduce legislation in the event that the existing authorities and mechanisms are not sufficient to accomplish the implementation of the Y2K early warning system. We look forward to working in partnership with FEMA within the context of its existing authority to achieve this goal.

One of the themes of our hearing today is preparedness of emergency service agencies at the state, county and local government levels. To illustrate some of concerns in this area, I refer you to this photograph and chart. I will go through a step by step analysis of all the Y2K bugs which would have to be overcome before the fire and police department personnel pictured here would be able to make it to the scene to render emergency assistance.



1. The alarm on the premises would have to operate correctly to warn that a fire had broken out. Have these systems been certified as Y2K compliant?

2. The alarm would either automatically alert the fire department, or someone nearby or in the building would call 9–1–1.

3. The telecommunications system would have to be viable for an emergency call to be placed, and the 9–1–1 system and Public Safety Answering Point or PSAP receiving the call would need to be compliant.

4. The Computer Aided Dispatch or "CAD" System would have to be compliant in order for the call to be dispatched in the most rapid and efficient or as a contingency, a manual dispatch system would need to be in place.

5. The emergency vehicles called to respond need to be fueled. Are the city government fuel pumps compliant? If not, has an alternative agreement been struck between the city and local gas stations?

6. The scheduling tool utilized by the police and fire departments would need to be compliant so that personnel would be present at work to answer the call.

7. The traffic signals along the route would need to be compliant so that the responding units would not be delayed. Has the local transportation department examined these?

8. Once on scene, firefighters would need to have access to a reliable source of water to be used to fight the fire. What is the Y2K status of the local water company?

9. Any medical equipment on scene would need to be compliant in the event it needs to be used to treat potential victims. Has all this equipment been checked for Y2K compliance?

10. Another very basic issue not to be overlooked every step of the way here is, do we have power?

11. In the information technology/data systems area, has the fire department been able to check its data base to see if any hazardous materials are stored at this location?

While this example may appear to overstate the case in its detail, it highlights the broad array of Y2K preparation issues facing city, county and local governments.

I have often said I need to be as Paul Revere in spreading the word about the Year 2000 Problem. Today, I'd like to lead a discussion about those who must assume the role of the Minute Men—those in government at the federal, state, and local levels who must be ready to respond to emergencies on a moment's notice. I am talking about our nation's emergency preparedness and disaster relief agencies, which include FEMA and the Red Cross; our state emergency management offices and the National Guard; and local emergency response departments—the police, fire, and Emergency Medical Services upon which our citizens rely every day of the year.

I must admit that as the senator who has earned the moniker Paul Revere, not Chicken Little, this is a very sensitive topic. The call today is for preparation, not panic. We must recognize however, that with 15 months left to go before January 1, 2000, to fail to plan will be to plan to fail!

Due to continuing concerns about the complete readiness of our core sectors such as electrical power and telecommunications, we are at this point unable to accurately describe how the world will look after we greet the New Year on January 1, 2000. Therefore, we must begin a dialogue on our preparation for potential Y2K disruptions, as well as our efforts to assess the preparation level of the emergency services and emergency planning organizations upon which we depend at every level of government.

We are not yet sure of what the scope or the nature of Y2K disruptions will be due to the lack of firm assessments about the status of certain industry sectors. I suspect that we will have a better idea as time goes on, but it is endemic to the hidden and invasive nature of the Y2K problem that we may not know for certain what the difficulties will be until they are actually upon us. We are challenged to plan in some new ways, and to exercise flexibility as we engage in emergency preparedness.

I want to express my confidence that we will continue to progress in every major sector in terms of Y2K remediation, and that the prospects for wide scale disruptions will be greatly lessened over the next 15 months. However, responsible leaders at every level of government owe it to their citizens to engage in planning for a wide range of possible events. There is a greater likelihood of the occurrence of numerous small and diffused disruptions and minor annoyances which could combine to form a sort of loud din of Y2K "noise" across the country, than there is for large scale disruption. We must begin to develop strategies for dealing with that type of situation as well. We hope that the presence of officials from across the broad spectrum of federal, state, county, and city government will promote discussions about such strategies at our hearing today.

Regarding the overall Y2K preparation level of state governments on the whole, some of the news I have to deliver is not terribly optimistic. Data recently provided to this committee by Gartner Group of Stamford, Connecticut indicates that only 50 percent of the states are evaluated as Level 111 Status under Gartner Group's scale. A Level III rating indicates the state has completed its project plan, has assigned resources, has completed a detailed risk assessment, remediated, and tested 20 percent of mission critical systems, conducted vender reviews, and completed contingency plans. Thirty percent of the states are listed at Level 11, indicating that they at least have developed an inventory of operational dependencies. Ten percent of the states are evaluated as Level 1, indicating that they had begun their projects, had identified a champion, were aware of the problem, and began conducting their inventories. The remaining 10 percent are evaluated as "uncertain" indicating they

were unaware of their Y2K preparedness status. I find that to be very disturbing. We sincerely hope that progress in this area will be accelerated.

However, there is also some good news to be told in this area. Several of the largest intergovernmental councils and professional organizations are actively engaged in Y2K awareness programs. The National League of Cities, the National Association of Counties, and the International City/County Management Association, in conjunction with Public Technology Inc. are sponsoring a Y2K awareness program entitled "Y2K and You." The Metropolitan Washington Council of Governments has published a Year 2000 Best Practices Manual. These programs are good examples of what an effective dialogue among state, county, and local governments can achieve.

Let me express my personal gratitude to Senator Susan Collins, whose strong interest and dedication to this issue have made this hearing possible. I also want to extend the committee's thanks to all of our witnesses, especially to those who traveled long distances on relatively short notice to be here today. And finally, I want to express the committee's enthusiasm to those of you who will be bringing forth some ideas today that truly place you and your organizations on the cutting edge of Y2K emergency preparedness and planning.

BENNETT'S Y2K DISCLOSURE BILL CLEARS LAST LEGISLATIVE HURDLE, ON ITS WAY TO WHITE HOUSE WHERE CLINTON EXPECTED TO SIGN

LANDMARK LEGISLATION WILL ENCOURAGE INDUSTRY DISCLOSURE ON Y2K SOLUTIONS, PROMOTE SHARING OF CRITICAL INFORMATION FOR Y2K READINESS

WASHINGTON, DC.—Clearing the way for presidential signature, the House of Representatives today passed landmark legislation sponsored by Senator Bob Bennett (R–Utah), chairman of the Senate Year 2000 Committee, which will allow U.S. businesses to share essential information for Y2K preparation and solutions.

"Because of the late date in this session, and the complexity of the issue, we were all told there was no chance of passage of this legislation during this Congress," said Bennett.

"The fast track of this legislation's passage shows what can be done when the administration and the Congress work together in good faith.

"The type of disclosure which will result from this bill will move us significantly toward a Y2K solution. Today's action is an important first step, but that's all it is. We will aggressively address other vital Y2K demands when the Congress reconvenes next year. In the meantime, I'm extremely pleased with today's important progress."

The purpose of the "Year 2000 Information and Readiness Disclosure Act," S. 2392, is to help break the silence and encourage full disclosure and exchange of Year 2000 computer problems, solutions, test results, and general readiness. Bennett maintains that the reason for this stony silence, according to the 70 witnesses who have appeared before the Special Committee on the Year 2000, is fear of litigation that can arise from the good faith sharing of information believed to be correct and true at the time shared, but which later turns out to be incorrect. "All of their testimony can be reduced to this: We need quality Y2K information," Bennett said.

S. 2392 provides limited liability protection for a limited time for specific types of Year 2000 information that is considered essential to remediation efforts. What it does not do is provide liability protection for failures that may arise from Year 2000 problems. The bill thus promotes company to company information sharing while not limiting rights of consumers.

S. 2392 highlights

Limited liability protection for statements.—First, note that the bill does not avoid liability for selling products that do not work. What the bill does do is encourage information sharing by protecting allegedly incorrect Year 2000 statements from liability, as well as the persons who make such statements, unless the plaintiff can prove by clear and convincing evidence that the information was false or provided recklessly, or with the intent to deceive.

For persons who merely republish a third party's allegedly incorrect Year 2000 statement, the bill provides for liability in situations where republishers fail to provide adequate notice to persons with whom they share information about either the source of the information or its verifiability. Liability also exists for republishers if the information was provided either falsely or with the intent to deceive.

To further encourage the free flow of information, the bill also provides liability protection for allegedly inaccurate defamatory or disparaging statements unless it

can be shown by clear and convincing evidence that the information provided was done so either falsely or recklessly.

In all the types of claims above, "Year 2000 Readiness Disclosure Statements" are further protected if a claim reaches trial by not permitting these statements to be admitted into evidence as actual proof that the statement was untrue or incorrect. These disclosure statements are not restricted from other uses during litigation, however. For example, these statements would be available for discovery or admissible into evidence as a business record.

Defines specific types of Y2K information

—One broad category of protected statements is called "Year 2000 Statements." Year 2000 Statements may appear in any format including oral or written statements. Year 2000 statements, however, do not include filings with the Securities Exchange Commission or banking regulators, or statements made pursuant to the sale of securities.

—A subset of Year 2000 Statements are called "Year 2000 Readiness Disclosure Statements." Readiness disclosure statements must be clearly labeled as such in written or electronic form and concern one's own products or services.

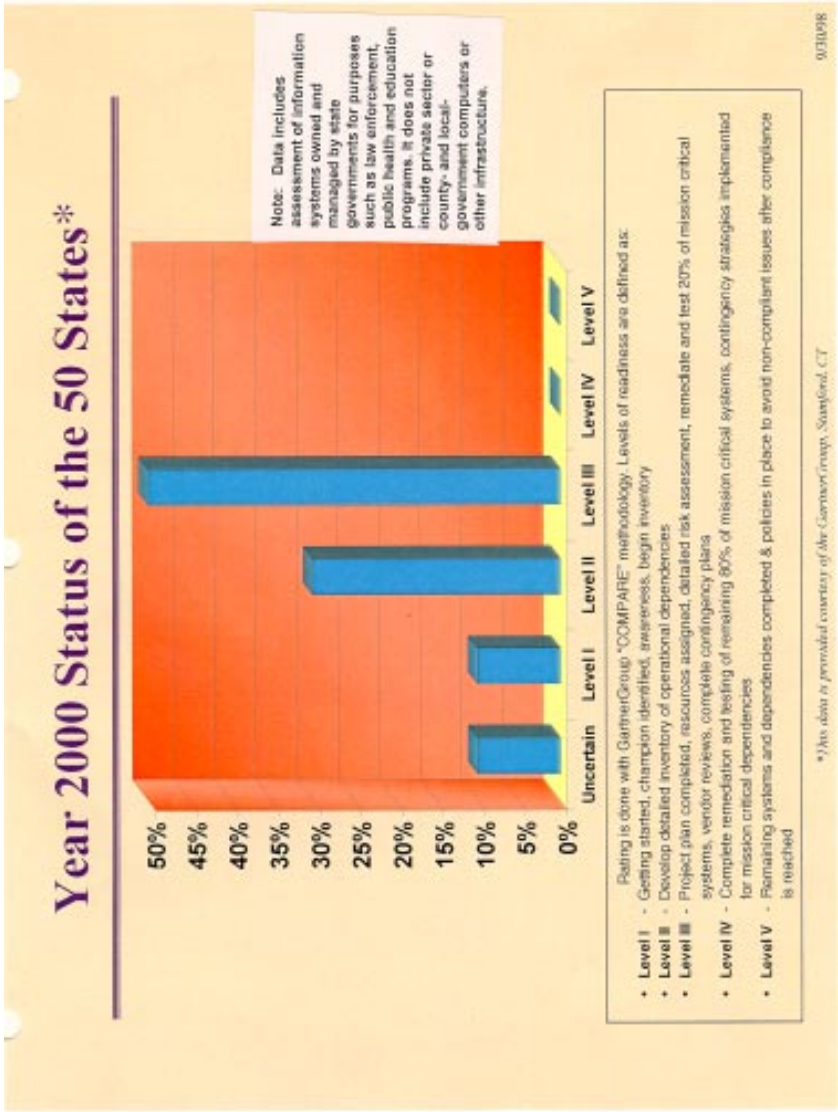
—Defines "Year 2000 Processing" broadly in order to clarify that the "Year 2000 Problem" or "Millennium Bug" is not simply a software problem related strictly to January 1, 2000, but also involves other dates and hardware problems.

Protection for information provided to the government.—In some cases, the federal government may feel it needs confidential information from the private sector to help the government repair its own year 2000 problems or for contingency planning in the case of failures. To help facilitate the flow of information from the private sector to the government, the bill ensures the confidentiality of voluntary industry or economic sector information provided to the federal government from being released to any third party without the approval of the entity giving the information.

Antitrust.—The Justice Department does not feel that the sharing of information under this bill will result in antitrust concerns. However, we have incorporated language they supplied into the bill to confirm that understanding. The bill thus provides that the antitrust laws shall not apply to such information sharing except where a boycott or price fixing results. The antitrust laws will remain in full effect with respect to issues not related to information.

Encourages the use of Internet Websites.—The bill promotes the use of Internet Websites by stating that where the adequacy of notice about year 2000 testing or solutions is at issue, the posting of such information on an Internet website is considered adequate notice, except under certain circumstances.

Establishes a National Information Clearinghouse and Website.—This provision establishes a single government website at the General Services Administration as the hub for basic Y2K information for consumers, small businesses, and local governments. The website is to also serve as a central links to other government websites and information clearinghouses on such efforts.



PREPARED STATEMENT OF BOB CASS

THE CITY OF LUBBOCK'S Y2K DRILL—SIMULATION OF DECEMBER 31, 1999

I. Major systems/areas relative to emergency operations
- A. Electric Utilities
  1. System Control and Data Acquisition system (SCADA)
  2. Inertia Switches/Breakers
  3. Generators
  4. Fuel Systems
     - a. Natural Gas
     - b. Diesel

B. Water Utilities
System Control and Data Acquisition system (SCADA)
C. Computer aided Dispatch Systems
1. Police System (average 24 calls/hour—25 percent increase in calls w/ power outage)
2. Fire System
3. Texas Crime Information Center (TCIC)/National Crime Information Center (NCIC) [criminal history and outstanding warrants]
4. Mobile Data Terminals
5. Records Systems
D. Communications
1. Telephone System
2. 911 System
3. 800 MHz Radio System
a. Police
b. Fire
c. Emergency Services
d. Public Works
4. Pager System
5. Cellular Telephones
E. Traffic Control Systems
1. Traffic Signal control cabinet Testing
2. Prioritizing high volume intersections for Police control if electricity is lost
3. Stop sign installations at all remaining signalized intersections (i.e. portable stands, traffic signal poles, sign poles, etc. * * *)

II. The Y2K exercise

A functional exercise was developed to test the organization's response to possible Year 2000 failures of internal and external systems. The exercise was designed to test the organization's ability to provide services to the citizenry under several "worst case" scenarios. Managers were evaluated on their thoroughness, realistic approach to the exercise, and the level of coordination demonstrated in their responses.

Objectives

A. Identify the internal elements that affect the services provided by the organization.
B. Identify the external elements that have an impact on internal services provided.
C. Ensure that contingency plans provide realistic solutions for potential systems failures.
D. Instill public confidence in the organization's ability respond to Y2K problems.

Lessons learned

A. The organization must continue to plan and prepare for Y2K through 1999.
B. The organization must establish priorities to ensure adequate response to multiple issues. As we had anticipated one of the major points of vulnerability for Lubbock was electric power. We had several scenarios thrown at us that left portions of the city without electric service for brief periods of time. Such disruptions were ambiguous—while typical of weather problems, Y2K problems could also be the culprit. As a result we experienced periods where we were without some of our radio systems, all cellular phones and pagers. When power outages occurred we also lost operation of our wastewater treatment plant and one sewer lift station.
C. It is critical to have good working relationships with entities that we rely upon for other services (i.e. electrical power, gas supplies, EMS and FAA, etc.). When situations occur like during the Y2K drill, it is imperative that you have a method of constant communication with these entities. We were called upon to allow landings of several aircraft that were diverted from other airports that had lost radar service.

III. Recommendations

Lubbock is unique in that there are three power companies serving the city, one of which is owned and is managed by the City of Lubbock. This affords the City the ability to "island" itself from the national grid system in the event of widespread power disruptions.

While Lubbock has a unique electric power situation, most of the nation's cities do not. It is of utmost importance for the federal government, and more importantly you as members of the Senate, to urge the electric industry leadership to insure that

their production and transmission systems are Y2K compliant. A failure to assure reliable electric service can be devastating.

Each city should adequately address the five following basic questions relevant to Y2K:

1. Is the organization Y2K Compliant?
2. What are the basic consequences of Y2K failures for the organization?
3. Can all problem areas be addressed prior to January 1, 2000?
4. Are there sufficient resources within the organization to address all Y2K issues, if not, are there outside resources that can provide support?
5. Have contingency plans been developed to deal with the effects of Y2K?

RESPONSES OF BOB CASS TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Do you feel it is critical that every major city or local government carry out a similar simulation, or are there ways to more economically share the lessons learned from exercises such as your own?

Answer. From our perspective, it would be very difficult for a city to know their level of readiness without conducting some type of simulation and/or developing a readiness tracking system. It is true however, that lessons learned from an exercise would be beneficial to other cities.

Question 1A. Are you aware now of other cities and municipalities that plan to do a similar exercise?

Answer. We have determined that Montgomery County in Maryland is planning to have a similar exercise in December 1998. Other cities have indicated that plans are being made to conduct an exercise, however, we are not aware of specific dates being set.

Question 1B. Are organizations of municipalities such as the U.S. Conference of Mayors, the League of Cities, or the International City/County Management Association prepared to capture lessons learned from your Y2K dry run?

Answer. Public Technology, Inc. (PTI), the National League of Cities (NLC), the National Association of Counties (NACo), and the International City/County Management Association (ICMA) have launched the Y2K and YOU Campaign (http://pti.nw.dc.us/membership/y2k/) to make local appointed and elected officials aware of the impact of the Year 2000 problem. The Y2K and YOU website has local government links to the City of Lubbock's Y2K webpage and those of thirteen other local government entities.

As part of this campaign, a "tool kit" was delivered to over 15,000 U.S. city and county governments. The tool kit contains a comprehensive package of resource materials on the Year 2000, including a video explaining the issue. To order a tool kit, contact pubs@pti.org.

Question 2. Have you learned anything from your simulation of a Y2K emergency that would indicate more Federal Government assistance is needed?

Answer. Passing legislation limiting the liability for those entities who are performing "due diligence" in preparation for the transition to the year 2000 is beneficial. In addition, special legislation to allow CDBG entitlement cities to use some percent of their allocated funds to address the Y2K problems could help.

Question 3. What impediments did you encounter in preparing for your recent Y2K exercise?

Answer. No major impediments were encountered. The entire city staff as well as other agencies were more that willing to provide their support in the development of the exercise. Our Exercise Control Team was responsible for developing and administering the exercise.

Question 4. What were the greatest problems you encountered during the actual exercise?

Answer. The emergency response to the Y2K issues in the early stages of the event is not significantly different than any other natural or man made disaster. However, some of the major issues faced during the exercise were the loss of electric power to a major portion of the city, telephone systems went down, the 9–1–1 system went down, police and fire communications were lost, and we lost natural gas to approximately one fourth of the city. (See attached copy of the Exercise Scenario).

Question 5. What would you consider to be the greatest challenge to cities overall in regard to Y2K preparedness?

Answer. We feel the greatest challenge is to ensure the organization has identified and tested internal systems and developed realistic contingency plans based on a worst case scenario. In addition, the city should maintain an awareness of the community's readiness by conducting a community wide Y2K Community Readiness As-

sessment. The assessment will provide information as to the readiness of it's critical business partners (suppliers) for continued operations in the Year 2000.

Question 6. What do you consider to be the most pressing Y2K issues for your own city's emergency service agencies?

Answer. The most pressing issues facing emergency services agencies are to ensure an accurate inventory of the systems with embedded chips is taken and the problem areas identified are correct as early as possible. In addition, there are specific issues that need to be addressed within the public safety area. For example, the patrol officer could face problems with his vehicle, police radio, mobile data terminal, radar systems, and traffic signal systems. The fire fighter could have similar situation with additional problems with fire apparatus, fire radio systems, gas analyzers, cascade system for filling air bottles, and the readiness of neighboring volunteer agencies who have mutual aid with the city.

PREPARED STATEMENT OF SENATOR SUSAN M. COLLINS

Thank you, Mr. Chairman. Before I begin, I would like to thank the Chairman and his staff for their hard work on this important topic. The Chairman should be commended not just for his efforts on today's hearing, but on the entire Y2K issue. The Chairman's tireless efforts on the Y2K matter have helped many in this country understand the importance of being prepared in order to prevent serious problems at the turn of the century.

One of the issues that the Committee will focus on at today's hearing is how the year 2000 will affect computer systems used by the many law enforcement departments that we have throughout our country. In particular, an obvious area of interest is how 911 service will be affected and what municipalities should do to ensure that there will not be coverage problems.

The 911 system had modest origins, beginning as a simple "hotline" system in 1968. In the thirty years since the system was first introduced, the 911 safety net has become an integral part of American life. Today, Americans living in 90 percent of our communities can take for granted the fact that if they dial 911, someone will be on the other end of the line to offer assistance.

And 911 is a number that we dial often in this country—over 300,000 911 emergency calls for assistance are placed in this country each day, close to 110 million calls per year.

As the size of the 911 system has grown over the years, the technology that supports our emergency services has continued to advance at a tremendous rate. Many places in the country now enjoy the advantage of so-called "enhanced" 911 systems. These enhanced systems automatically pinpoint a caller's location and telephone number for the 911 operator.

911 calls are received at what is known as Public Safety Answering Points, or "PSAPs." [P-Saps] There are over 4,500 of these PSAPs throughout the country. The person answering the phone at these PSAPs is often required to fill out a computer screen which looks something like this [Reference 30 X 40 Poster Board], particularly in the case of "enhanced" 911 systems.

Earlier this summer, FCC Commissioner Michael Powell began playing an active role in promoting awareness about this potential communications problem in the public safety community. In June, the FCC held a public safety roundtable which attracted many nationwide experts in the field of public safety communications.

This symposium concluded that while the Y2K problem poses a threat to these communications, the problem is fixable. Unfortunately, the fix can be expensive, with some departments finding that the best solution to the problem is to completely replace the old non-compliant systems. Moreover, the Association of Public Safety Communications Officers has estimated that there are over 50 components in a PSAP that are Y2K-vulnerable.

In addition to 911 systems, law enforcement agencies use other sophisticated information technology systems in their day-to-day efforts to fight crime. Examples include the National Crime Information Center, the National Law Enforcement Telecommunications System, and the individual criminal information data systems operated individually by all 50 states.

These systems enable officers to obtain the most updated information on wanted persons, stolen vehicles, criminal histories, and Department of Motor Vehicle records. The ability to dependably and quickly access such information is essential both to officer safety and to the speedy and effective administration of justice at all levels of government.

The good news here is that the Committee has been assured that these systems will be fully able to meet its Year 2000 challenge, and that their links to the sys-

tems of all 50 states will remain fully operational. The challenge for local law enforcement agencies is to be sure that their own links to these vital information systems, and any similar systems which they might operate on a regional or agency-wide level are both compliant and compatible with the larger systems.

Also, at the local agency level, there often is a great deal of "interconnectivity" between some of the emergency service department's records systems and those of other city agencies, such as the court system, the corrections department, and even local utility companies, thus increasing the potential for Y2K related problems in this area.

I am hopeful that we will be able to gain more information on these important issues in today's testimony. Thank you, Mr. Chairman.

PREPARED STATEMENT OF VICE CHAIRMAN CHRISTOPHER J. DODD

Thank you Mr. Chairman, for your leadership. This Committee continues to have a very active hearing schedule as we review Year 2000 issues in a variety of industry sectors. The Committee has examined the energy sector, transportation, health care and financial services and will soon hold a general business hearing with an emphasis on small business. Today, we will review emergency preparedness and disaster relief on a national, state and local level. Indeed few functions of government are more fundamental and important than our government's readiness to respond to the needs of its citizens in emergencies.

These emergencies can be on a grand scale such as floods, tornadoes and earthquakes or they can be personal emergencies, where one person may need the police or the fire department or an ambulance. In all of these situations, there is a shared common denominator, communication systems that receive the calls and direct the response. And most importantly these systems may be very vulnerable to year 2000 problems.

Sophisticated information technology systems serve as important tools for law enforcement today. Systems such as the National Crime Information Center or NCIC, the National Law Enforcement Telecommunications System, or NLETS, and individual criminal information data systems operated by each state enable of fleers to obtain the most updated information on wanted persons, stolen vehicles, criminal histories, and Department of Motor Vehicle records. The ability to dependably and quickly access such information is essential both to officer safety and to the speedy and effective administration of justice at all levels. A recent survey conducted on the effectiveness of NCIC indicates that during a one year period, 81,750 "wanted" persons were found, 113,293 individuals were arrested; 39,268 missing juveniles and 8,549 missing adults were located; and 110,681 cars valued at over $570 million were recovered as a result of NCIC's use. The good news is that we have been assured that this system will be fully able to meet its Year 2000 challenge, and that its links to the systems of all 50 states will remain fully operational. The challenge for local law enforcement agencies is to be sure that their own links to these vital information systems, and any similar systems which they might operate on a regional or agency wide level are both compliant and compatible with the larger systems. Also, at the local agency level, there often is a great deal of interconnectivity between some of the emergency service department's records systems and those of other city agencies, such as the court system, the corrections department, and even local utility companies, thus increasing the potential for Y2K related problems in this area.

As we have found to be true in so many other areas, Y2K's presence is insidious in the area of emergency services. One major police department related to our staff that its city's government was required to remediate their gasoline pumps in order to assure that gasoline would continue to flow to its patrol cars on January 1, 1998. This problem had the potential to effect the entire fleet of city government owned vehicles. In this particular case, the computerized gasoline pumps perform a time and date calculation based upon the last time a particular gas credit card was used to fuel a vehicle, and therefore was vulnerable to Y2K. In another case, the sheriff of a large western county related that his department was currently examining its computerized detention files which are used to track "time in" and "time out" of the county jail facility, as well as hearing date information for inmates.

According to the Bureau of Justice Statistics, there are over 17,000 police and sheriffs departments in the United States. The International Association of Fire Chiefs estimates that there are 32,000 fire departments in this country. We also should not overlook the fact that approximately sixty-five percent of our country's Emergency Medical Service agencies reside within the organizational structure of our nation's fire departments.

These statistics clearly indicate the scope of the emergency service sector at the state, county, and local levels of government is enormous. The task of assuring that each of these agencies meets the challenge of providing uninterrupted and reliable service in the Year 2000, is an immense one. It is a task that must be tackled in each and every city, township, county, and state government in the country.

In addition to the technical aspect of Y2K vulnerabilities, we must also consider the possibility that January 1, 2000 may bring with it an enormous increase in the demand for service from our emergency response agencies. Will there be an increase in the need for additional traffic control personnel in the event of certain Y2K failures in the transportation sector? How many additional elevator extrications will the fire departments be called upon to perform? None, we hope, but these are all things we must consider as we plan.

While the preparedness of emergency service agencies is the most vital aspect of Y2K preparation for state, county and local governments, we must recognize that it surely is not the only Y2K problem that those governments face. It is in fact, only one aspect of the much larger Y2K challenge confronting the mayors, city and county executives, state CIOs, and governors throughout the nation as we continue to move closer to our ultimate deadline.

As I mentioned at the beginning of my statement, the federal government must be able to respond to earthquakes, floods and other natural disasters. And I share Senator Bennett's heartfelt thoughts to those who have suffered through Hurricane George. The destructive power of this hurricane must remind us how very essential it is that our state and national emergency response systems operate without impediment. The Federal Emergency Management Agency (FEMA) along with the Red Cross and the National Guard has always provided a safety net to our citizens whose lives and communities have been devastated by natural disasters. It is essential that these organizations maintain their continued readiness.

On a final note, I want to enthusiastically endorse the creation of an early warning system that might give this country some notice, even if it is only a matter of hours, that Year 2000 failures occurring internationally are headed our way. January 1, 2000 dawns in the middle of the Pacific Ocean and comes 17 hours before our dawn in the United States. We should leverage this advantage that nature and chance has provided us, and a "Y2K First Alert System" is an excellent way to do so.

Again, thank you Mr. Chairman, I look forward to hearing today's panels.

PREPARED STATEMENT OF JOHN THOMAS FLYNN

CONGRESSIONAL TALKING POINTS

Good morning, Mr. Chairman. My name is John Thomas Flynn. I speak before you today as president of NASIRE, representing the Chief Information Officers of the States, and as Governor Pete Wilson's Chief Information Officer for California.

I want to express my appreciation for the opportunity to update this committee on states' Year 2000 (Y2K) readiness, particularly as it affects emergency preparedness. To get right to the point: as to states' overall remediation efforts, compliance among the 50 states with all aspects of mission critical legacy systems, ranges individually from under 10 percent complete, to reports of more than 90 percent complete. I would point out that these figures are based upon NASIRE's self-reporting online survey, *Y2KRemediation in the States*, (located at www.amrinc.nettnasire/y2k).

According to the latest survey results, just under half (24) of those responding have completed remediation of at least 50 percent of their mission critical systems. Our NASIRE survey defines "mission critical" as:

> Systems that the state has identified as priorities for prompt remediation. Such systems CAN encompass public safety, public health, as well as financial and personnel aspects of government services.

No state has declared itself 100 percent complete as yet. In addition, due to the various interpretations surrounding the term, as well the legal ramifications involved, we might never see total compliance claimed until long after the turn of the century.

As the remediation process has evolved from addressing software applications and interfaces, desktop systems and embedded technologies, a key focus of activity in the states has involved contingency planning, operational recovery and of particular importance to this hearing today, emergency preparedness.

As to the general condition of the states' emergency preparedness and the readiness of state emergency response agencies I would offer the following.

Disaster relief services are facets of a civilized society that citizens should be able to depend on.

Imagine the residents of New Orleans or the Florida Keys managing without state emergency and disaster services with Hurricane Georges positioned to wreak havoc at any moment. Recall the total power blackout that occurred for several weeks in the business district of Auckland, New Zealand earlier this year. Would recovery and rebuilding efforts work at full capacity or at all if their systems and networks were nonfunctional? Would citizens have access to life-saving medical aid?

Recall the Galaxy 4 satellite that put 50 million pagers and other telecommunications services out of commission. One satellite. 50 million customers affected. When you think about how many lives are touched by one action, or in this case, inaction, the magnitude of the Year 2000 situation begins to take shape.

Regarding specific emergency preparedness issues, eleven states responded to the NASIRE survey including:

> Arizona, Colorado, Connecticut, Florida, Georgia, Illinois, South Carolina, Texas, Washington, West Virginia, Wyoming

NASIRE CIO's reported that close working relationships have been established with their emergency management organizations, and their mission critical system remediation has been given the highest priority. A few specifics:

For example, the State of Arizona holds bi-weekly meetings with Y2K coordinators from the Public Utility Commission, Attorney General's Office, Administrative Office of the Courts and the Department of Emergency and Military Affairs to coordinate assessment, planning and response activities related to Y2K failures. Staff representatives from both senators McCain and Kyl were recently invited to these meetings.

The Colorado 2000 Council has asked the Colorado Office of Emergency Management and the Federal Emergency Management Association (FEMA), to participate in Colorado's Council. This council is a coalition of public and private industry representing critical service sectors such as telecommunications, public safety and water, to name just a few.

In California, the Governor's Office of Emergency Services (OES) is a stand-alone cabinet-level agency like the Department of Information Technology, which reports directly to the Governor.

Having this kind of authority naturally leads to quicker and more comprehensive responses. As you may know California, during the last decade, has suffered through flood, fire, drought, riots and other natural disasters with responses coordinated by this department.

As CIO for California, my office is partnering with California OES Director, Dr. Richard Andrews, along with our California Year 2000 Intergovernmental Task Force, which is comprised of state, county and city CID's, for a Western States Y2K Summit on Emergency Preparedness and contingency planning this fall. Dr. Andrews and I have been in contact with the emergency directors, state CIO's and Y2K managers of these states who have voiced unanimous enthusiasm for this endeavor. We believe the model and subsequent action plan we develop for this summit will be of value to states not only in the western region, but beyond.

As a general rule, emergency management services do not fall directly under the responsibility of IT organizations. However, those who work in the IT environment are prepared to work with sister agencies with missions more directly tied to providing support and order during a disaster. This is and has been the case in the many other government entities which merit equal attention such as public utilities (water, electricity, telecommunications), court and criminal functions (prison systems) and financial benefits (retirement disbursements, food stamps, health care).

I thank you for the opportunity to speak, and would be pleased to answer any questions.

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES

[A survice of NASIRE: Representing chief information officers of the States]

ALABAMA (Last updated 8/10/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
NA	AL has implemented a separate Y2K mainframe test bed with Y2K compliant operation system and tools for agencies to use for testing. There is also an AS/400 resource center.	$85–$100M	Considering (Some current members are aware of the Y2K problem and may be considering both funding and liability issues.)	The AL Dept. of Finance has an integrated accounting, purchasing and personnel system for most of the state agencies. The accounting covers departmental or agency level accounting as well as the State's Comptroller. Many of the agencies providing direct services and benefits are utilizing the Finance Department's mainframe computer. The Finance Department provides fee based services for agencies, but the larger ones mentioned above have their own programming staff.

CIO: Larkin B. Nolen, Chief Information Officer, Information Services Division, Dept. of Finance, 64 N. Union St., Ste. 200, Montgomery, AL 36130, Phone: 334–242–3800 Fax: 334–240–3228 lnolen@isd.state.al.us

Contact: Rick Boyce, Year 2000 Project Coordinator, Dept. of Finance, 64 North Union Street, Ste. 250, Montgomery, AL 36130, Phone: 334–353–3447 Fax: 334–353–5663 rboyce@isd.state.al.us

Contact: Dr. John H. Parsa, Manager Special Projects, Information Services Division, Dept. of Finance, 64 N. Union St., Ste. 250, Montgomery, AL 36130, Phone: 334–242–3104 Fax: 334–353–5663 jparsa@isd.state.al.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

ALASKA (Last updated 9/9/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
86 Mission Critical Business Functions (43% of 199 key functions), including: all supporting automation systems, interfaces, embedded and process control systems, supplier/customer dependencies, and associated contingency plans.	A number of critical enterprise-level systems are already converted. Compilation of status data is expected to be available by 10/1/98.	FY 2000 costs for Y2K are currently estimated at $25 million.	Not to date. Proposals are under consideration, however.	Governor Tony Knowles issued Administrative Order #177 on 8/28/98, declaring Y2K to be state agencies' highest priority and elevating the State's Y2K program to a cabinet-level office. Since then a new Y2K status reporting system has been implemented, with updated status information expected to be available by 10/1/98.

CIO: Mark O. Badger, PhD, Chief Technology Officer, Information Technology Group, Dept. of Administration, P.O. 110206, Juneau, AK 99811–0206, Phone: 907–465–2220 Fax: 907–465–3450 mark_badger@admin.state.ak.us

Contact: Bob Poe, Year 2000 Project Manager, Office of Management & Budget, P.O. Box 110020, Juneau, AK 99811 Phone: 907–465–4660 Fax: 907–465–3008 Bob_Poe@gov.state.ak.us

ARIZONA (Last updated 9/25/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
245	60–70%	$103.0M (This is for data systems not embedded systems. This includes appropriated and non-appropriated dollars. It also includes replacements and remediation, some of these replacements are occurring for other reasons, but Y2K makes the timing critical. It also includes personnel costs, which I believe some states have not included.)	Yes, Special funding (HB2001); No, Liability hold harmless. The Arizona League of Cities is circulating a broad based liability protection bill for municipalities, but I have not yet reviewed a draft.	None.

CIO: John B. Kelly, Chief Information Officer, Gov't Information Technology Agency, 1102 W. Adams St., Phoenix, AZ 85007, Phone: 602–340–8538 Fax: 602–340–9044 jbkelly@gita.state.az.us

Contact: Art Ranney, Information Technology Oversight Manager, Government Information Technology Agency, 1102 W. Adams Street, Phoenix, AZ 85007, Phone: 602–340–8538 Fax: 602–340–9044 adranney@gita.state.az.us

ARKANSAS (Last updated 7/27/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
50	40%	$35.0M	Yes. (A general use appropriation has been made available for all Arkansas State agencies to accomplish Y2K compliance.)	We are currently conducting y2k audits of all state agencies, higher ed institutions, and public schools. This is probably the most valuable thing we have done.

CIO: Michael Hipp, Director, Dept. of Information Systems, #1 Capitol Mall, P.O. Box 3155, Little Rock, AR 72201–3155, Phone: 501–682–2701 Fax: 501–682–4310 michael.hipp@mail.state.ar.us

Contact: Stephanie Mains, Year 2000 Project Office, Division of Operations, Department of Information Systems, P.O. Box 3155, #1 Capitol Mall, Little Rock, AR 72201, Phone: 501–682–4399 Fax: 501–682–4310 stephanie.mains@mail.state.ar.us

CALIFORNIA (Last updated 9/25/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
633	50%	$239 million.	3 Measures were proposed for the 1997–98 legislative session, none were successful (AB1934; AB1710 and SB2000). 2 measures are on the Governor's desk for consideration (AB1345 and SB1178)The 1998–99 Budget Act includes $20 million for the Year 2000.	Information can be found at <www.leginfo.ca.gov>.

CIO: John Thomas Flynn, Chief Information Officer, State of California, 801 K St., Ste. 2100, Sacramento, CA 95814, Phone: 916–445–3050 Fax: 916–445–6529 jtflynn@doit.ca.gov

Contact: Claudina Nevis, Deputy Director, Special Projects, Dept. of Information Technology, 801 K St., Ste. 2100, Sacramento, CA 95814, Phone: 916–445–5900 Fax: 916–445–6524 claudina.nevis@doit.ca.gov

Contact: Robert Dell'Agostino, Acting Chief Deputy Director, Dept. of Information Technology, 801 K St., Ste. 2100, Sacramento, CA 95814, Phone: 916–445–5900 Fax: 916–445–6524 bob.dellagostino@doit.ca.gov

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

COLORADO (Last updated 9/24/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
239 systems are rated critical of a total of 840 systems.	6% are fully converted for Year 2000 functionality. The majority of the remaining systems are in the testing phase.	$31.95M (Covers information systems only. Does not include higher education or embedded systems.)	Considering	90% of Critical systems are planned for completion by June, 1999.

CIO: Steve McNally, Staff Director, Commission on Information Mgmt., Dept. of Personnel/Gen. Support Svcs., 1525 Sherman St., Ste. 100, Denver, CO 80203–1712, Phone: 303–866–3222 Fax: 303–866–2168 steve.mcnally@state.co.us

Contact: Brian Mouty, Statewide Year 2000 Project Manager, Dept of General Support Services, 1525 Sherman St., #100, Denver, CO 80203, Phone: 303–866–3222 Fax: 303–866–2168 brian.mouty@state.co.us

CONNECTICUT (Last updated 9/23/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
765 (Systems for which Y2K remediation strategies have been defined.)	50%	$125.0M (Although only $95.0M in funding is available.) Embedded systems and PC exposures not fully known—may drive total costs higher.	Yes.	None.

CIO: Rock Regan, Chief Information Officer, Dept. of Information Technology, 340 Capitol Ave., Hartford, CT 06106, Phone: 860–566–7093 Fax: 860–566–1786 rock.regan@po.state.ct.us

Contact: Peter Sullivan, Director, Year 2000 Program Officer, Dept. of Information Technology, 340 Capitol Avenue, Hartford, CT 06106, Phone: 860–566–6246 Fax: 860–566–6291 peter.sullivan@po.state.ct.us

DISTRICT OF COLUMBIA (Last updated N/A.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
No answer.	No answer.	No answer.	No answer.	None.

CIO: VACANT, Chief Technology Officer, Government of DC, 441 Fourth St., N.W., Rm. 960, Washington, DC 20001, Phone: 202–727–2277 Fax: 202–727–6857 mike@dcgov.org

DELAWARE (Last updated 7/17/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
71 (Included are public safety systems, critical general ledger/accounting, critical court systems, public health and some critical welfare systems, critical revenue systems, unemployment insurance, and payroll-but not all benefits.)	62% (Complete or already compliant.)	$6.0M	Yes, Legislated funding.	None.

CIO: John J. Nold, Executive Director, Office of Information Services, 801 Silver Lake Blvd., Dover, DE 19904, Phone: 302–739–9628 Fax: 302–739–6251 Nold@ois.state.de.us
Contact: Kathy Donovan, Year 200 Coordinator, Office of Information Systems, 801 Silver Lake Blvd., Dover, DE 19901, Phone: 302–739–9602 Fax: 302–739–9686 ldpmpvam@state.de.us

FLORIDA (Last updated 9/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
492	74% (Using August data-this is the overall percentage of work completed in the remediation of mission critical systems.)	$75.0–90.0M	Yes, provides the Governor special powers in addressing a Y2K failure in an agency and extends the state's sovereign immunity to include Year 2000 failures. Passed as CS/HB 3619 in the 1998 session.	Florida is conducting further research into the potential impact of embedded chips in products & services.

CIO: P. J. Ponder, Chief Legal Counsel, Information Resource Commission, 4050 Esplande Way, Ste. 235, Tallahassee, FL 32399–0950, Phone: 850–488–4494 Fax: 850–922–5929 ponderp@irc.state.fl.us
Contact: Glenn W. Mayne, Project Manager, Executive office of the Governor, Office of Planning and Budgeting, 426 Charlton Bldg., Tallahassee, FL 32399, Phone: 850–921–2235 Fax: 850–921–2353 glenn.mayne@laspbs.state.fl.us

GEORGIA (Last updated 7/15/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
375 (Business criticality as defined by 71 agencies.)	Still developing metrics and consolidated reporting.	$152.0M	Yes, liability and financial (SB638).	None.

CIO: Paul Mason, Director, Information Technology, Dept. of Administrative Services, 1402 W. Tower, 2 Martin Luther King Dr., Atlanta, GA 30334, Phone: 404–656–3992 Fax: 404–656–0421, pmason@doas.state.ga.us
Contact: Erwin Fraas, Senior Technology Analyst, Information Technology Policy Council, P.O. Box 38391, Atlanta, GA 30334, Phone: 404–657–1351 Fax: 404–657–1355 btthomas@itpc.state.ga.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

HAWAII (Last updated 4/13/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
No answer.	No answer.	No answer.	No answer.	None.

CIO: Thomas I. Yamashiro, Administrator, Information & Communication Svcs. Div., Dept. of Accounting & General Services, 1151 Punchbowl St., Room B10, Honolulu, HI 96813, Phone: 808–586–1910 Fax: 808–586–1922 tyamashi@icsd.hawaii.gov

Contact: Barbara Tom, Data Processing Systems Manager, Information & Communication Svcs. Div, Dept. of Accounting & General Services, 1151 Punchbowl St., Room B10, Honolulu, HI 98613, Phone: 808–586–1920 Fax: 808–586–1922

IDAHO (Last updated 8/14/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
21	60%	$16.0M	No.	Most mission critical applications are in test mode. Testing and data bridge remediation are the gating issues at this time. No specific legislation has been proposed or is anticipated.

CIO: J. Miles Browne, Project Team Manager, Information Technology Division, Dept. of Administration, 650 W. State Street, P.O. Box 83720, Boise, ID 83720–0004, Phone: 208–334–2771 Fax: 208–334–2307 mbrowne@adm.state.id.us

Contact: Dean Pierose, Member, ITRMC Project Team, Dept. of Administration, 650 W. State Street, P.O. Box 83720, Boise, ID 83720–0089, Phone: 208–334–3535 Fax: dpierose@adm.state.id.us

ILLINOIS (Last updated 8/4/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
349	59% of the Critical Systems effort.	$82.3M (For all electronic data processing efforts.)	Yes—SB1674, establishes Year 2000 Technology Task Force.	None.

CIO: William M. Vetter, Bureau Manager, Bureau of Communication & Computer Svcs., Dept. of Central Management Services, 120 W. Jefferson St., Springfield, IL 62702, Phone: 217–782–4221 Fax: 217–524–6161 wvetter@cms084r1.state.il.us

Contact: Paul R. Lopes, Chief of Operations/ Computer Services, Bureau of Comm. & Computer Svcs., Dept. of Central Management Services, 120 W. Jefferson St., Springfield, IL 62702, Phone: 217–785–4037 Fax: 217–524–6161 paul%lopes@ccmailgw.state.il.us

INDIANA (Last updated 7/20/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
51	4%	$34.6M	Yes, funding.	None.

CIO: Laura Larimer, Director of Information Technology, Dept. of Administration, Indiana Government Center, 100 North Senate Ave., N. Rm. 551, Indianapolis, IN 46204, Phone: 317–232–3171 Fax: 317–232–0748 llarimer@isd.state.in.us

Contact: William Pierce, Director, Director of Year 2000 Office, 125 West Market Street, Indianapolis, IN 46204, Phone: 317–233–2009 Fax: 317–233–8315 bpierce@dpoclan.state.in.us

IOWA (Last updated 9/9/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
270 (Each agency in the Executive Branch determined the critical systems for their enterprise. This figure does not include the number of critical systems that are related to the embedded remediation.)	41%	$30.0M (This figure does not include the costs related to the embedded systems remediation.)	No.	None.

CIO: James R. Youngblood, Director, Information Technology Services, Hoover State Office Building, Level B, Des Moines, IA 50319, Phone: 515–281–3462 Fax: 515–281–6137 jim.youngblood@its.state.ia.us

Contact: Paul Carlson, Year 2000 Project Manager, Dept. of Management, State Capitol Bldg., Rm. 13, Des Moines, IA 50319, Phone: 515–281–7117 Fax: 515–242–5897 pcarlso@max.state.ia.us

KANSAS (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
827	67%	$23.0M	Considering liability.	None.

CIO: Frederick Boesch, Chief Information Architect, Information Resource Council, 300 SW 10th Ave., State Capitol Bldg., Rm. 263E, Topeka, KS 66612–1572, Phone: 785–296–3011 Fax: 785–296–2702 fredb@dasec.wpo.state.ks.us

Contact: John Oliver, Senior Policy Advisor, Office of the Chief Information Architect, LSOB Rm. 751–S, 900 S.W. Jackson, Topeka, KS 66612–1275, Phone: 913–296–5260 Fax: 913–296–1168 johno@dadisc1.wpo.state.ks.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

KENTUCKY (Last updated 9/29/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
96 (Mainframe systems only. Critical systems under management of agencies have not been defined. Information has been extracted from May 31, 1998.)	57%	$4.0M	Yes, Y2K contingency fund was passed in the 1998 session.	Kentucky is on target to complete renovation by 7/1/1999.

CIO: Aldona K. Valicenti, Chief Information Officer, Commonwealth of Kentucky, Office of the Governor, 493 Capitol Annex, Frankfort, KY 40601, Phone: 502–564–2611 Fax: 502–564–7882 avalicenti@mail.state.ky.us

Contact: John Tomlinson, Year 2000 Statewide Coordinator, Information Systems, 101 Cold Harbor Dr., Frankfort, KY 40601, Phone: 502–564–8715 Fax: 502–564–6856 jtomlinson@mail.state.ky.us

LOUISIANA (Last updated 9/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
399 Mission Critical Systems as of September 1998.	30%	Not known at this time. (Although the majority of Year 2000 costs were embedded in the general operating budget of state departments, the following information is available: FY97–98 Budgeted $16.4; FY98–99 Requested $61; $5 established for Y2K fund pool.)	Considering (The state is reviewing all legal aspects of the Year 2000 problem and consideration is being given for introducing legislation in the next legislative session schedule for March 1999.)	None.

CIO: Dr. Allen Doescher, Assistant Commissioner, Technical Service & Communications, Office of Information Resources, Div. of Administration, P.O. Box 94095, Baton Rouge, LA 70804–9095, Phone: 504–342–7000 Fax: 504–342–1057 adoesch@.doa.state.la.us

Contact: Chris LeBlanc, Year 2000 Project Manager, Div. of Administration, P.O. Box 44335, Baton Rouge, LA 70804–4335, Phone: 504–342–9675 Fax: 504–342–5137 cleblan@doa.state.la.us

MAINE (Last updated 9/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
180 (The number of critical systems out of 257 systems that we are currently tracking. The critical systems were determined by tracking data from each of the state agencies and only those agencies which have supplied information to the Department of Administration & Finance, Bureau of Information Services.)	40%	$11.0M (This figure is for the state agencies with critical systems only.)	No, but it was considered.	None.

CIO: Robert Mayer, Chief Information Officer, Bureau of Information Services, Dept. of Admin. & Financial Services, 145 State House Station, Augusta, ME 04333–0145, Phone: 207–624–7840 Fax: 207–287–4563 robert.a.mayer@state.me.us

Contact: Valton L. Wood, Jr., Div. Mgr. Infor, Svcs/Development Svcs., Bureau of Information Services, Dept. of Administrative & Financial Svcs., 145 State House Station, Augusta, ME 04333–0145, Phone: 207–287–3631 Fax: 207–287–4563 valton.wood@state.me.us

MARYLAND (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
341	To Be Determined (We are in the process of updating our database so that an accurate assessment can be made. The state has 22 vendors as partners in this effort. Approximately $35M has been obligated to date.	$100.0M	No.	None.

CIO: Leslie E. Hearn, Chief Information Officer, Dept. of Budget & Management, Office of Information Technology, 45 Calvert St., Annapolis, MD 21401, Phone: 410–974–5236 Fax: 410–974–5045 lhearn@dbm.state.md.us

Contact: Alexius O. Bishop, Year 2000 Coordinator, Office of Information Technology, 45 Calvert St., Annapolis, MD 21401, Phone: 410–974–2191 Fax: 410–924–5045 abishop@dbm.state.md.us

MASSACHUSETTS (Last updated 7/20/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
262	33%	$79.0M	Yes, funding.	None

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

CIO: Val Asbedian, Director, Strategic Planning, Information Technology Division, One Ashburton Place, Room 801, Boston, MA 02108, Phone: 617–973–0762 Fax: 617–727–3766 val.asbedian@state.ma.us
Contact: Val Asbedian, Director, Strategic Planning, Information Technology Division, One Ashburton Place, Room 801, Boston, MA 02108, Phone: 617–973–0762 Fax: 617–727–3766 val.asbedian@state.ma.us

MICHIGAN (Last updated 8/20/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
793	42%	$55.6M (This is what has been appropriated as supplemental funding for Y2K problems in executive branch agencies.)	Yes, funding.	None.

CIO: George Boersma, Chief Information Officer & Deputy Dir., Director's Office, Dept. of Management & Budget, 1st Flr., Lewis Cass Bldg., P.O. Box 30026, Lansing, MI 48909, Phone: 517–373–1006 Fax: 517–373–7268 boersmag@state.mi.us

Contact: Gerald W. Williams, Director, Year 2000 Project Office, Dept. of Management & Budget, 1st Flr., Lewis Cass Bldg., P O Box 30026, Lansing, MI 48909, Phone: 517–373–3725 Fax: 517–335–1575 williamsj3@state.mi.us

MINNESOTA (Last updated 9/15/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
1,300 (During the inventory phase of the Minnesota Year 2000 Project, 1,100 custom applications were identified by state agencies.)	75% (70 percent of custom applications are complete. A deadline of December 31, 1998 has been established to complete conversions of mission critical systems. Testing is an ongoing process that will continue through 1999.)	As of June 1998, the Minnesota legislature has appropriated $28.7M for conversion of mission critical systems. State agencies are also using an estimated $22 from operational fund budgets to address embedded technologies and standard upgrades of h/w, s/w.	Considering.	None.

CIO: Beverly Schuft, Assistant Commissioner, Technology Management, Dept. of Administration, 320 Centennial Bldg., 658 Cedar St., St. Paul, MN 55155, Phone: 612–296–5320 Fax: 612–296–5800 bev.schuft@state.mn.us

Contact: Jim Close, Year 2000 Project Manager, Technology Management Bureau, Dept. of Administration, 320 Centennial Bldg., 658 Cedar St., St. Paul, MN 55155, Phone: 612–296–5944 Fax: 612–296–5800 jim.close@state.mn.us

MISSISSIPPI (Last updated 7/16/1998.)

How many critical systems do you manage?[1]	What percent of these critical systems are converted?[2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
30	50% (Should be at least 75 percent by December 1.)	$8.0M	No.	None.

CIO: David L. Litchliter, Executive Director, Dept. of Information Technology Svcs., 301 N. Lamar St., Ste. 508, , Jackson, MS 39201, Phone: 601–359–1395 Fax: 601–354–6016 litchliter@its.state.ms.us

Contact: Teresa Karnes, Client Planning Manager, Strategic Services Division, Dept. of Information Technology Svcs., 301 N. Lamar St., Ste. 508, Jackson, MS 39201, Phone: 601–359–2615 Fax: 601–354–6016 karnes@its.state.ms.us

MISSOURI (Last updated 9/16/1998.)

How many critical systems do you manage?[1]	What percent of these critical systems are converted?[2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
225	70% Converted; 50% implemented.	$57.0M	Yes, funding. Liability being considered.	None.

CIO: Mike Benzen, Chief Information Officer, Office of Information Technology, Jefferson Bldg., Rm. 1315, 205 Jefferson St., Jefferson City, MO 65101, Phone: 573–526–7741 Fax: 573–526–7747 benzem@mail.oit.state.mo.us

Contact: Dave Schroeder, Deputy Chief Information Officer, Office of Information Technology, Jefferson Bldg., Rm. 1315, Jefferson City, MO 65101, Phone: 573–526–7744 Fax: 573–526–7747 schrod@mail.oit.state.mo.us

MONTANA (Last updated 9/3/1998.)

How many critical systems do you manage?[1]	What percent of these critical systems are converted?[2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?
211	34%	$5–6	No.

Comments

None.

CIO: Anthony Herbert, Administrator, Division of Information Services, Dept. of Administration, 125 N. Roberts, P.O. Box 200113, Helena, MT 59620, Phone: 406–444–2700 Fax: 406–444–2701 therbert@mt.gov

Contact: G. Scott Lockwood, Year 2000 Compliance Officer, Information Services Division, Dept. of Administration, P.O. Box 200113, Helena, MT 59620, Phone: 406–444–2029 Fax: 406–444–2701 slockwood@mt.gov

NEBRASKA (Last updated 7/21/1998.)

How many critical systems do you manage?[1]	What percent of these critical systems are converted?[2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
82 (Not broken down by criticality.)	30%	$6.0M (Initial total estimate.)	Yes, funding, liability and personnel (www.state.nv.us/doit/y2k).	None.

CIO: Steven L. Henderson, Deputy Administrator, Central Data Processing, Dept. of Administrative Services, 501 S.14th St., P.O. Box 95045, Lincoln, NE 68509, Phone: 402–471–2065 Fax: 402–471–4864 aicsteve@vmhost.cdp.state.ne.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

Contact: Steven L. Henderson, Deputy Administrator, Central Data Processing, Dept. of Administrative Services, 501 S.14th St., P.O. Box 95045, Lincoln, NE 68509, Phone: 402–471–2065 Fax: 402–471–4864 aicsteve@vmhost.cdp.state.ne.us

NEVADA (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
278 (Criticality was determined by individual agency directors in regard to which systems they elected to include in our CDC project.)	86% (This number is derived from project schedule information regarding both work completed and work in progress.)	$15.2M (This figure is the current base contract with our vendor for century date change work. We have also established Time and Material work orders with CTA for an additional $5.5 to $6.0M for related work. Thus total cost around $21.0M.	Yes, funding. (Legislation for partial funding support was passed in 1996 utilizing parts of the existing Cigarette Tax.)	None.

CIO: Marlene Lockard, Director, , Dept. of Information Technology, 505 E. King St., Ste. 403, Carson City, NV 89701, Phone: 702–687–4090 Fax: 702–687–3846 mlockard@doit.state.nv.us

Contact: Tom Loux, Year 2000 Project Manager, Applications Design & Development Unit, Department of Information Technology, 1340 South Curry St., Carson City, NV 89701, Phone: 702–687–4091 Fax: 702–687–1155 tloux@doit.state.nv.us

NEW HAMPSHIRE (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
63 (This is number of state agencies, boards and commissions.)	10% (Several are in testing phase.)	$60.0M (This includes costs to replace outdated systems and correct Y2K at same time.)	Yes (Requires agencies to develop work plans and to report quarterly compliance status, Chapter 255, Laws of 1998: Effective June 25, 1998: legislative bill—www.state.nh.us/gencourt/bills/98bills/sb0464.html)	None

CIO: William Armstrong, Information Technology Manager, Division of Information Technology Management, Dept. of Administrative Services, 4 Hazen Dr., Concord, NH 03301, Phone: 603–271–6533 Fax: 603–271–6531 warmstrong@admin.state.nh.us

Contact: Vicki Tinsley, Information Technology Manager, Div. of Information Technology Mgmt., Dept. of Administrative Services, 4 Hazen Drive, Concord, NH 03301, Phone: 603–271–1522 Fax: 603–271–531 vtinsley@admin.state.nh.us

NEW JERSEY (Last updated 9/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
195	40% (back in production)	$120.0M (this is the cost to remediate ALL systems).	Yes, funding; considering liability.	None.

CIO: Wendy Rayner, Chief Information Officer, Office of the Governor, State House, P.O. Box 001, Trenton, NJ 08625, Phone: 609–777–2245 Fax: 609–777–0357 wwr@capitol.statehouse.state.nj.us

Contact: John W. Longworth, Executive Branch Year 2000 Coordinator, Div. of Information & Management Svcs., Dept. of Education, 100 Riverview Executive Plaza, Trenton, NJ 08625–0500, Phone: 609–633–9773 Fax: 609–633–9865 jlongwor@doe.state.nj.us

Contact: Wendy Rayner, Chief Information Officer, Office of the Governor, State House, P.O. Box 001, Trenton, NJ 08625, Phone: 609–777–2245 Fax: 609–777–0357 wwr@capitol.statehouse.state.nj.us

NEW MEXICO (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
4,436 (Only 317 were found to be non-Y2K compliant.)	49%	$12.2M	No.	None.

CIO: James Hall, Chief Information Officer, Office on Information & Comm. Management, Office of the Governor, State Capitol Bldg., Rm. 400, Santa Fe, NM 87503, Phone: 505–827–3000 Fax: 505–827–3026 jhall@gov.state.nm.us

Contact: Jody Larson, Office on Info. & Communication Staff, Office on Information & Communication Mgmt., Governor's Office 4th Fl., Capitol Bldg., Santa Fe, NM 87503, Phone: 505–827–3019 Fax: 505–827–3026 larsonj@gov.state.nm.us

NEW YORK (Last updated 7/17/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
43 (Statewide priority systems—top "40.")	73%	$83.0M (Plus $221.0M in other funded replacement projects.)	Considering, liability; yes, funding & personnel.	None.

CIO: Camaron Thomas, Director, Office for Technology, Executive Chamber, State Capitol, Albany, NY 12224, Phone: 518–473–5622 Fax: 518–473–3389 infresmg@emi.com

Contact: Gary Davis, Year 2000 Project Leader, NYS Office for Technology, State Capitol, New York, NY 12224, Phone: 518–473–5622 Fax: 518–402–2019 davisg@emi.com

Contact: Julie Leeper, Year 2000 Project Coordinator, NYS Office for Technology, State Capitol, Albany, NY 12224, Phone: 518–473–5622 Fax: 518–473–3389 leeperj@emi.com

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

NORTH CAROLINA (Last updated 9/15/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
1,147	59%	$124.8M	Yes, centralized program office, funding; considering, other issues.	Year 2000 legislation was passed to set up the NC Year 2000 Project Office which facilitates, supports, monitors and leverages the state's Year 2000 remediation efforts. Additional legislation is being considered regarding liability.

CIO: Richard C. Webb, Asst. Secretary for Information Technology/CIO, Information Technology Services, Dept. of Commerce, 3700 Wake Forest Rd., Raleigh, NC 27609–6860, Phone: 919–981–2680 Fax: 919–981–5043 rwebb@sips.state.nc.us

Contact: Debra C. Jones, Statewide Y2K Program Director, Year 2000 Project Office, 3900 Wake Forest Road, Raleigh, NC 27609, Phone: 919–981–5528 Fax: 919–981–5374 dcjones@sips.state.nc.us;MOKeefe@sips.osc.state.nc.us

NORTH DAKOTA (Last updated 9/25/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
66	82%	$1.0M	No.	None.

CIO: Jim Heck, Director, Information Services Division, 600 East Boulevard Ave., Bismarck, ND 58505–0100, Phone: 701–328–3190 Fax: 701–328–3000 heck@pioneer.state.nd.us

Contact: Larry Lee, Contingency Planning Specialist, Information Services Division, 600 East Boulevard, Bismarck, ND 58505–0100, Phone: 701–328–2721 Fax: 701–328–3000 msmail.II12@ranch.state.nd.us

OHIO (Last updated 10/1/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
These have been determined and tracked by the individual agencies. We're in the process of gathering data and logging it into a central database. As of this date, 200 critical systems have been identified to this central file.	32% have been converted and are in production.	Original estimate of total cost for Year 2000 remediation was about $61 million. As of this date, we do not see the need for additional funding.	No, so far only cursory discussion has been held on this subject.	None.

CIO: Sandra Drabik, Director, Dept. of Administrative Services, 30 E. Broad St., 40th Fl., Columbus, OH 43266–0401, Phone: 614–466–6511 Fax: 614–644–8151 dir—drabik@ohio.gov

Contact: Fred Dowdy, Year 2000 Administrator, Computer ServicesDivision, Dept. of Administrative Services, 1320 Arthur E. Adams Drive, Columbus, OH 43221–3595, Phone: 614–752–7456 Fax: 614–644–-2858 odn—dowdy@ohio.gov

OKLAHOMA (Last updated 7/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
No answer.	No answer.	No answer.	No answer.	None

CIO: William N. Shafer, Director, Information Services Division, Office of State Finance, 2209 N. Central, Oklahoma City, OK 73105, Phone: 405–521–2804 Fax: 405–522–3042 bill.shafer@oklaosf.state.ok.us

Contact: Jerry G. Stillwell, Data Processing Administrator, Office of State Finance, 2209 N. Central, Oklahoma City, OK 73105, Phone: 405–521–2844 Fax: 405–522–3042 jerry.stillwell@oklaosf.state.ok.us

OREGON (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
248 (By Aug 31, a statewide list of mission critical systems will be confirmed. This list will be monitored closely to assure State of Oregon Year 2000 compliance.	32.2% (July 1998 data identifies over 32% of these systems are completed)	$92.0M (State of Oregon agencies 1997 Statewide Year 2000 Assessment identified $102M. Agencies effective management lowered that amount to $92.0M, presented to the Oregon Legislature in January 1998.)	Yes, Agency responsibility, coordination of policies and promotion of qualified workforce; Executive Order for compliance; Considering, Immunity/Liability.	None.

CIO: Don Mazziotti, Chief Information Officer, Information Resources Mgmt. Division, Dept. of Administrative Services, 155 Cottage St., N.E., Salem, OR 97310-0315, Phone: 503–378–3161 Fax: 503–378–5200 Don.Mazziotti@state.or.us

Contact: Barbara Jensen, State Year 2000 Project Office, Information Resource Management Div., Dept. of Administrative Services, 155 Cottage St., NE, Salem, OR 97310–0310, Phone: 503–378–5458 Fax: 503–378–5200 Barbara.Jensen@state.or.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

PENNSYLVANIA (Last updated 9/28/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
27,446 programs or 469 MC applications.	99%	$24M (For mission critical only. The total estimated cost for all systems is $40M)	Considering.	HB2273, HB2406, SB1434 All legislative bills are pending.

CIO: Larry A. Olson, Deputy Secretary, OA/Office for Information Technology, Governor's Office for Administration, 209 Finance Building, Harrisburg, PA 17120, Phone: 717–787–5440 Fax: 717–787–4523 lolson@oa.state.pa.us

Contact: Charles F. Gerhards, Director, Commonwealth Technology Center, OA/Office for Information Technology, 1 Technology Park, Harrisburg, PA 17110, Phone: 717–772–8000 Fax: 717–772–8113 cgerhard@oa.state.pa.us

Contact: Larry A. Olson, Deputy Secretary, Office for Information Technology, Governor's Office of Administration, 209 Finance Building, Harrisburg, PA 17120, Phone: 717–787–5440 Fax: 717–787–4523 lolson@oa.state.pa.us

PUERTO RICO (Last updated 7/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
174 (Includes all critical systems reported by the agencies.)	9% (Includes all critical systems reported compliant and tested by agency.)	$12.0M (Amount only includes costs reported by agencies supported with documents.)	Yes, reporting mechanism (SR585 requires agencies to report progress on the critical systems Y2K compliance status and the related costs). See www.senado.gvmt.pr.us/)	None.

CIO: Jorge E. Aponte, CPA, Information Systems Director, Office of Budget & Management, P.O. Box 9023228, San Juan, PR 00902–3228, Phone: 787–725–8646 Fax: 787–724–1374 japonte@ogp.prstar.net

Contact: Francisco J. Colon, Associate Director, Office of Budget and Management, P.O. Box 9023228, San Juan, PR 00902–3228, Phone: 787–725–9420 Fax: 787–721–8239 fcolon@ogp.prstar.net

RHODE ISLAND (Last updated 7/16/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
n/a	The major core systems are in the process of remediation and implementation. Many depts. are still in the remediation process, other depts. need to upgrade the versions of software and hardware for smaller systems.	Less than $10.0M (This year's FY99 budget contains $2.5M on top of $.5M allocated for the Y2K effort in FY98.)	No.	None.

CIO: Barbara Weaver, Chief Information Officer, Office of Library & Information Services, Dept. of Administration, One Capitol Hill, 4th Fl., Providence, RI 02908, Phone: 401–222–2222 Fax: 401–222–4260 barbwr@lori.state.ri.us

Contact: Sally J. Spadaro, Year 2000 Coordinator, Office of Library & Information Services, Dept. of Administration, One Capitol Hill, Providence, RI 02908, Phone: 401–222–1229 Fax: 401–222–2083 sally—spadaro@doa.state.ri.us

SOUTH CAROLINA (Last updated 9/29/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
440—this total is the number of NON-COMPLIANT mission critical systems.	42%—percentage of ALL SYSTEMS WHICH ARE COMPLIANT. Mission critical are included.	$31.2 million	No.	Currently focusing on total mission critical systems. Next report will contain this information.

CIO: Ted Lightle, Director, Office of Information Resource, Dept. of Budget & Control Board, 1201 Main St., Ste. 1500, Columbia, SC 29201, Phone: 803–737–0075 Fax: 803–737–0069 lightle@oir.state.sc.us

Contact: William T. Majors, Assistant Deputy Director, Office of Information Resources, Information Systems Opereration, 300 Gervais St., Columbia, SC 29201, Phone: 803–737–8242 Fax: 803–737–9507 fmajors@fds.state.sc.us

SOUTH DAKOTA (Last updated 9/8/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
205	Certified: 15% mainframe, 4% PC/LAN, 31% network components remediated: 38% mainframe, 22% PC/LAN, 57% network components.	$3.7M (This does not include costs for judicial and higher education systems.)	Considering.	None.

CIO: Otto Doll, Commissioner, Dept. of Administration, Bureau of Info. & Telecommmunications, 700 Governors Dr., Kneip Bldg., Pierre, SD 57501, Phone: 605–773–4165 Fax: 605–773–6040 ottod@is.state.sd.us

Contact: Jan Newman, Year 2000 Project Coordinator, Office of the Commissioner, Bureau of Information and Telecommunications, 1017 18th St. NE, Watertown, SD 57201, Phone: 605–882–5118 Fax: 605–886–8872 jann@is.state.sd.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

TENNESSEE (Last updated 9/14/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
148 (We are tracking 233 systems of which 148 are classified as mission critical.)	56% (Mission critical systems are at 51 percent completion. We are 82 percent complete based on man hour effort for all applications; remaining applications are scheduled for 12/31/1998 completion date.	$15.5M (estimate for total Y2K effort).	Yes, funding (The Appropriation Bill for 1997–1998 provided $6M and the Appropriation Bill for 1998/1999 provided an additional $4M for a total of $10M.).	None.

CIO: Bradley Dugger, Chief of Information Systems, Office of Information Resources, Dept. of Finance & Administration, 318 8th Ave., N., 11th Fl. TN Tower, Nashville, TN 37243–0288, Phone: 615–741–2569 Fax: 615–532–0471 bdugger@mail.state.tn.us

Contact: Ray Selvage, Information Systems Manager, Office for Information Resources, Dept. of Finance & Administration, 312 8th Ave. N. 10th Fl., TN Tower, 312 8th Avenue North, Nashville, TN 37243–0288, Phone: 615–741–7354 Fax: 615–741–4589 rselvage@mail.state.tn.us

TEXAS (Last updated 7/17/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
437 (The Texas Year 2000 Project Office does not manage any of these systems-we only provide oversight and monitoring. We have approximately 19 priority agencies who are responsible for managing the remediation efforts of these 437 systems.)	0% (At this time, there are no critical systems that have been through testing. 100 percent of these systems have been assessed, and most are in the remediation phase.)	$170.0M (This is the cost to remediate ALL systems in priority agencies—those with mission-critical systems. We do not have figures on remediation costs specifically for those 437 systems.)	Considering.	None.

CIO: Carolyn T. Purcell, Executive Director, Dept. of Information Resources, 300 W. 15th St., Ste. 1300, Austin, TX 78701, Phone: 512–475–4720 Fax: 512–475–4759 carolyn.purcell@dir.state.tx.us

Contact: Shannon Porterfield, Year 2000 Coordinator, Dept. of Information Resources, P.O. Box 13564, 300 W. 15th St., Ste.1300, Austin, TX 78711–3564, Phone: 512–475–4740 Fax: 512–475–4759 shannon.porterfield@dir.state.tx.us

UTAH (Last updated 9/18/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
532 (It is very difficult to define critical. We have a subset that we have called highly mission critical/must not fail systems that is only about 30 systems.)	51%	$50.0M ($12.0M has been directly appropriated for additional Y2K expense in addition to IT base budgets, a majority of which is being used for Y2K.)	Considering, Government immunity.	None.

CIO: David Moon, Chief Information Officer, Governor's Office, 210 State Capitol, Salt Lake City, UT 84114, Phone: 801–538–1524 Fax: 801–538–1557 dmoon@gov.state.ut.us

Contact: David Fletcher, Deputy Director, Dept. of Administrative Services, 3120 State Office Bldg., Salt Lake City, UT 84114, Phone: 801–538–3010 Fax: 801–538–3844 dfletche@state.ut.us

VERMONT (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)n/a	Has Year 2000 legislation been passed or proposed in your state?	Comments
50	50–60%		No.	None.

CIO: Patricia A. Urban, Chief Information Officer, 109 State St., Montpelier, VT, 05609–0210, Phone: 802–828–3322 Fax: 802–828–3320 purban@cio.state.vt.us

Contact: Patricia A. Urban, Chief Information Officer, State of Vermont, Administration / CIO, 109 State St., Montpelier, VT 05609–0210, Phone: 802–828–5846 Fax: 802–828–3398 purban@cio.state.vt.us

VIRGINIA (Last updated 7/21/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
*	51% (Completed all four phases of remediation)	$80–83M	Yes, Immunity, liability and establishing Century Date Change Initiative Project Office and its oversight	* We require agencies report on their Priority Business Activities. Within this framework, we track progress and cost based on 5 reporting categories and their potential impact on a priority business activity.

CIO: Donald W. Upson, Secretary of Technology, Office of Technology, 9th Street Office Bldg., Ste. 503, Richmond, VA 23219, Phone: 804–786–9579 Fax: 804–786–9584 now@state.va.us

Contact: Bette H. Dillehay, Director, Century Date Change Initiative, Council on Information Management, Project Office, Washington Bldg., Ste. 901, 1100 Bank St., Richmond, VA 23219, Phone: 804–786–8163 Fax: 804–371–7952 bdillehay@cim.state.va.us

SURVEY ON YEAR 2000 REMEDIATION IN THE STATES—Continued

[A survice of NASIRE: Representing chief information officers of the States]

WASHINGTON (Last updated 9/16/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
458	50%	$83.5M	Yes, Liability (failed in last session, SB6718-Year 2000 liability of state and local governments)	None.

CIO: Steve E. Kolodney, Director, Dept. of Information Services, 1110 Jefferson St., SE, P.O. Box 42445, Olympia, WA, 98504–2445, Phone: 360–902–3500 Fax: 360–664–0733 stevek@dis.wa.gov

Contact: Steve E. Kolodney, Director, Dept. of Information Services, 1110 Jefferson St., SE, P.O. Box 42445, Olympia, WA 98504–2445, Phone: 360–902–3500 Fax: 360–664–0733 stevek@dis.wa.gov

Contact: John O. Saunders, Manager, Year 2000 Program Office, Dept. of Information Services, 1110 Jefferson St., SE, P.O. Box 42445, Olympia, WA 98504, Phone: 360–902–3526 Fax: 360–586–8992, saunders@dis.wa.gov

WEST VIRGINIA (Last updated 9/11/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
59—critical applications identified, as of 9/9/98—31 are compliant.	80% of all software that IS&C is responsible for has been completed. No data is available for software remediation contracted for by other state agencies.	Not Available. Higher education is included in the monitoring but cost not available.	None.	IS&C will complete its remediation by June 30, 1998. All other agencies will complete contracted work by December 31, 1998, with the exception of four critical systems. These four will be completed on or before June 30, 1999.

CIO: Samuel M. Tully, Ph.D., Spec. Asst. to the Gov't & CTO, Governor's Office of Technology, 505 Capitol Street, Ste. 200, Charleston, WV 25305, Phone: 304–558–3784 Fax: 304–558–0136 stully@governor.com

Contact: N. Michael Slater, Director, IS&C, Dept. of Administration—ISC, Bldg. 6, Rm. B110, 1900 Kahawha Blvd. E., Charleston, WV, 25305, Phone: 304–558–5311 Fax: 304–558–4867 mslater@gwmail.state.wv.us

WISCONSIN (Last updated 7/22/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
21 (The 43 state agencies in Wisconsin state government manage 102 critical applications, per our own definition—see www.state.wi.us/y2k/critapps.htm for the definition. The identification of critical was based on an agency perspective.	n/a	$35M	Considering liability.	None.

CIO: Bruce Reines, Director, Bureau of Technology Policy & Planning, Dept. of Administration, 101 E. Wilson, 8th Floor, P.O. Box 7844, Madison, WI 53707–7844, Phone: 608–266–8878 Fax: 608–266–2164 reinewb@mail.state.wi.us

Contact: Bill Braham, Information Technology Coordinator, Technology Management, Dept. of Administration, 101 E. Wilson 8th Floor, P.O. Box 7844, Madison, WI 53707–7844, Phone: 608–266–0625 Fax: 608–266–2164 brahab@mail.state.wi.us

WYOMING (Last updated 9/25/1998.)

How many critical systems do you manage? [1]	What percent of these critical systems are converted? [2]	How much do you estimate it will cost? (in millions)	Has Year 2000 legislation been passed or proposed in your state?	Comments
26 (17 are managed by the Division of ITD and 9 are managed by the respective agencies	30%	(Not including higher education) WY has spent to date $10.5+ million with another $4.7 million obligated. We are also in the middle of an inventory and assessment validation contract ($1.35 million) that will give us the numbers of what we have to do to complete our Y2K remediation.	Legislation is being considered, but noting formal is available at this time.	ITD will be meeting with the Joint Appropriation Committee on July 27 to discuss our situation.

CIO: Larry Stolz, Chief Information Officer, Info. Planning & Coordination Division, Dept. of Administration & Information, Emerson Bldg., Rm. 214, 2001 Capitol Ave., Cheyenne, WY 82002, Phone: 307–777–6410 Fax: 307–777–3696 lstolz@missc.state.wy.us

Contact: A. Evonne Rogers, Year 2000 Project Leader, Information Technology Division, Dept. of Administration, 2001 Capitol Avenue, Rm. 237, Cheyenne, WY 82002, Phone: 307–777–5072 Fax: 307–777–6725 eroger@missc.state.wy.us

[1] "Critical systems" would be defined as systems which effect public safety, public health, and financial and personnel aspects of government services.

[2] "Converted" would be defined as complete assessment, remediation, and testing.

Note: Survey results reflect "best guess" estimates on behalf of the states and is as current as the dates listed in the column "Date Last Updated." They are intended as a reference point for NASIRE members and should not be reproduced without permission of NASIRE. Please contact individual state Y2K Coordinators or CIOs for confirmation or updates of survey results.

RESPONSES OF JOHN THOMAS FLYNN TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. NASIRE, as representative of 50 state CIO's, has a perspective on Y2K problems that is unique. Would you please tell the Committee the three to five functional areas where state governments are having the most difficulty in Y2K remediation?

Answer.

1. The number of legacy information technology systems is high and many of them are quite old, making it more difficult to find resources with the required knowledge to effect the needed remediation.
2. The proliferation of desktop systems has resulted in an almost endless variety of software which runs on those desktop systems, all of which must be assessed to ensure that they are Y2K compliant and replaced where they are not. The costs are expected to be considerable.
3. Legislative and federal mandates continue to require resources and effort by the same staff that is heavily involved in the Y2K remediation effort.
4. Ensuring that all of the interrelationships between systems, both at the state level and with other external entities, are identified and addressed.
5. What we don't know.

Question 2. The 50 states house the 3,800 counties where all the 265 million Americans live.

a. Is there any relationship between state and county governments in the Y2K remediation process?

Answer. Yes, there is. As an example, in the state of California, there is an intergovernmental task force chaired by the state CIO and includes some County CIO's and/or their representatives.

b. What are the critical Y2K interfaces and interconnections between state and county governments that potentially could have serious impact on the public?

Answer.

1. Emergency response
2. Law enforcement
3. Health and welfare
4. Revenue
5. Transportation

Question 3. Has NASIRE made any arrangements to share technical resources between states after the Y2K date if emergencies occur?

Answer. No.

Question 4. The Gartner Group presentation seems to rate the State Y2K efforts less complete than the NASIRE data. Would you comment on the level of accuracy on the NASIRE self-reporting online survey?

Answer. There is no universally accepted national standard for reporting on the Y2K remediation effort. I do not know the source of the Gartner statistics. The NASIRE survey represents each individual state's assessment of its Y2K effort based on its own standards, and was updated immediately prior to my appearance before the Committee. However, as you have noted in your question, self-reporting is not validated.

Question 5. Mr. Flynn you made some very telling points in your testimony concerning responses to emergency situations like hurricanes and power outages that were single events. What do you think will happen nationally where multiple information technology breakdowns within and between states may occur?

Answer. This is why all of the states and their departments need to address business continuity planning for all high impact scenarios as soon as possible. The business continuity planning must also include global scenarios addressing potential problems, not just within a state but across the nation. In California, our departments are beginning to address business continuity planning now. As with other states, we are putting a lot of effort into determining with whom we interface and how we interact with entities outside of the state departments, whether that be local governments, the Federal government, the private sector or other states.

Question 6. The results of the Gartner Group survey which Senator Bennett presented today paints a much bleaker picture of overall preparedness than does the NASIRE survey which you provided us with today. Would you comment on why there might be discrepancies between these two surveys? Do you feel that this is a good example of why independent verification of an organization's Y2K status is important?

Answer. As noted above, there is no universally accepted national standard for reporting on the Y2K remediation effort. Even within individual states, it has been difficult to reach consensus on what constitutes a "system," what "mission critical" means (what is mission critical to one department may not be mission critical to the state as a whole), and what are the completion criteria which indicate compliance. Independent verification of an organization's Y2K status would be more useful if there is universal agreement on the metrics to be used to measure the status of the Y2K remediation effort.

Question 7. Surveys such as that which NASIRE performed are very important in assessing how sectors such as state government are preparing for Y2K. However, we are concerned that surveys that are not carefully controlled and result in a rosier assessment than is justified might do more harm than good and can lead to a sense of complacency. When we look at the actual data reported, we find wide variations, such as New Mexico which reports over 4400 critical systems, and New Jersey which reports only 195. Our question for you is, in general, what steps has NASIRE taken to validate the data?

Answer. NASIRE does not have the resources available to validate data from individual states. NASIRE has made the assumption that the individual states have established their own standards for assessing and reporting the progress of their agencies and departments to their Legislatures and administration. Since there is no national standard, we have to rely on the standards set by the individual states.

PREPARED STATEMENT OF ELLEN GORDON

Mr. Chairman and members of the committee: On behalf of the National Emergency Management Association, I would like to thank you for the opportunity to appear before you today to discuss the Year 2000 technology issue as it relates to emergency preparedness, response and recovery throughout the country. NEMA represents the state directors of emergency management in all the states and territories who are responsible to their governors for protecting life and property from disasters and emergencies.

State Emergency Managers are aware of Y2K issues and the possibility that they may be called upon to respond to the consequences of a Y2K technology failure or disruption. NEMA recently conducted a survey of state emergency management agencies to determine overall awareness of the Y2K issue and this is what we learned:

—All states have Y2K program for state agencies. State Y2K programs differ in organization and implementation strategies.

—All state emergency managers indicate their emergency operations centers are or will be compliant by Year 2000.

—All states are confident that their emergency management systems that are owned and operated by the state will be Y2K complaint.

—At this time, most states cannot assure that emergency management systems being utilized by local governments will be Y2K compliant.

NEMA has determined that the resolution of the Y2K problem in emergency management systems, especially at local government levels, needs focused leadership. NEMA has seen reports indicating that up to fifty percent of local governments do not believe they have a Y2K problem; therefore, it cannot be determined that all levels of government emergency management systems such as 911, communication systems, alarms, sensors, or other equipment will continue to function properly after Year 2000. Embedded systems may lead to failures in electrical transmission, water and sewer systems, medical devices and telecommunications. Each of these is critical to public health and safety.

As all disasters typically involve local emergency management agencies first, NEMA believes that it is important to determine the impact of Y2K on local emergency management systems which could produce deficiencies in providing for the public health and safety. As President of NEMA, I am in the process of urging all state emergency management directors to provide information and assistance, as appropriate, to their local emergency management agencies. It is imperative that capabilities be in place and ready to respond to the consequences of a potential Y2K technology disruption.

As we determine significant problems in emergency management systems, I intend to immediately advise the Director of FEMA of any major shortfall in local government emergency management systems and seek assistance to preclude adverse impact on the public. Hopefully, the partnership of NEMA and FEMA can help local governments avoid significant adverse consequences of the Y2K dilemma.

Role of state emergency management in Y2K

Local government has the front line of authority and responsibility for events or emergencies. If the emergency overwhelms local resources or capabilities, the State provides assistance and resources as determined in the State Emergency Operations Plan. The role of state emergency management is to coordinate and provide assistance as required during a disaster or emergency regardless of whether the disaster is a hurricane, tornado, civil riot or a Y2K related major disaster. These responsibilities are common to every state's emergency operations plan. Most state agencies have disaster preparedness plans that include all-hazards preparedness, response arid recovery procedures. All State and local government emergency management agencies have emergency management infrastructures in place to coordinate their agency's role in disaster response and recovery.

NEMA anticipates the Y2K problem will be dealt with much the same as any other disaster—through an integrated and coordinated emergency response system that I just described. The resources and types of people needed may differ for a Y2K event, but the emergency response system remains the same.

Interstate mutual aid

NEMA administers the national Emergency Management Assistance Compact (EMAC), a system for interstate resources to supplement federal disaster assistance when merited or replace federal assistance when it is not. The goal of the EMAC is to provide rapid assistance using the closest available resources. As an interstate mutual aid agreement, the EMAC establishes the legal mechanism and operational procedures to facilitate rapid disaster response using the unique resources possessed by member states in the form of personnel, equipment and materials.

Currently, twenty-two states and one territory are signatories to the compact. Several more states are planning to introduce the compact into their state legislatures in 1999. EMAC has been tested extensively this year during the Florida wildfires and Hurricane Bonnie. As we speak, a number of EMAC member states are providing assistance to the Gulf Coast states impacted by Hurricane Georges. These recent activations have proven that EMAC works. It is an efficient and effective system for states to help each other during disasters.

Interstate mutual aid through compacts like EMAC, may prove extremely beneficial should the infrastructure fail in a Y2K scenario, particularly if only a few areas within a state or a region are impacted. However, should all states be impacted in a significant manner, mutual aid between states may not be possible. Individual states will not be able to spare limited personnel or resources outside state boundaries.

Federal assistance to state and local governments

Should state resources and capabilities be overwhelmed by Y2K problems, states would look to the Federal government for assistance. At this time, state emergency management agencies through NEMA are working with FEMA and other Federal agencies with responsibilities in the Federal Response Plan as to the procedures needed in responding to a multi-state event due to Y2K technological failures or disruptions.

In summary, NEMA, with the support of its member states and territories and in partnership with FEMA, is working to ensure state emergency management systems are Y2K compliant. I am also pleased to report that many state emergency management agencies already have plans to activate their emergency operations centers on December 31, 1999. Many are also planning to "run up the clock" on their systems prior to December to test the systems. Y2K preparedness activities are in addition and complementary to our mission of coordinating and facilitating resources to minimize the impact of disasters and emergencies on people, property, the economy and the environment.

The most immediate need is for states to work with their local governments to identify potential system failures and develop contingency plans to manage the consequences of those failures. In addition, the states need more information and guidance from the Federal government as to what assistance will be available to state and local governments in a Y2K "disaster," particularly if it becomes a multi-state event.

Thank you again for inviting NEMA to provide testimony before you today on this important issue. I would be happy to answer any questions you may have at this time.

RESPONSES OF ELLEN GORDON TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question. What are your expectations regarding the Federal Government's role in assisting states in responding to Y2K disruptions?

Answer. NEMA suggests that FEMA and other federal agencies support states through the same mechanisms as in any other emergency situation, whether man-made events or natural disasters. If state and local emergency management capabilities are insufficient to manage the consequences of Y2K-related disruptions, states will request assistance through the Stafford Act.

In addition, NEMA recommends that FEMA and other relevant federal agencies begin identifying high-risk areas and potential threats related to the Y2K problem. These agencies should then share this information through their outreach efforts with states. Such information is important because states and localities may be unaware of non-compliant facilities within their jurisdictions.

Question. As you interpret it, how do potential Y2K disruptions fit within the scope of the Stafford Act's definitions of "disaster" and "emergency?"

Answer. Disruptions resulting from the Y2K problem may qualify as emergencies and disasters as defined by the Stafford Act. The Y2K problem has the potential for significantly impacting public health and safety and therefore may require state assistance. If the negative consequences of the Y2K problem exceed both state and local resources, the Stafford Act authorizes the governor to request federal assistance. Whether Y2K-related disruptions are considered "emergencies" or "disasters" will depend upon the magnitude of each situation.

Question. What impediments do you see in terms of the federal government's ability to respond to Year 2000 related disruptions or emergencies?

Answer. Federal agencies in the Federal Response Plan that are not compliant will be impediments to the effective response to any Y2K-related emergencies. In addition, it is essential that all requests for federal assistance be processed in a timely and efficient manner.

Question. What recommendations do you have for FEMA regarding steps that the agency can take prior to the Year 2000 in preparing itself to respond to requests for assistance from states or localities suffering from Year 2000 problems?

Answer. FEMA should work to ensure that all federal agencies in the Federal Response Plan are Y2K compliant and prepared for any potential consequences which may occur. FEMA should also partner with states to identify high-risk areas and potential threats within their jurisdictions and to develop fail-safe plans in the event any critical infrastructure fails.

Question. What would you consider to be the "threshold" beyond which we might expect that a state would request assistance from the Federal government in response to Year 2000 problems?

Answer. The "threshold" for requesting assistance for Y2K-related emergencies should be the same as any other type of emergency as defined by the Stafford Act. If state and local emergency management capabilities are insufficient to respond to the consequences of the Y2K problem, governors can then ask the President to issue a federal disaster declaration.

Question. Describe the efforts being made by state emergency managers to assess the state of readiness of the emergency management systems at the county and local level?

Answer. Overall, state emergency management directors have begun working closely with local coordinators to improve awareness of the Y2K problem, ensure that critical emergency response systems are compliant, and assess the threat to local public health and safety. States have been asked to survey local coordinators as part of FEMA's and NEMA's efforts to increase awareness in the emergency management and response community.

Question. As a state emergency manager, what role do you envision for the National Guard in the event of Y2K disruptions?

Answer. As with any other state emergency, NEMA strongly recommends that the National Guard remain state assets. The National Guard should be at the governors' disposal should any Y2K-related emergencies occur.

Question. It was very interesting to hear of the results of the NEMA survey of state emergency managers. It is reassuring to hear that all 50 Emergency Operations Centers will be Y2K compliant in time. Can you tell me how confident you are with these results? Will NEMA take any steps to independently verify these results?

Answer. The survey results represent the opinions of state emergency management directors and their staffs on whether their own critical systems will be compliant. It is NEMA's understanding that all states now have programs tasked with ensuring that state agencies are Y2K compliant. NEMA has asked the states to survey

their local counterparts as part of FEMA's assessment efforts. The results of this assessment should be available in November 1998.

Question. You mentioned that Y2K emergencies will be like other emergencies, but that different resources and types of people will be needed to respond. When is it likely that you will know what those resources and skills are so that you can take steps to assure you will have them in an emergency situation?

Answer. State emergency management agencies across the nation are active partners in interagency Y2K councils and task forces. This partnering and communication throughout state government provides an excellent forum to identify resources and types of personnel needed to address this problem.

Question. You rightly point out that EMAC may fail for a large scale problem like a Y2K outage since each participant in the compact may be reluctant to share limited resources since they might be uncertain of what their own state's needs might be. Does this mean that everyone will then be seeking federal assistance?

Answer. Whether there will be a significant demand for federal resources will depend upon the impact of Y2K disruptions and the ability of state and local authorities to respond. If states experience only minor disruptions, there will only be a few requests and EMAC assistance may be adequate. If states experience major emergencies, EMAC assistance will probably be inadequate or unavailable. In this case, the federal government will be a key response organization since state, local and private resources will probably be exhausted.

Question. You mentioned that many state emergency management agencies already have plans to have their Emergency Operations Centers up and running on December 31, 1999. Can you tell us how many plan to do this, and which states they are.

Answer. Because EOC's are usually operational only during confirmed emergencies, the decision to activate them will depend upon each state's own risk assessment and level of preparedness. At least ten states have reported plans to activate their EOC's prior to January 1, 2000, including Delaware, Florida, Idaho, Indiana, Iowa, Maine, Maryland, New Hampshire, Washington, and Wisconsin. Other states are conducting risk assessments to determine whether full EOC activation will be necessary.

PREPARED STATEMENT OF JOHN A. KOSKINEN

Good morning, Mr. Chairman. I am pleased to appear again before the committee to discuss the role of the President's Council on Year 2000 Conversion in the development of contingency plans and appropriate emergency responses to any difficulties that may arise as we make the transition to the year 2000 (Y2K).

Before I discuss this issue, let me express the Administration's appreciation for the strong support this Committee has provided in the development and passage of the "Year 2000 Information and Readiness Disclosure Act." In particular, the assistance you, Mr. Chairman, Senator Dodd and Senator Kyl have provided has been an indispensable part of the success we have achieved. As the President has said, this bipartisan legislation provides us with an important opportunity to help our Nation prepare its computer systems for the new century.

I would also note that this Committee has made a major contribution in promoting awareness of, and action on, the Y2K problem with hearings that have examined public and private sector progress in important economic sectors that range from electric power to transportation to telecommunications. While all of us need to continue to support the efforts of Federal agencies to prepare their systems—and several Federal agencies still face significant challenges in preparing their mission-critical systems for the year 2000—the real risk of major disruptions comes from possible failures outside the Government, particularly among small and medium-sized organizations in both the public and private sectors.

Even with the best efforts of all of us, we need to understand and expect that not every system and embedded chip will be found and fixed. To minimize disruptions caused by these failures, businesses and government agencies must focus on contingency planning in addition to their remediation efforts.

FEDERAL AGENCY ACTIVITIES

Federal agencies are developing continuity of business plans for their core business functions. OMB, in its quarterly progress reports, has asked the agencies to report on their progress in this area, and is looking closely at their planning activities as it develops the President's fiscal year 2000 budget. OMB is also engaged in preliminary reviews of possible emergency expenditures should Congress provide such funding. OMB has encouraged agencies to review the recent GAO guidance on

contingency planning along with the plan developed by the Federal Government's leader in addressing the year 2000 problem, the Social Security Administration. Agencies with the greatest year 2000 challenges are the ones most in need of business continuity plans.

PROMOTING AWARENESS OF CONTINGENCY PLANNING

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?

Federal agencies have had to confront the second type of contingency planning in their relationships with the States. In many cases, States help to carry out important Federal programs such as Medicaid and unemployment insurance. These programs depend upon Federal-State data exchange points, and Federal agencies have been working with their State counterparts to ensure that these exchange points are compliant. But even if the data exchange points are ready for the year 2000, service delivery could still be jeopardized if the State systems behind the data exchanges fail. Federal agencies like the Labor Department, for the unemployment insurance program, are now working with the States to ensure that backup plans are ready to support continued service delivery should State systems, or other non-Federal systems, fail.

HELPING TO UNDERSTAND WHAT IS LIKELY TO HAPPEN

One of the Council'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. This information will be important to organizations as they develop and refine their contingency plans. For example, everyone is concerned about having electric power. But that doesn't mean that they should all immediately buy their own generators without having a better sense of where outages are possible and what their likely duration will be.

The Council has established cooperative working relationships with umbrella groups in electric power and other important sectors. The focus has initially been on increasing awareness and the level of activity by those operating in each sector. We are also, however, developing assessment processes whereby the umbrella groups will be surveying their members on a regular basis to determine their state of readiness. Summary reports will then be provided to the Council and the public. Good examples of this process can be seen with the reports the Council received recently from the Electric Power and Oil and Gas Working Groups. These assessments provide us, and the public, valuable information about the status of these important industries. Over time, such information will allow everyone to adjust their contingency plans appropriately.

I might note that the "Year 2000 Information and Readiness Disclosure Act" will increase our ability to obtain assessments since it provides protection to the information provided by individual companies to their umbrella groups, thereby increasing the likelihood of candid responses.

FEDERAL EMERGENCY RESPONSE MECHANISMS

As you know, the Federal Government, in coordination with State and local governments, plays a key role in responding to disasters and other emergencies and is looked to for leadership at those times. I will let Mr. Suiter of FEMA describe in more detail the Federal Government's role, but I would point out that the year 2000 problem provides a unique emergency response challenge.

With most major emergencies, such as hurricanes or blizzards, authorities are dealing with one localized problem in a town, county, State, or region. With the Y2K problem, however, it is possible that emergency response systems could face multiple system failures occurring at roughly the same time in different places. For example, in a worst case scenario for a city or town, authorities could face the failure of the power plant, the water treatment plant, and transit systems. And such problems could occur in many different towns, cities, or regions at the same time. While

no one of them alone may be a major problem, simultaneous failures will test the capacity of our emergency response systems, and I am pleased that FEMA has agreed to chair the Council's Emergency Services Working Group.

The Federal Government has separate response systems related to specific types of emergencies. Internationally, we have an apparatus for responding to emergencies such as famine and refugee assistance as well as military threats. Domestically, we have the systems and relationships that FEMA will discuss with you. We are presently reviewing our inventory of emergency response mechanisms and authorities to ensure that there is no confusion across organizational lines on January 1, 2000 and that we can handle the possibility of multiple requests for the same resources.

In addition to FEMA, which has the lead on domestic emergency issues, the Council is working with the National Security Council, the Departments of State, Defense, and Justice, and others who are responsible for challenges we may face internationally to coordinate Federal emergency response efforts. In particular, we are beginning to look at scenarios that may involve disruptions in key foreign countries as well as difficulties at home so that we can map out plans for appropriate Federal action. In foreign countries, we are concerned about how Y2K-related disruptions may affect our embassies, American citizens living abroad, and American businesses. At home, we anticipate that the multiple burdens placed upon State and local disaster authorities may result in an increased demand for Federal help.

The American people have confidence in our ability to respond in the wake of natural disasters. As we have seen with the recent hurricanes in the Carolinas and the Gulf Region, many are reluctant to leave their homes, not only because they want to protect their property, but because they are confident that emergency response authorities can maintain order and provide key services no matter what the situation. Our objective is to ensure that the American people have the same level of confidence in the Federal Government's ability, and that of their State and local officials as well, to respond to any year 2000-related disruptions.

MONITORING THE TRANSITION TO THE YEAR 2000

We all want to ensure a smooth transition to the year 2000. For most organizations, including Federal agencies, the primary year 2000 focus up to this point has been on fixing or replacing non-compliant systems and embedded chips. But as we enter 1999, that will change.

The Council is committed to encouraging businesses and helping Government agencies to prepare for likely problems and to develop viable contingency plans. We have to expect some problems on January 1, 2000. If we share information and plans, however, we can generate public confidence in our preparedness and minimize the impact of those problems on everyone.

RESPONSES OF JOHN A. KOSKINEN TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Mr. Koskinen, everything you say in your statement is true regarding what we need to do and the urgency of getting it done. However, I must say I am disappointed by the total lack of specifics in your testimony. We are now less than 15 months, or 5 fiscal quarters, from midnight, December 31, 1999. The country needs a clear action plan with leadership from the executive branch to deal with this problem.

By the end of today, this committee will have heard from 70 witnesses. Repeatedly, when questioned about the status of contingency plans, the response we heard was, "It's very difficult to plan while so much is unknown. We need better information." In addition, if the witness was from a Federal agency, we frequently were told that they were waiting for guidance from the President's Council. Can you tell us when we will see sector assessments from the President Council? Can you tell us what is taking so long? What is it going to take to accelerate the release of these assessments?

Answer. The Council's working groups continue to work with their industry partners to gather information for assessments on the status of year 2000 efforts in key economic sectors. As noted in my testimony, we have recently received initial industry assessments for two critical areas—electric power and oil and gas. These assessments are available to the public and will be updated regularly.

Our goal is to have initial assessments for the other key economic sectors, which we will also make available to the public, before the end of this year. Once completed, these assessments will have provided us a process that we can replicate to update them throughout 1999.

The time frame for these initial assessments is dictated largely by where industries are in the process of remediating their systems. Much like the Federal Government, most private sector entities will not have completed their testing work until the end of this year or the beginning of 1999. That information—where industries are after they have completed the bulk of their testing—is what will be most valuable in determining where disruptions are most likely to occur and what contingency plans are most appropriate.

The Council is committed to continue to work with umbrella groups and industry associations to do whatever it can to expedite their information gathering. We have constructed a standard assessment template for use in information gathering and are hopeful that the recently enacted "Year 2000 Information and Readiness Disclosure Act" will encourage companies to be more willing to answer queries about their progress.

Question 2. Mr. Koskinen, have you provided any target dates for the completion of the remaining assessments? Do you anticipate that the assessments will become specific as time moves on and offer more insight to where we might experience regional problems? I have told the Council's working group chairs that the target date for the completion of initial assessments is December 11, 1998. Those that cannot meet that time table will advise us when the first assessments provided by the private sector umbrella groups and industry associations will be available.

Answer. As we move through 1999, assessments will undoubtably become more refined, with information on where in the country industries foresee the greatest likelihood for disruptions. The Council is also committed to maintaining a dialogue with State and local officials on the potential for regional disruptions in the public sector services which continue to concern us greatly.

Question 3. FEMA contends that without assessments they cannot begin Y2K emergency preparedness planning. When do you think FEMA can expect to have these so they may begin their planning efforts? How would you advise FEMA to plan in the absence of such assessments?

Answer. As was the case for the electric power and oil and gas sectors, FEMA will have assessment information as soon as the Council does. But as Mr. Suiter testified, while FEMA would like to have the most detailed information on the status of year 2000 efforts in key sectors as soon as it is available, there are things that it can do, and is doing, to prepare for the possibility of emergencies created by the year 2000 problem.

FEMA has met with the Federal agencies that play key roles in emergency response and has been working to ensure that those agencies will not have difficulties in getting resources to where they need to be should emergency situations develop on January 1, 2000.

FEMA has also been communicating with State and local emergency response officials to make sure that systems at those levels will be ready for the year 2000. FEMA is beginning a series of regional meetings with local response agencies to prepare them for the unique aspects of possible year 2000 failures. FEMA plans to report in greater detail about the general preparedness of the country's emergency systems in the first quarter of next year.

Question 4. Under the Assignment of Emergency Preparedness Functions of Executive Order 12656, the Director of FEMA is tasked to act as an advisor to the National Security Council on issues of national security and emergency preparedness, including civil defense, continuity of government, and technological disasters. In most of our hearings we have viewed Y2K as a management problem, do you think Y2K would qualify as a technological disaster? Do you think the Director of FEMA and the NSC should be discussing Y2K and the possible implications it may hold for national security and emergency preparedness?

Answer. Until January 1, 2000, whether or not the Y2K problem will qualify as a technological disaster remains to be seen. However, recognizing the unique nature of the problem and the challenges it poses, we have coordinated meetings between FEMA, NSC and other Federal response agencies such as the State Department, and they have already begun to work together to review Y2K impacts on national security and emergency preparedness. Senior level officials from the NSC and FEMA now meet regularly to discuss how they can best coordinate their efforts over the next 14 months.

Question 5. Mr. Koskinen, you have expressed concern about the international sectors. Could you please tell us which portions of the world concern you the most?

Answer. Like businesses and other organizations, countries that are paying attention to the problem are of less concern than those that are not. Countries that are aware of the problem and are working on it are basically doing all we can ask of them. But those that are not paying attention, or think the problem doesn't apply to them, are the source of our greatest risk.

That being said, the countries of most concern are developing nations around the world, particularly in South and Central America, and Africa. We are also concerned, however, about countries whose more immediate economic challenges hamper their ability to devote appropriate attention to the Y2K problem, as is the case for many South Asian nations, Russia, and the Newly Independent States.

To help bring greater coordination to the work of countries around the world, we are arranging with the United Nations to organize a meeting of national year 2000 coordinators from around the world in New York City on December 11, 1998. But the magnitude of the global challenges should not be underestimated.

PREPARED STATEMENT OF SENATOR JON KYL

On Monday night, the Senate passed the Chairman's "Year 2000 Information Disclosure Act" (S. 2392) by unanimous consent, and around 5:30 p.m. yesterday evening the House passed S. 2392. I would like to thank our colleagues in the House for their strong support and fast passage of the bill. The rapid bi-partisan efforts to pass this legislation demonstrates how serious Congress is about the Year 2000 computer problem. I think it has become obvious to every member of this Committee that prospective Y2K failures present a very serious problem for the United States, and for other nations as well. Because of the potential adverse consequences for our nation's security, economic health, and public safety, we need to do everything we can to keep Y2K failures from happening. In every hearing of this Committee, the different industry sectors have all asked for help in sharing information.

Chairman Bennett asked me to look into this legal impediments to information sharing and to review S. 2392. At my direction, Senate Judiciary and Y2K Committee staff hosted a series of industry briefings over the summer on their information-sharing concerns, followed by negotiations among an ad hoc, bipartisan group of Congressional staff, industry, and Administration representatives. The result was a well crafted narrowly constructed piece of legislation which enables industry to exchange the Y2K information needed to prevent failures.

The purpose of the legislation is to ensure that concerns over liability do not have a chilling effect on sharing essential Y2K information. So, for example, if in good faith you provide information about what you have done to fix some Y2K glitch, you can't be sued just for providing that information if it later proves to be incomplete, confusing or misleading to someone else. Of course, if you deliberately lie, or are reckless in what you say, this bill won't protect you. It's also important to understand that this bill does not absolve anyone of responsibility for damages that may arise from Y2K failures.

Clearly, the Y2K problem has the potential to impact our nation's emergency response systems and operations which are heavily dependent upon information technology. The "Year 2000 Information Disclosure Act" will be critical in helping to prevent failure, improve readiness and promote contingency planning. However, despite the best efforts of industry and government to prepare for Y2K, there may be failures. The severity and length of time for these disruptions is not known. Indications are that Y2K will be more of an inconvenience that a catastrophe. However, we must push beyond complacency and carefully consider the contingency planning that may be necessary in the Year 2000.

Y2K contingency planing is unique, because of the uncertain reliability of the infrastructures we rely on in an emergency. Relying on old contingency plans is not enough. From a state and local perspective it is critical that law enforcement, firefighters and other first responders begin to think broadly about the reactions they may encounter in their communities because of the Y2K problem. For example, a coincidental failure of an ATM at a local bank could cause people to panic thinking that a Y2K problem has put their money is at risk.

My Subcommittee on Technology and Terrorism has been looking at emerging information warfare threats to our nation's critical infrastructures, such as telecommunications, power, and transportation, and what we need to do to protect them. Our inability to map the critical interconnections in our national information infrastructure (NII) demonstrates not only a weakness in our Y2K contingency planning efforts, but the need for a more reasoned security policy.

I would like to thank the chairman for this timely hearing. Preparation, and not panic, is the key to successfully meeting the challenges of Y2K. And hopefully, in the course of meeting these urgent Y2K challenges, we will gain insights into how to make America's critical infrastructures more robust and secure against other, more deliberate, threats.

PREPARED STATEMENT OF GOV. MICHAEL O. LEAVITT

Thank you Senator Bennett and members of the committee for the opportunity to testify about the state of Utah's progress in preparing for the Year 2000 technology problem and to provide you, on behalf of the National Governor's Association, an overview of the preparedness response from the vantage point of the states.

THE NGA STANDPOINT

Under the leadership of the governors, states are working to address the Y2K problem. Progress is varied. For some it is significant—advanced to the point where testing is already under way, including testing of law enforcement and emergency management systems. Other states lag behind.

There also are varied degrees of collaboration between state and local jurisdictions, which will be the front-line entities to deal with public safety and emergency management concerns under best and worst-case Y2K scenarios.

Most states are aware of the need to work cooperatively with local jurisdictions to ensure that critical systems will continue to function. At this point, the challenge is to make sure all governors and states reach out to local governments to raise the level of awareness about the scope and implications of the problem and provide assistance.

As vice chairman of the NGA, I would like to describe some of the steps the governor's association has taken to help states meet their Y2K responsibilities.

In July the NGA hosted a "Year 2000 State Summit" attended by senior-level policy aides and chief technology officers. Discussions centered on state, local and private-sector coordination and on a common agenda for the states to ensure public confidence in state systems and state-regulated industries.

Additionally, the NGA has published an issue brief titled "What Governors Need to Know About Y2K." It outlines the steps governors should take as chief executive officers, guarantors of public safety and public leaders. NGA also is working with representatives of groups representing other state and local elected officials to promote cooperation and communication among all levels of government.

The NGA welcomes the Senate's passage this week of the "Good Samaritan" legislation authored and sponsored by members of this committee. A significant number of large computer systems and embedded systems will experience Y2K-related failures. Greater information sharing by private and public entities would only help states prepare more effectively.

WHAT UTAH IS DOING

The state of Utah is moving forward. Our outlook is one of cautious optimism. We are not complacent. Nor are we panicked by the complexity of a problem with the potential to disrupt lives and with some ramifications beyond the state's control. In essence, we can program to cover problems that are known, but we must also plan for a myriad of possibilities that remain unknown.

In the realm of the known—compliance—our progress is measurable. Utah began its inoculation drive against the Millennium Bug more than two-and-a-half years ago. The first steps involved the testing, replacement, and reprogramming of more than 600 information technology systems.

At this time, more than 51 percent of those systems are fully compliant. The target date for all systems to be compliant is July 1999.

Under a previous decision unrelated to Y2K, the state of Utah developed an "alternate site" for its data center and mainframe computing resources to have backup in the case of an earthquake or major emergency. The alternate site is in Richfield, about 130 miles from Salt Lake City.

Half of the state's data center and mainframe resources are located there, and as of now, there also is a mainframe set up specifically for Y2K testing. The Y2K mainframe allows for full-scale tests of large systems, applications and databases as if they were running in the year 2000.

Utah's Y2K compliance efforts also include identifying the information technology systems that are mission critical—those pertaining to public health or safety, collection of revenues and disbursement of benefits to those in need. Those systems are receiving first priority in the coordination and deployment of resources.

The unknown component of Y2K falls in the area of contingency planning.

For Utah's Y2K efforts, contingency planning deals with two broad categories: (1) What the state will do if information technology systems are not remedied in time or they unexpectedly fail due to unforseen glitches; and (2) how we will maintain essential services in the event that critical infrastructure services are disrupted or cut off.

All state agencies have been directed to consider both aspects in their contingency planning and to have complete plans submitted by December 31, 1998. Every plan must delineate how services are to be delivered, including manual processes that might have to be employed.

The state has coordinated the purchase of a software package to help various agencies conduct detailed contingency planning. The agencies furthest along in that planning are also the agencies reporting the most work to be done with regard to planning. It is the same maxim that applies to the Y2K problem in general: The more you look, the more you find. And the more you find, the more it costs. Total costs for all Y2K efforts in Utah are expected to top $50 million.

Like every state agency, the Division of Comprehensive Emergency Management (CEM) has undertaken system remediation and will be in compliance long before the date change. In its contingency role, the division requires some coordination with the Federal Emergency Management Agency. In the next couple of months, CEM expects to install the upgraded version of the Federal Emergency Management Information System (FEMIS).

Current schedules call for installation in October of a FEMIS upgrade at Tooele County Emergency Management and at the Deseret Chemical Depot, the Army facility in Tooele County which stores and demilitarizes the largest stockpile of chemical weapons in the United States. That installation must occur prior to the upgrade at the state division, now slated for the end of December. Those systems will be certified by FEMA as being year 2000 compliant.

The state emergency management division also is in the process of integrating Y2K contingency planning with the state's existing Emergency Operations Plan—which covers response to disasters ranging from earthquakes to dam failures. The authority of the governor is laid out in the emergency plan, and drastic Y2K scenarios would be covered therein.

Since I assumed the office of governor in January 1993, I have activated the Utah National Guard once—when massive snowfall disrupted transportation in the most populous counties, overwhelming the capacity of local governments.

Activation of the Emergency Operations Plan is triggered when the governor declares a "state of emergency." If the disaster is beyond the capabilities of the local jurisdiction or involves two or more counties or a wide area of the state, the state assumes responsibility for the overall coordination of all state and local government emergency relief operations.

Those state operations may be augmented by military support assistance, special forms of disaster assistance available from federal agencies acting under their own statutory authorities or in accordance with the provisions of compacts with other states.

While taking care of its own operations, the state also has a vested interest in encouraging Y2K preparation within the private sector and at the local level. To facilitate those efforts, I have appointed the Governor's Coalition For Year 2000 Compliance to track the status of city, county, business and industry efforts and to promote general awareness by the public. The state has established and maintains a web site to disseminate information about the Y2K problem to the public.

We have established year 2000 coordinators in every school district of the state and throughout the higher education system. Those entities have been encouraged to develop contingency plans as well.

Contingency preparation is of paramount concern. Scenarios must be plausible, yet broad enough to cover an array of potential ramifications. What happens at the city and county level if there is a breakdown in the 911 system? What about the compliance of monitoring systems at refineries or the systems that control manufacturing processes. How do we keep essential state buildings running in the event of power failures? Is it realistic to obtain emergency generators and food supplies for institutional operations like prisons and the state hospital?

The greatest difficulty in "business recovery" or contingency planning is trying to decide what scenarios to plan for. In another year, we will know much more about Y2K readiness on the part of infrastructure providers such as utilities and transportation grids, and we will likely need to refine contingency plans continually as we move closer to the time when they may be needed.

Part of the unknown relates to how our large computing systems exchange data with the federal government, private entities and other states. Even if our system is compliant, problems can be introduced if the other data exchanges are not compliant. An inventory of all data exchanges with the federal government has been created, and we are proceeding to evaluate and test them.

The task moves forward—system by system; step by step, with the foresight we have today and the flexibility to modify what we will know tomorrow. We undertook this process early and will continue it through the date change to 01–01–00. Utah

will not be the first location on the globe to roll over to 2000, and we will be monitoring other areas for electrical failures, infrastructure breakdowns and business disruption when the sun rises on the new millennium in our time zone.

It is the state of Utah's expectation that we will greet that dawn informed, confident, and ready.

RESPONSES OF GOV. MICHAEL O. LEAVITT TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Would you agree with the assessment that the states have a long way to go? In your estimation, can the Federal Government be doing more to help state and/or local Governments prepare for the millennium rollover?

Answer. While it is accurate to say there is a long way to go still, I do not believe that state governments, on the whole, have "too far to go"—in other words, the reporting that is occurring through the National Association of State Information Resource Executives (NASIRE) and other organizations indicates that most state governments are making appropriate progress toward completion of compliance efforts. Most States are reporting between 30 percent and 70 percent completion rates. I can really only speak for our State—in our case we are now 60 percent complete with remediation and testing of our mission-critical systems and feel we will have all of those systems compliant in time. I do not know as much about local governments across the nation. In our State, our assessment is that larger municipalities are well on their way to becoming compliant, but that some smaller and medium-sized cities have only recently begun compliance efforts and have much to do still. The Federal Government could help local governments by assisting their national organizations in efforts to raise awareness and assist in compliance efforts. The best thing that the Federal government can do for the states is to assure remediation of their own mission critical systems, particularly those that heavily support State programs and operations. Additional funding for federally mandated systems such as unemployment and welfare systems would be useful.

Question 2. Were all 50 states represented at the NGA's "Year 2000 State Summit"? Can you tell us what kind of follow up to expect from the summit?

Answer. 48 of 50 states were represented at the NGA Summit. As a result, more states have been involved with support for local governments, there is an increased level of understanding between key Federal departments and their state counterparts, and both State and Federal governments are working to complete data exchange projects. NASIRE has completed an online status survey to track overall status of the states. Most states expect to have their own systems fully prepared for Year 2000. States have become involved with PTI, NaCO, and other associations to provide outreach to counties and cities. Many States are also working through their public service commissions to monitor the status of the utility industry. States have also been involved in supporting National Y2K Action Week, SBA's small business outreach, and outreach to the education community. A funding problem still exists with some local governments. Technical resources continue to be a challenge. We will need to work together to address these issues into the next century.

Question 3. From your perspective as one of 50 Governors responsible for the safety and well-being of your citizens, what more should be happening at the Federal level to help reduce the uncertainty in making Y2K preparations?

Answer. One of the things that would be helpful is alluded to in your next question. To the extent that the Federal Government is assessing the compliance efforts and readiness of various industry sectors (transportation, utilities, financial institutions, etc.) it would be helpful if the states could receive regular reports about progress in those sectors. That would help the states in their emergency response planning efforts. Similar reports about the status of Y2K compliance by other countries would also be helpful. As the Year 2000 date change gets closer, the need for timely and accurate information and reporting from the federal government level will increase. States' contingency and business continuity plans are prepared based on a set of assumptions. As certain types of failures are eliminated as possibilities, it becomes easier to determine where these efforts should be focused. When the actual date change occurs, an "early alert" system with clearly defined communication channels about what is working and what is not in various states and at the federal level would be important.

States need to hear from the IRS on their data exchanges and to know the scope of Federal contingency plans. Much could be done to coordinate on contingency and business continuity issues. States need to be informed of the DOD's "consequence management" plan to provide resources to local government in emergency situations. There should be a national database of all Federal applications that are criti-

cal to States that includes status information about the progress that has been made with renovating, testing, and implementing these systems. States could also make available to the federal government detailed status information on the progress of federally supported State systems.

Question 4. Governor Leavitt, how would the availability of national assessments help your state's emergency response community prepare?

Answer. As indicated in the previous response, regular assessments of various industry sectors, as well as regular, accurate information about Federal Government information systems, would be extremely helpful. One of the things we find in discussing this problem with local governments, public safety officials, and emergency response personnel, is that most "emergency operation plans" that exist to respond to natural disasters rely heavily on the concept of "getting help from somewhere else." The plans for smaller communities is often simply to turn to larger communities, community groups, the Red Cross or other aid providers for help. The plans for larger communities is often to turn to the State, the National Guard, or the Federal Government. State plans often talk about turning to other states or to the Federal Government or national associations to bring in help, supplies, etc. The problem with Y2K is that these kinds of emergency operations plans may not be viable—the answer can't simply be to turn to someone else for help, because everyone else will be dealing with the problem as well! This may create a serious problem in trying to carry out existing emergency operations plans. Communities, states, and organizations need to be prepared to draw upon their own people and their own resources to deal with possible emergencies and contingencies. One thing that would be helpful in emergency response planning would be to have the Federal Government help prepare information for the States on how the Red Cross, FEMA, and other national-level organizations are going to divide up and focus their resources in the event of emergencies. What will their priorities be? Where will they deploy manpower? If this were to turn out to be a nation-wide problem, instead of a regionally localized disaster, will they be able to respond, or are they even planning to?

Question 5. Governor Leavitt, what is the single greatest Y2K concern you have for your state and continuity of emergency services?

Answer. My greatest concerns would be that we ensure the continuation of electrical power, water, financial, and telecommunications services across the state, that we put in place the necessary emergency operations plans to deal with possible problems, and that we provide adequate and necessary information to the public without creating undue concern or panic.

PREPARED STATEMENT OF SENATOR DANIEL PATRICK MOYNIHAN

I was delighted to see that the House passed S. 2392 ("The Year 2000 Information and Readiness Disclosure Act") last night. The Senate passed this bill on Monday night and I am proud to be an original cosponsor of this most important piece of legislation. This "Good Samaritan" legislation is intended to promote the open sharing of information about Year 2000 (Y2K) solutions by protecting those who share information in good faith from liability claims based on the dissemination of that information. I want to make it clear that this legislation does not address liability that may arise separately from actual Y2K failures of systems or devices. The head of the President's Council on Y2K, John Koskinen, said that passing this bill is one of the most important things that we could do on the Y2K front. I agree.

Our hearing today will assess how well prepared Federal, state, and local governments are for the Y2K problem. The hearing will focus on the ability of these governments to continue to provide emergency services in the wake of the Y2K problem, and their responsibility in addressing potential Y2K related emergencies or disruptions. The results so far show that much work remains to be done.

In a survey of the fifty state governments, the GartnerGroup found that none of the states have completed their testing and implemented contingency plans. The survey also found that ten percent of state governments have not even begun to address the problem yet. Closer to home, New York State Comptroller H. Carl McCall released a survey on the progress of New York State local governments on the Y2K problem. The survey found that many of New York State's local governments, particularly smaller ones, are unprepared to face the Y2K problem. I commend Mr. McCall for the work he has done on this issue and for doing this survey. But the survey reveals that New York, as does the rest of the country, has a lot of work to do in a very short amount of time.

On July 31, 1996, I sent President Clinton a letter expressing my views and concerns about Y2K. I warned him of the "extreme negative economic consequences of the Y2K Time Bomb," and suggested that "a presidential aide be appointed to take

responsibility for assuring that all Federal Agencies, including the military, be Y2K compliant by January 1, 1999 [leaving a year for 'testing'] and that all commercial and industrial firms doing business with the Federal government must also be compliant by that date."

January 1, 1999 is quickly approaching. I believe the "Good Samaritan" legislation will encourage Federal, state, and local governments to work together in addressing the computer problem. I remind my colleagues of John Locke's conception of government as a fiduciary trust with the obligation to act in the interest of the people. If we do not address the Y2K problem, then we have not fulfilled our fiduciary responsibilities.

PREPARED STATEMENT OF MAJ. GEN. EDWARD J. PHILBIN

Mr. Chairman, I am Major General Edward J. Philbin, USAF (Ret.), the Executive Director of the National Guard Association of the United States (NGAUS). I am present to offer opinions on the problems that may arise as a result of non-compliant computers and computer dependent systems that are unable to transition through midnight, 31 December, 1999 and the role the National Guard could and probably will play in managing emergencies arising from those problems. My testimony generally reflects the opinions of the Association and its members, who are the commissioned and warrant officers of the Army and Air National Guard. It should not be construed as representing the official positions of the Department of Defense or of the National Guard Bureau.

It is increasingly evident that an appreciable part of the nation's infrastructure could be adversely affected in some way, by what is commonly referred to as the Y2K problem. In general, the National Guard has the capacity to provide Military Support to Civilian Authorities (MSCA) and can contribute a myriad of human and equipment resources to restore essential operations disrupted by Y2K generated incidents.

Considering the possibilities of a large scale disruption of governmental, commercial and other routine daily activities, it is certain that the National Guard will be among the first organizations activated to assist in the revitalization of the nation's computer dependent infrastructure. As with hurricanes, floods and other incidents requiring a quick reaction by a well-trained and equipped on-site team, no other organization will be able to respond in support of police, fire fighting and other civilian emergency responders, to major crisis situations that may be caused by Y2K disruptions as well as the National Guard. The National Guard's practiced interaction with state and local organizations and its connections to the National Command Authority provide a unique emergency response capability not found in any other federal or state organization.

The immediate need is to determine what responsibilities the Guard will be expected to assume in the management of the Y2K related problems, that many analysts have forecast, which have the potential to trigger the destabilization of societal functions. The National Guard needs to be prepared to assist in maintaining or reestablishing essential stability in the civil sector.

I suggest that the Department of Defense (DOD) must develop a clear concept of how the National Guard will be required to respond to the spectrum of problems that could be created by a Y2K disruption. The DOD, through the Chief of the National Guard Bureau (NGB), must now coordinate with the Adjutants General and the Governors to determine the likely, locality specific scenarios that may arise in a Y2K situation.

The DOD should also assist the Governors and State Emergency Response Coordinators to ensure that the National Guard itself will not be impaired by the effects of a Y2K incident at a time when it will be most needed.

I suspect that, to date, this has not been a priority effort on the part of the DOD, even though to properly prepare for possible Y2K disruptions, the OSD must be cognizant of the importance of the National Guard being made fully capable of responding to any such technical breakdown.

We must be certain that the National Guard will not itself be a victim of any Y2K disruption. All National Guard units in 3,200 locations throughout the nation, must possess computer dependent equipment that is Y2K compliant. Responding to the consequences of a Y2K disruption will be futile if the National Guard's operations are plagued by the very consequences the Guard is attempting to manage. It is critical that the Y2K response requirements of the National Guard be fully funded to ensure that it is able to respond quickly and effectively to the needs of the community. I respectfully request, Mr. Chairman, that this Committee urge the Senate to provide full funding for Y2K compliance upgrading of National Guard equipment as

one of the highest priorities for such funding, since the Guard will be among the first responders to a Y2K incident together with police, fire-fighting and other civilian emergency response personnel.

The critical first step in ensuring that the National Guard will be fully prepared for a possible Y2K calamity is the collection and sharing of information. When I was Commander of the New Jersey Air National Guard, the State Adjutant General, for the first time requested all of his commanders to conduct a survey to identify all of the Army and Air Guard resources that could be made available in response to a state emergency. My survey of the New Jersey Air National Guard identified a surprisingly long list of both mundane and sophisticated equipment which could be useful in responding to a state emergency. I strongly recommend that such a survey of the available resources of both the Army and Air National Guard of each state and territory be conducted prior to midnight on 31 December 1999. Equally important, we must determine how the National Guard will interact with the Federal Emergency Management Agency (FEMA) and the DOD in response to Y2K induced emergencies. Command and control of multiple agencies must result in mutual support rather than multiple collisions in addressing emergency situations.

Therefore, a comprehensive study should be conducted on the potential roles of and the interaction between the FEMA, the DOD, and the National Guard of the various states and territories in response to Y2K induced problems. I applaud the recent inclusion of the National Guard in the President's Y2K subcommittee on emergency response chaired by FEMA and believe that the subcommittee, with the DOD, National Guard Bureau (NOB) and the Adjutants General must develop a cohesive strategy that prepares this country for any event of mass effect leading up to and after midnight, 31 December 1999. Mr. Chairman, let me stress the need for the Adjutants General to play an important role in the development of this strategy. In most cases, it will be the Adjutants General who will integrate the planning efforts for their respective states, with those to be developed by the National Command Authority.

As you are aware, the Quadrennial Defense Review highlighted the role of the National Guard in homeland defense of the United States. While the Guard stands ready to meet the needs of the citizenry during any Y2K incident, it is important that in preparing for that eventuality, the National Guard's ability to respond to it's Total Force mission of rapidly expanding our Army and Air Force in response to a national threat not be denigrated. Funding for current combat readiness resourcing should not be used to enhance the Guard's ability to respond to a Y2K event. As an example, it is becoming increasingly evident that the current structure of the Active Duty Army cannot execute the two Major Theater Wars (MTW) strategy without the assistance of the Army National Guard Combat Divisions and Brigades. This increased dependency on the National Guard requires increased, not decreased combat readiness resourcing to enable the Guard to accomplish its historic combat mission. Mere reallocation of current funding to Y2K missions will have a negative effect upon the National Guard's ability to recruit, train and keep our soldiers and airmen combat ready to respond at a moments notice to a national threat.

The Year 2000 challenges present an emergency scenario unlike any other in our nation's history. Our technological society has grown extremely dependent upon the continuity of computer driven systems and networks and as a consequence, the nation's vulnerability has increased appreciably. Any significant disruption of our computer dependent infrastructure could result in a significant societal disruption. However, with the cooperative interaction of federal and state governments, the military, the private sector, and with serious advance preparation, the impact of such an event on the American people can be significantly reduced, if not totally eliminated.

Mr. Chairman, members of the Committee, I would like to thank you for the opportunity to offer the opinion of the National Guard Association of the United States on the readiness of the National Guard to deal with potential Y2K emergencies. As we have for over three and a-half centuries, the National Guard of the United States, Army and Air, stands ready to protect the nation against military threats and local disasters. This concludes my statement subject to your questions.

RESPONSES OF MAJ. GEN. EDWARD J. PHILBIN TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. In your testimony you indicated the criticality of fully funding the Y2K response requirements of the National Guard to ensure that it is able to respond quickly and effectively. What is the amount necessary to fully fund the National Guard's Y2K requirements, both Army and Air divisions? You imply that it

is not fully funded—can you address the current funding budgeted for the National Guard's Y2K requirements? Have requests been made for any shortfalls?

Answer. Full-funding of the National Guard to enable it to effectively respond to a Y2K incident is essential. I have received estimates that the Army National Guard will require approximately $38 million for Automation, Logistics, Manpower and TDY support to be able to ensure mission capability for Y2K incidents. This amount does not include weapon systems but rather those resources that would most likely be needed during any such incident. Estimates of Air National Guard requirements vary greatly and consequently would be difficult to pinpoint at this time.

Question 2. General Philbin, you make a strong case for the importance of the National Guard in a Y2K emergency. Certainly, the Guard is used time and time again, such as today in the southern United States, to deal with major disasters. I am surprised however that the call for a survey such as you're suggesting has never been done. You mentioned the survey that was done when you were commander of the New Jersey Air National Guard. It seems natural to me that surveys and inventories be done to assess readiness. Doesn't anyone have the responsibility to do this for the National Guard? Shouldn't someone be doing it within the Department of Defense?

Answer. The National Guard has been successfully providing assistance to the American public during natural disasters or civil disturbances for more than 360 years. This has allowed the Guard to adapt, and review its response to such events in order to provide effective Military Support to Civil Authorities (MSCA). Many of the traditional MSCA roles of the National Guard can and will be utilized during a Y2K event. However, the unique possibilities that could unfold during a Y2K event are unprecedented. Surveys have been conducted to determine the capabilities of the Army and Air National Guard to be able to support events, such as floods, fires, tornadoes, and riots, that have a historical precedence. These surveys focus on the premise that an interruption will occur to a portion of normal operations of the nation's infrastructure. No event, has the capability to disrupt governmental, commercial and other daily activities as the Y2K millennium bug, shutting down the technological components that drive our society. A survey specifically targeted on Y2K events needs to be conducted in order to determine what capabilities the National Guard can offer to support the return to normal function capability.

Question 3. Your have strongly recommended that a survey of available resources of both the Army and Air National Guards of each state and territory be conducted prior to midnight on 31 December 1999? Aren't there National Guard documents that already exist which provide the requirements for organizations and equipment as well as ones that indicate the authorized and actual levels? What would be achieved by a survey such as the one you propose that does not already exist? How would the results of such a survey be useful?

Answer. Accountability of all National Guard equipment and organizations is maintained by the National Guard Bureau and the Department of Defense and is usually focused on the Guards constant readiness. However, no study has been conducted to determine specifically what the Guard and its resources can contribute on January 1, 2000. The Y2K millennium bug is significant in that it will provide both foreseen and unforeseen challenges. A survey of equipment to determine what resources are available for all possibilities during a Y2K event will allow the Guard to better organize a response plan. Insight as to what assets the Guard can contribute during the following hours and days of the Y2K event are essential in order to allow the National Guard Bureau and the Department of Defense time and foresight to enhance their coordinated response plan.

Question 4. Your point is well taken that before the National Guard can perform any of its emergency response functions it must ensure that it will not be impaired itself. Would you discuss the current status and milestones of the Army and Air National Guards' Y2K programs? Are the programs adequately funded?

Answer. Being the Executive Director of the National Guard Association and not the National Guard Bureau, it would not be feasible for me to provide a progress report. The Chief of the National Guard Bureau and/or the Army and Air National Guard Directors are better positioned to discuss their progress in achieving Y2K compliance. However, I am sure the National Guard Bureau and the Adjutants General are working diligently to determine their compliance posture and how they would support the states in a Y2K situation, should one occur. With that said, it is my belief that the National Guard may very well require additional funding to support their compliance review and response capability, but I must defer to the National Guard Bureau to provide specifics.

Question 5. Both the Army and Air Force active components have comprehensive Y2K programs that include their respective National Guard. What is the basis of

your statement that efforts for fixing the guard Y2K problems are not a priority within the DOD?

Answer. As demonstrated in the past, the Department of Defense prioritizes funding as a function of the "first to fight" concept as it applies to the military forces to execute the National Military Strategy. The services are more inclined to insure Y2K compliance as it relates to force projection requirements and their ability to engage an enemy on the battlefield. I doubt that serious efforts have been made by the Department of Defense to address the role of the National Guard to support the restabilization of domestic activities due to a Y2K event. I am sure that if the services had full funding available, they would resource all of their requirements across the spectrum. However, threat reduction to the United States over the past decade has also entailed a defense budget reduction. The DOD has taken the approach that the Y2K millennium bug is a metaphoric enemy set to attack. They are focusing on their mission-critical systems, to ensure that the services are prepared to perform their duties to defend the nation. The National Guard, in addition to defense of the nation, remains focused on support of local and state governments in ensuring that society's infrastructure is returned to and remains functional during a Y2K event. It is equally important for the National Guard to defend America's borders from attack, or respond to aid our allies. However, with a set time, where our nation will face significant dilemmas due to the vulnerability of our technologically dependent society the Y2K event requires the full attention of the National Guard and the Department of Defense.

Question 6. In your testimony, you express concern over the issue of command and control of multiple agencies in addressing emergency situations. Specifically what part of the Federal Response Plan and current command and control structure under the plan requires refinement or modification? What aspects of possible Y2K scenarios would cause a need to change current command and control relationships?

Answer. Response to Y2K events begins at the local level. Once local authorities reach the limit of their capacity, state resources will be required, as in other emergency situations. The capability to activate the National Guard now becomes a factor for the Governor. The command and control relationships are in place to respond to situations requiring military support. However, the possible magnitude of a Y2K response situation may be greater than local resources can handle. Integration with law-enforcement, fire, medical and other state and federal agencies will require significant inter-agency cooperation on an unprecedented scale. It would be prudent to study the capabilities of the National Guard to determine what levels of support they could provide along with their ability to respond to a Y2K event.

PREPARED STATEMENT OF SERGEANT JOHN S. POWELL

INTRODUCTION

> If the predictions of computer system failures in everything from automobiles and ATMs to the IRS to traffic signal controls and a plethora of other systems that support everyday life are even partially realized, the overload on public safety services will be tremendous. The "bug" is insidious, potentially impacting anything with a microcomputer chip—anything that has a keypad or timer, displays a date, stores numbers, or performs calculations. Consider for a moment the possible loss of a few personal items: digital clocks and wristwatch, automatic coffee maker, camcorder, home alarm system, pager, personal computer, radio, telephone, television, thermostats, VCR, and last (but certainly not least) access to ATMs, financial records, and retirement income (if you're lucky enough to have it)! Couple these potential failures for millions of people with increased turn-of-the-millennia activity and the impact on public safety services could be crippling. The last thing public safety agencies will then want to contend with is problems with their own operational systems.
>
> —The APCO Bulletin

How big is the overall problem? After reviewing published documents and interviewing a number of Y2K experts, "Silicon Valley Tech Week" concluded in its April 13, 1998 issue: "None of the mission critical sectors in the U.S. are even close to being Y2K compliant, say the experts. Not the 9,000 electric utility plants. Not the 11,000 banks. Not the telecommunications companies. And certainly not the U.S. Government."

IRS Commissioner Charles Rossotti told the Wall Street Journal: "If we don't fix the century-date problem, we will have a situation scarier than the average disaster movie you might see on a Sunday night." "Twenty-one months from now, there could

be 90 million taxpayers who won't get their refunds, and 95 percent of the revenue stream of the United States could be jeopardized." [1]

FCC Chairman William Kennard, being questioned by the U.S. Senate, concluded, "[I am] * * * concerned that the year 2000 problem has the potential of disrupting communications services worldwide * * *. Every sector of the communications industry—broadcast, cable, radio, satellite, and wireline and wireless telephony—could be affected."

There are, however, other dates both before and after January 1, 2000, that must also be considered. These include:

1. January 1, 1999: Many spreadsheets and financial applications look forward during the current year and will see the next year ends in "00." Those functions that examine a date range may not be able to handle an ending date ("00") that is lower in value than the current date ("99").

2. August 22, 1999: GPS rollover (reset to zero). GPS is now the most widely used system for public safety person/vehicle location applications. Beyond this fundamental application are other telecommunications uses, not the least of which is serving as the common time base for synchronizing transmitters in wide area simulcast systems, including most of the nations large commercial paging operations. In addition to geopositioning and telecommunications applications, GPS is used in major banks and thousands of financial institutions for accurate date and time recording and synchronization.

3. September 9, 1999: "Nines end-of-file problem" in legacy systems using 9999 in the date field to denote "end-of-file" (EOF). Most of these programs are mainframe-based, written in high-level computer languages such as COBOL. Pubic safety applications include large Criminal Justice Information Systems and motor vehicle/drivers license systems.

4. February 29, 2000: Not a normal leap year (rule: if the year is divisible by four but not divisible by 100, or if the year is divisible by 400, it is a leap year). Many computer programs perform the first two tests (divisible by 4, but not divisible by 100) but do not include the last test. Those that do not will be off by 1 day from March 1 through December 31, 2000.

LOCAL LAW ENFORCEMENT AGENCY STATUS REPORT

The following agency status reports were collected by three of the Regional Law Enforcement and Corrections Technology Centers operated by the National Institute of Justice during the past 10 days:

Aiken County, South Carolina Sheriff's Department

This department is in the process of purchasing new dispatch equipment and CAD/RMS software based on a modernization assessment done by NLECTC-SE in which Y2K compliance was recommended.

Arvada, Colorado Police Department

The Arvada Police Department is in the process of replacing their CAD/RMS system in a previously scheduled system upgrade. Y2K issues are a specification in the RFP and the contract for installation and operation. They are currently negotiating with their radio system provider (they share a trunked 800 megahertz system with an adjacent agency) to provide necessary maintenance and upgrades to address Y2K issues. This process is already budgeted for and is underway. The City information management department has engaged a consultant to assess and make recommendations regarding the "lesser" information systems in the City, including the police department, to address Y2K issues. All of the major information systems have already been brought into Y2K compliance or are in the process of being brought into compliance.

Charleston, South Carolina Police Department

This department is in the process of replacing and/or upgrading their CAD/RMS system based on a modernization assessment done by NLECTC-SE in which Y2K compliance was recommended.

Charlotte-Mecklenberg, North Carolina Police Department

A county-wide Y2K board is currently reviewing every major system that has a computer chip as a component as well as major system software packages (including radio, information management, heating and air conditioning, elevators, cars and security systems). Thus far, they have not identified the magnitude of the problem. As the list is completed they are asking manufactures for Y2K certification. They

[1] IRS Commissioner Charles Rossotti. "The Wall Street Journal, 04/22/98.

are concerned that certain chips in key components have built-in Y2K problems that can only be solved by replacement.

La Vista, Nebraska Police Department

The La Vista Police Department conducted an assessment of their internal information management system and found it to be Y2K non-compliant. They are in the process of spending $18–19,000 for an entirely new system that will be Y2K compliant. The police department has been provided funding for this by the City of La Vista which has taken a very aggressive stance toward ensuring Y2K preparedness. The police department is the last department of the City requiring compliance upgrades. The City is also coordinating with public service providers (electricity, gas, telephones, etc.) to ensure they are prepared as well.

Leavenworth, Kansas Police Department

The Leavenworth Police Department is in the process of building a consolidated building and systems with the Leavenworth County Sheriff's Department. This consolidated and upgrade is occurring irrespective of Y2K issues but contractual specifications will include Y2K compliance issues. Current systems are not Y2K compliant. This places a significant time constraint on the acquisition and installation process to ensure operation of the new systems prior to Y2K.

Medical University of South Carolina Department of Public Safety

MUSC has a large committee representing a cross section of all departments of the university that has been in existence for over a year to address the Y2K problem. Systems are being modified, upgraded and/or replaced with a completion target of mid year 1999.

Monroe County, Florida Sheriff's Department

This department has rewritten all their COBOL code to accommodate the four digit year and adjusted all chronological date accordingly. They have a model of an old Posse Code (Federally funded many years ago) that appears to be running fine. All code is now adjusted, but they are running in a test mode as a parallel system.

Mount Pleasant, South Carolina Police Department

This department's vendor has made an offer to upgrade their software for Y2K compliance for approximately $30,000. They are researching other options and are awaiting a modernization report by NLECTC-SE before proceeding with an RFP.

Nashville, Tennessee Police Department

Their Unisys Clearpath 4400 has a service package to upgrade and correct Y2K problems. They have run BIOS checks on all old computers and upgraded programs where necessary. They are replacing their central hub.

San Diego, California Police Department

San Diego PD has a full-time effort to head off the Y2K problem with 2 people assigned. San Diego describes this as a HUGE problem affecting operations across the board, especially Computer Aided Dispatch and ARJIS, their regional justice information system. The police department is working with the city on a coordinated approach.

Selma, Alabama Police Department

The Selma computer system was recently destroyed by a lightning strike and they are in the process of replacing the entire system to link communications, booking, records and eventually other municipal government data bases. New system will be Y2K compliant. This department is next in line for a NLECTC-SE process review addressing their information technology modernization needs.

Saluda, North Carolina Police Department

This is a four officer department that is totally computerized. With their small size (and reducing costs of equipment needed) they upgraded on a timely basis and are Y2K compliant internally. Their concern is other systems they tie into.

STATEMENT

Thank you for this opportunity to provide the Senate Special Committee on the Year 2000 Technology Problem with information on what I believe to be the "state of the nation's local public safety agencies" with respect to Y2K issues, as well as what we should be doing to better prepare for what was recently described on the national news as "the deadline that not even Congress or the President can extend."

Two "wakeup calls" this year highlight our dependence on critical telecommunications services. During the week of April 13, AT&T lost its entire frame relay data

network for 24 hours. The failure was caused by a software glitch in a single network circuit card that was being loaded with updated software while still connected to the network. 6,600 customers, including major financial institutions and their ATM/credit card networks, lost service. Then on May 19, Hughes Corporation's Galaxy IV satellite failed, disrupting paging service to millions of paging receivers, including critical notification systems used by federal, state, and local public safety agencies.

We've all seen the horrific predictions being made by some of the millennium fundamentalists. Unfortunately, it appears that the majority of Americans, if they are aware of the Y2K issue at all, consider it to be a "computer problem." The current status of local government agencies is somewhere in between, with larger agencies clearly being more susceptible to the problem, but at the same time also being more aware of the surrounding issues and having more resources available to deal with those issues.

Senator Bennett, Committee Chair, posed a series of five questions in his letter of September 16 [See Attachment A]. Each of these is addressed in a separate section below.

I. What is the role of APCO and the IACP in assessing the vulnerability of emergency service response agencies to year 2000 problems and any efforts to increase awareness about the problem?

First, as individual membership organizations, public safety associations generally do not have a specific role in assessing the vulnerabilities of agencies to pending events. However, the larger associations play a major role in promoting awareness and providing education to their members and the general public safety community concerning events that could impact the provision of services. Associations also serve as a statistical resource to those government agencies who are responsible for making such assessments.

Clearly, awareness and education are keys to dealing with the Y2K issue. This nation has nearly 19,000 law enforcement agencies at the state and local level; Attachment D is a breakdown of state and local law enforcement agencies by region across the United States. Ninety percent of the law enforcement agencies have fewer than 24 sworn officers and fully half have fewer than 12 sworn officers. The United States also has over 32,000 fire agencies at the state and local level. Eighty percent of the fire agencies are staffed fully by volunteers. Many of these agencies are not yet aware that problems may exists, much less the potential severity that the Y2K problem could have on both their internal and external operations.

Both associations annually host the world's largest public safety conferences in their related fields. At this year's event held this past August in Albuquerque NM, APCO conducted seminars to address the myriad of Y2K issues facing public safety agencies to ensure consistent delivery of service. The IACP will hold its conference at Salt Lake City from October 17–22. The Year 2000 Problem will be a topic of discussion at the Communications and Technology Committee meeting and at other scheduled meetings. John Clark, Deputy Chief for Public Safety in the Federal Communications Commission's (FCC) Wireless Telecommunications Bureau will be addressing the Major City Chiefs specifically on Y2K issues.

Fortunately for the public safety community, the FCC has been very active on Year 2000 issues. Commissioner Michael Powell, the FCC Defense Commissioner and agency representative to the President's Council on Year 2000 Conversion, convened a Public Safety Year 2000 Roundtable on June 1 in Washington DC. Panel members included a number of state/local public safety officials, as well as representatives from federal agencies, public safety equipment manufacturers, and consultants dealing with the Y2K problem. Both APCO and the IACP were represented on the Roundtable.

APCO and the National Institute of Justice are discussing the development of a series of short (one or two day) Y2K seminars targeted at public safety chief officers and upper level management to specifically address issues in each of the 4 impact areas discussed in the following section. We hope that these seminars could draw from subject matter experts within APCO and from our sister associations. APCO and NIJ both believe it is critical that such a series of seminars, beginning as soon as January, be conduct at little or no cost to participants, promoting maximum attendance from the thousands of small public safety agencies in the US. The National Institute of Justice operates a series of Regional Technology Centers across the US that are capable of supporting the logistics for these seminars, but the National Institute of .Justice will need a budget augmentation if it is to fund these at no cost to participants.

II. Address ways that Y2K problems might impact the operations of local law enforcement agencies. The third area involving other related issues is also discussed in this section

Local public safety agency response to the Y2K problem has several facets. *First, internal systems must be made compliant.* Nearly every agency has at least one system that will need to be checked. In the case of law enforcement it is the terminal used to access state and federal criminal justice information systems. For fire agencies it is probably alarm systems that are commonly used to automatically report fires. Additionally, many modern pieces of fire apparatus (including both engines and trucks) have microprocessor-based controllers that monitor the functions of water pumps, ladder extenders, etc.

There are several levels of systems that are potentially impacted by the Y2K "bug;" in general they are:

1. *Legacy firmware-based systems:* Difficult or impossible to upgrade, but probably not critical unless validating date ranges, these systems are extensively used in process control application, including traffic signal light controls, elevator controls, and standalone access control systems. Early standalone systems (access control, for example) had sufficient read-only memory (ROM), but limited random access memory (RAM). Programmers went to great lengths to preserve RAM. Many such systems are still in use! Formats were designed to store dates in a manner that permitted rapid mathematical manipulation. The most common (YYDDD or YYMMDD) require 2 bytes (16 bits) for a 2 digit year code. Application and report generating programs using date ranges (for age, access card validity, etc) can not function across a century boundary if they use a 2-digit year code.

Firmware-based systems also include most of the home electronic items mentioned at the start of this Statement: alarm systems, digital clocks, wristwatches, automatic coffee makers and similar appliances, automatic setback thermostats, pagers, radios, "smart" telephone sets, televisions, camcorders and VCRs.

2. *Mainframes:* Getting much of the attention, but usually programmed in higher level languages such as COBOL making updates easier, these systems include many federal/state CJIS-type databases.

3. *Mini-computers:* More difficult to update because code is often written in lower level languages such as C++ and optimized for speed, these systems include message switches and older and/or larger CAD/RMS systems.

4. *Personal Computers:* Finally, PC-based workstations are a common man-machine interface to many 9–1–1 and alarm reporting systems, Computer Aided Dispatch (CAD), dispatch consoles, Records Management Systems (RMS), telecommunications and trunked radio switches and a host of related systems. Email systems in LAN, Intranet, WAN and Internet applications link personnel and off-site facilities. Mobile Data Terminals (MDTs) are a thing of the past; the new game is Mobile Computing Terminals (MCTs) based on PC architecture. Within the Personal Computer, there are multiple levels to be addressed:

—*Hardware BIOS:* Over 90 percent of PCs built before 1997 have a bios-level problem. Many of these should be easy to fix.

—*Operating Systems:* Nearly all OS vendors are now addressing date handling problems with patches or the release of compliant upgrades.

—*Applications Software:* Many software packages still have a two-digit date problem. A test of 5000 general software packages found 64 percent had some problem.

—*Data Within Single Application:* most databases and spreadsheet applications have 2-digit dates.

—*Data Shared Between Applications:* applications may make different "guesses" about the 4-digit year when encountering 2-digit year fields.

For proposed resolution to these problems, we can again turn to the FCC's June Roundtable. All of the consultants agreed that there is a quite straightforward process to be used for equipment evaluation. The recommended steps include: equipment inventory, analysis for problem potential, manufacturer/vendor inquiry and certification, testing (independent or in-house), correction or replacement of non-compliant systems, and re-testing. A critical recommendation was the testing of all components of a system operating together as a final test once corrections have been made. Use "IVE"—Independent Verification of Everything!

The consultants further agreed that in some cases the cost, both in time (or lack thereof) and money, is leading agencies to replace systems rather than attempt to upgrade an existing investment. In fact, many agencies are using the Y2K bug as an opportunity to perform much needed replacements of outdated systems.

Equipment manufacturers present were primarily from the land mobile radio community. Several stated that their public safety equipment lines are so new that

the problem was addressed in the initial design. Others, including Ericsson and Motorola, stated they have some embedded equipment that may be impacted and offer information on determining Y2K compliance of their equipment on their Internet web sites. In particular, Motorola provides a search engine that allows access to information on Y2K compliance of their equipment in 3 categories: tested and passed, tested and did not pass (with additional information provided), and not yet tested. Unfortunately, Motorola has more recently stated that some older equipment, primarily in the high-level encryption arena used by federal agencies, is not compliant and will not be updated.

The best general news from this Roundtable is that the Y2K bug will not impact most conventional radio dispatch equipment (radio system infrastructure and field subscriber units). However, some radio system management equipment and software (report generators, etc) may need upgrades, particularly for trunked radio systems. Unfortunately, the same is not necessarily true of other critical public safety software such as Computer Aided Dispatch (CAD) and Records Management (RMS) systems. These systems are widely used; the majority are legacy systems in service for some years, and will require upgrades to the point that many agencies are considering full replacement. The critical factor for these latter systems is the long lead time for government procurements coupled with a potential overload on vendors over the next 15 months. The attached documents from the City of Oakland, California, [Attachments B & C] highlight the problems in dealing with CAD systems, and the costs and time elements involved in correcting such problems.

The next area of impact on state and local agencies is dealing with potential disruption of outside services, primarily utilities such as power and 9–1–1 services, and the delivery of consumables. The critical "72 hours" of self-reliance that disaster planners generally acknowledge as the amount of time before outside help is available at a disaster scene might not apply if the problem is indeed nationwide in scope. As an example of some of these issues, I will briefly examine the East Bay area of Northern California where the University of California at Berkeley is located:

The utility supply is of critical importance:

(1) *Electric power.* Nearly all elements of daily campus life would be profoundly affected by a prolonged power outage. With the predictions that some nuclear-fueled plants will be required to cease operations due to the thousands of imbedded systems that can not possibly be tested in the next 15 months, utilities will be forced to rely in fossil fuel and water-driven plants. Fortunately, both are in abundance in Northern California. Nonetheless, Pacific Gas & Electric Company generates a significant amount of its power at its Diablo Canyon nuclear plant. California, as with most states, is dependent on a regional power grid. Most people still recall the massive New England power outage caused by the failure of a simple relay. PG&E states on its Web site that it has inventoried—but not yet assessed for potential Y2K problems—its embedded systems, and that it plans to complete repair or replacement of these systems by the 4th quarter of 1999, which leaves little margin for error.

(2) *Water supply.* Another core consideration is water: whether it will continue to flow to the campus, and whether it will continue to be correctly treated. An adequate supply of water is critical to fighting some types of fires, and for treating some types of chemical exposures. A complex series of steps is typically used to treat water. Failures due to Y2K-related problems at treatment facilities (even those involving an excess of treatment chemicals, as is alleged to have occurred in a Y2K rollover test at an Australian water utility) could affect the health of local residents, as well as heating and cooling systems, laboratory experiments, and much more.

Beyond that, the East Bay Municipal Utility District (EBMUD) is dependent on multiple electric utilities to supply power to its pumping stations and treatment facilities. Power outages at various points throughout its system could thus adversely impact water supply and treatment. The treatment facilities all have standby diesel generators, as do some of the "more critical" pumping stations. In addition, there are some portable generator trucks that can be deployed in an emergency. These are all dependent on an adequate supply of diesel fuel being available to permit operations to continue throughout a potentially prolonged power outage.

In addition, EBMUD relies on a Supervisory Control and Data Acquisition (SCADA) system for monitoring and controlling water pumping which is not Y2K compliant. However, the vendor of the utility's SCADA system appears to have successfully tested Y2K fixes at several natural gas utilities during Summer 1998, and these fixes should be applied to EBMUD's systems and tested by the first quarter of 1999.

(3) *Telephone systems.* The American public relies on a highly advanced land and radio-based telephone national telephone network that supports virtually all emer-

gency reporting via the almost universally available 9–1–1 system. A failure in this complex, computer-driven network, as happened to the AT&T network in mid-April would be devastating to emergency service providers.

Medical equipment compliance is another area of concern:

> Equipment used in local hospitals—and especially at teaching hospitals like UC San Francisco—might potentially be at risk for Y2K failures. Some failures have been reported in these devices, and there is still a great deal of uncertainty in this area.
>
> As reported in the Washington Post on September 24, 1998, Senator Chris Dodd (D-CT) has taken the unusual step of publicly identifying the nearly 1,200 medical device manufacturers who failed to respond to a June 1998 letter from the US Food and Drug Administration asking about possible Y2K problems.

The third area of impact, and clearly the most difficult to judge and plan for, is the additional workload that could be placed on agencies by public response to heightened fears toward the end of 1999, followed by actual problems after December 31. If even the minimal worldwide disruptions that have been predicted should occur, the additional workload placed upon public safety agencies, and law enforcement in particular, could be significant. This is an international problem and I understand that the Association of Chief Police Officers in the United Kingdom has already recommended that law enforcement agencies in Great Britain cancel all leave over the millennium holidays.

Last, and directly related to the third area, is dealing with the special needs of agency employees during the period of impact. It is a fact that people do not perform at anywhere near 100 percent if they are worried about their families or their homes. As with any disaster, public safety personnel will only be effective if they have prepared themselves and their families in advance. Year 2000 is inevitable; personal preparation is essential. What can you as an individual do to prepare? Suggestions include:

1. IVE—Independent Verification of Everything. Test all of your important home appliances by resetting the dates and allowing them to roll over the century and leap year dates. If you live by your PC as we do it should be at the top of the list, especially if you use it for on-line banking, financial management, or email communications with your office. Consider buying a small electric generator to support critical home electrical needs if power fails; remember to stock up on fuel in approved storage containers during December, 1999.

2. Bank and other financial services systems are linked in huge international networks where a single failure could cause network-wide problems. While the large banks, brokerage companies, mutual fund houses and stock markets state that they will be ready, smaller institutions without the fiscal and technical resources to properly address the problem may pose a higher risk. Correspond with your institutions and obtain written assurance that your data and your money will survive; then make sure you keep written copies of all account statements!

Credit card processing has already experienced snags as cards with expiration dates beyond 2000 encounter non-compliant processing equipment. Again, maintain copies of your account statements. Check them carefully and be prepared to dispute inaccurate bills.

Delays in clearing checks (including pay checks) are predicted. A number of Y2K "experts" are recommending keeping significant cash (up to 2 months worth) on hand as 2000 approaches.

3. Insurance policies and mortgage documents face similar problems. In both cases, obtain written documentation of coverage extending beyond 1999. For mortgages, it is important to obtain a lender-issued statement detailing payments (interest and principal) already made, as well as an amortization schedule showing payments during 2000 and beyond in case the lender's computer system is unable to issue payment coupons. Both institutions will still expect their payments to be sent!

4. Finally, but perhaps most importantly, is insuring that you will continue to receive income from your employer or retirement system. Take an interest in your agency payroll systems and offer advice and assistance as appropriate; all of us are dealing with the same problem! The Social Security Administration has been working on Y2K compliance for a number of years and should be ready for Y2K. Unfortunately, as stated above, some other federal government agencies (including the US Treasury Department) that must work with Social Security are far behind. Since many public safety agencies participate in local or state retirement systems, it is important that each of us again maintain detailed records of our account(s) and be prepared for disruption in payments if you are fortunate enough to be retired.

III. The next question posed by the Committee concerns Y2K issues in the campus policing and security environment

With one major exception, these issues are identical to the general public safety community. That exception is this: campuses, like military bases, are cities unto themselves, some small but others very large. In the case of UC Berkeley, we have a daily campus population that can approach 50,000. Within that "city", and unlike a general government city, the campus is responsible for all buildings, all operations, all services. Based on a detailed outside analysis, I can tell you that the University of California appears to be in very good shape overall with respect to Y2K.

Our internal systems are similar to the legacy systems in Oakland and other agencies described in the status report above. They include CAD, RMS, access control and fire alarm systems. The RMS system has been upgraded and now appears to be compliant. The CAD and Access Control Systems were first installed in 1984. As with the Oakland CAD system, both have seen hardware and software updates, but today function in much the same way as they did when first installed. These systems have far outlived their initial design lives. Perhaps George Orwell was right; however he selected the wrong means to the end!

The company that provided our CAD system last year contacted all of its installed base, providing a list of system hardware and software that needed to be upgraded before new Y2K-compliant CAD software could be installed. Those changes have been completed and UCPD is in fact today installing what should be the final upgrade to the police CAD system software. Once installed and thoroughly tested both alone and in conjunction with interfaced software such as RMS, the vendor will certify the system as Y2K compliant.

Fire alarms are also being examined. Most new or recently-remodeled buildings have microprocessor-based fire detection systems. As with fire codes around the country, should these systems fail on January 1, 2000, these buildings can not legally be occupied.

In general, outstanding issues within the University of California public safety environment have at least been identified and most are being addressed. Fortunately for us, the millennia falls during a period when classes are not in session. Thus we will have a small window of opportunity to correct inside problems. We will, however, suffer equally with problems from outside as previously discussed.

IV. Finally, the Committee asked for recommendations.

In my opinion, the single most important failure to be prevented is the widespread loss of electrical services for more than about 72 hours. Public safety backup generator systems generally have fuel supplies sized to support 72 hours of continuous operation. Beyond that time, it may be difficult to get fuel delivered and systems begin to fail. Every effort must be made to ensure this does not happen because the prolonged loss of power will quickly cripple most public safety facilities and communications systems.

The single most important issue is education, both of the American public and for those at all levels of government responsible for identifying, correcting and dealing with the Y2K Technology Problem.

As previously mentioned, APCO and the National Institute of Justice have started developing a series of Y2K seminars targeted at public safety chief officers and upper level management to specifically address issues in each of the 4 impact areas mentioned above. To conduct these seminars at little or no cost, thus promoting maximum attendance from the 10's of thousands of small public safety agencies, the National Institute of Justice will need a budget augmentation. Congressional support for a program of this type is extremely important if state and local agencies are to be properly educated on the wide range of Y2K issues that they must address over the next year.

Last, from the halls of Congress to the Oval Office, elected officials must make the Year 2000 Technology Problem a top public education priority. The American people need to be aware and be involved. We must have ongoing and realistic assessments of the potential for problems across the plethora of impacted services. A public caught off-guard by major failures on January 1, 2000 could result in devastating long-term impact on the welfare of this great nation.

As a Boy Scout and later serving as the Emergency Preparedness Officer at Berkeley during the Loma Prieta Earthquake, the drought, the floods and the Oakland Hills Fire, I learned the critical meaning of 2 words: BE PREPARED. We must be prepared.

Clearly, if there is a potential for failure within major segments of the world's public and private infrastructures, the one sector that can not be allowed to fail is the provision of public safety services, and in particular the delivery of appropriate law enforcement services.

ABOUT THE AUTHOR

John Powell has been active in public safety communications since 1971. He received a BSEE from the University of California at Berkeley in 1973. He joined the UC Police Department that same year and was promoted to sergeant in 1977. Mr. Powell served as an advisor to the California Legislature's Joint Committee on Fire, Police, Emergency and Disaster Services, and is a member of the California Law Enforcement Mutual Aid Radio System Executive Committee. He is a past-president of the Association of Public-Safety Communications Official's—International (APCO) and has been an APCO representative on the Project 25 Steering Committee since its founding in 1989. He is a member of the Communications & Technology Committee of the International Association of Chief's of Police and is IACP's technical representative to the National Public Safety Telecommunications Council (NPSTC). He is vice-chair of the Communications Subcommittee of the Law Enforcement & Corrections Technology Advisory Council to the National Institute of Justice. In August, Mr. Powell received APCO's highest award for "Long-Term Technical Contributions to the Art & Practice of Public Safety Communications." Mr. Powell is a life member of APCO, a member of IEEE and a fellow of the Radio Club of America.

[ATTACHMENT A]

U.S. SENATE,
SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM,
Washington, DC., September 16, 1998.

Sergeant JOHN S. POWELL,
University of California Police Department,
1 Sprout Hall Berkeley, CA

DEAR SERGEANT POWELL: The Special Committee on the Year 2000 Technology Problem, which I chair, is holding a hearing at 9:30 a.m., on October 2, 1998, in Room 192 of the Dirksen Senate Office Building. The hearing will encompass the Year 2000 readiness of state and local government emergency response agencies, as well as Federal emergency response preparedness. I am inviting you to testify on (1) the role of APCO and the IACP in assessing the vulnerability of emergency service response agencies to year 2000 problems and any efforts to increase awareness about the problem, (2) ways in which Year 2000 problems might impact the operations of local law enforcement agencies, (3) other Y2K related emergency preparedness issues for local law enforcement, (4) Y2K issues in the campus policing/security environment, and (5) any recommendations for Congressional or other governmental action which you believe might have a positive impact in this area.

Please submit 120 copies of your statement no later than 48 hours in advance of the hearing and an electronic copy in ASCII format. This will help Committee members and staff better prepare for the hearing.

Please limit your oral testimony to 5 minutes in length. Your written statement may be whatever length you believe appropriate, but should be accompanied by a brief written summary. Statements should be delivered to the Special Committee. The electronic copy may be provided on a disk, or e-mailed to year2000@y2k.senate.gov. Due to space limitations in the hearing room, there will be reserved seating for you and one other person. Other people from your office may use open seating. Thank you in advance for your participation. If you have any questions concerning the hearing, please contact Mr. Tom Bello, Committee staff, at (202) 224–5224.

Sincerely,

ROBERT F. BENNETT,
Chairman.

[ATTACHMENT B]

CITY OF OAKLAND
Interoffice Letter

TO: Avon Manning, Administrative Services Agency Director
FROM: Stephen Ferguson, Director Office of Communications & Information Services
DATE: September 16, 1996
SUBJECT: The "Year 2000" and Information Systems in the City of Oakland

SUMMARY

At midnight on December 31, 1999, when the calendar changes to January 1, 2000, many information systems around the world will either fail or not function properly. In some cases, the failure will occur long before 12/31/99, e.g., when a system must project or make calculations into the future for dates or payment schedules beyond 12/31/99.

In the City of Oakland, a number of business systems have been implemented over the past 15 years that will be affected by the "Year 2000" problem and must be addressed as a high priority. The three most critical areas needing immediate attention are: (1) Payroll/Personnel system, (2) Police Computer Aided Dispatch (CAD) system, and (3) PC software and hardware. In addition, there are many other systems in the City which will require modification; however, we believe these systems can be modified using existing staff within the course of their on-going maintenance duties.

The overall impact of the Year 2000 problem on the City should not be underestimated. The high priority, mandatory workload comes at a time when the information technology needs of the City are expanding and resources have been significantly reduced. Consequently, staff's ability to support new technology and systems demanded by agencies and departments will be curtailed at a critical time.

A detailed study of over 70 systems conducted by the Office of Communications & Information Services (OCIS) staff estimates that correcting the problems in systems affected by Year 2000 issues would take over 24,000 staff hours at a cost of $3,000,000. While this corrective approach specifically addresses the Year 2000 problem, there is little general benefit to the City. In other words, staff can spend about 18,000 hours correcting the Police CAD and Payroll/Personnel systems, but when completed, the City will continue to have both a CAD System that is over 17 years old, and a Payroll/Personnel System that is 11 years old, with minimal new functionality, despite the efforts expended.

Therefore, key recommendations include:

(1) Replace the Payroll/Personnel system at an estimated cost of $1,000,000.

(2) Replace the Police CAD system at an estimated cost of $300,000 to $500,000.

BACKGROUND

The reason for concern over the Year 2000 problem is often not easily understood by individuals outside information technology organizations. However, a general understanding of the issue is critical for senior management to support the commitment of resources necessary to solve the problem.

There are two factors that exacerbate the Year 2000 problem: the aging of many of the City's information systems, and the historical failure of systems developers to anticipate or acknowledge the problem.

Many systems currently in use in the City are based upon design specifications dating back to the late 1970's and early 1980's. The systems are sometimes referred to as "legacy systems." When the systems were originally developed, the designers assumed that these systems would last for seven to ten years and would then be replaced. Instead, many of these systems have been incrementally modified to meet changing business requirements and are still in use 10, 12, and even 15 or more years later.

A good example is the City's Police CAD System. The system was originally purchased by the City as a turnkey application in 1976. In 1983, staff began an effort to replace that system. The replacement project was built upon the premise that the new system had to function exactly like the old. The only changes were in the underlying hardware platform which involved newer, more reliable technology providing increased capacity to store and retain a greater volume of data on calls for service. Therefore, design considerations related to date issues were carried forward into the new system without regard for the Year 2000 (a date too distant to be considered a factor).

The second part of the problem relates to the way programmers were taught to handle dates required in systems. As a rule, programmer training totally ignored the Year 2000 problem. Historically, programmers and systems analysts have been taught to handle dates in a specific format. For example, the date "September 10, 1996" would be stored as 96/09/10. By storing the date in this two-digit (year/month/day) format, sorting information in date sequence was easier, and calculations of the time periods between two dates could be made in a standard way.

The Year 2000 problem results from the two-digit year used in the date field. For example, 1951 is stored as "51," 1996 is stored as "96," and 2000 would be stored as "00." The computer is programmed to calculate the number of years between these dates by subtracting the first year from the second year, i.e., 96–51 = 45. In

the year 2000, the calculation would be 00–51 = −51, an obvious error. In order to correct the calculation error, every program must be examined first to see if dates are used in this way, and, if so, then the logic changed accordingly. Furthermore, every data base must be changed to expand the year portion of the date field from two to four digits in order to include the century number.

Another aspect of the problem that is far more difficult to analyze and assess is the impact at the personal computer (PC) level. Staff has tested a number of systems in the City and found two problems. First, some PC's have logic chip problems with the internally stored date when changing to the Year 2000. As a test, we set the internal clock date to December 31, 1999, at 11:59:00 PM. When the system clock reached 12:00 AM, the date was erroneously set back to the default date of January 4, 1980. This condition will be a particular problem when a PC is used as a network server, e.g., Animal Control, Automated Purchasing, etc., or where a PC supports a departmental application using the system date.

The second PC problem is similar to the Year 2000 problem previously cited for legacy systems. While a PC may be capable of handling a date after 1/1/2000, an application/data base may not. This problem exists for in-house developed as well as purchased applications, e.g., LOTUS version 2.0 is not capable of working properly with the Year 2000.

As a result of these two problems, with the logic chip being the more serious, staff estimates the need to replace approximately 700 personal computers and numerous software packages prior to July 1999.

RECOMMENDATIONS

Staff recommendations are grouped into four areas: (1) Payroll/Personnel, (2) Police CAD, (3) PC hardware/software, and (4) Other Systems. Following the summary of recommendations for the Payroll/Personnel and CAD Systems (No. 1 & No. 2), a procurement methodology section has been included summarizing acquisition recommendations.

(1) Payroll/Personnel

Staff should immediately begin the process of selecting and implementing a new Payroll/Personnel System. The estimated cost for this project is approximately $1 million.

Selection of a new Payroll/Personnel System must take into consideration the following key factors:

—The system must be flexible in order to meet the City's payroll rules.

—The system must be part of an integrated suite of software that includes other financial systems.

—Given the short time line for successful implementation, the rapid procurement methodology outlined in recommendation No. 3 below should be followed.

(2) Police CAD

Staff should immediately begin the process of selecting and implementing a new Police CAD System The estimated cost for this project is $300,000 to $500,000.

A major consideration in the Police CAD project should be interoperability with the Police Records Management System. The project must also use the rapid procurement methodology outlined in recommendation No. 3 below.

(3) Procurement methodology for the payroll/personnel and police CAD systems

The time frames required to implement these systems are too short to use a formal bid or Request for Proposal (RFP) process. Therefore, staff recommends using a three-step methodology proposed by the Purchasing Division combined with an SMS cross-functional team. The steps in the process would be as follows:

For the Payroll/Personnel System, select a cross-functional team with representation from the Office of Personnel Resource Management, Office of Budget & Finance, Risk & Retirement Administration, City Auditor, and OCIS to run this project. For the Police CAD System, select another cross-functional team with representation from appropriate work units.

Each team would then be responsible for completing the following steps:

—Define major systems requirements including a high level check list of major functions to be incorporated in the system. Document the requirements. Develop a complete project plan outlining all steps in the process, responsibilities, and time frames.

—Conduct a survey of available systems using an informal RFP process. Attention should be paid to any selection processes recently completed by other agencies such as the City of San Jose, Oakland Unified School District, and the Port of Oakland. Evaluate each potential sys-

tem's capability against the requirements and using various types of interviews, presentations and ratings, select a preferred vendor.

—Negotiate an agreement with the preferred vendor for purchase and implementation of the system. Present the final recommendation to the City Council for approval of the contract.

(4) PC hardware/software

The City should establish a policy immediately requiring that all new personal computer systems and software purchases be Year 2000 compliant.

Each Agency should inventory all personal computer hardware and software and assess Year 2000 compliance no later than January 1, 1997. After completing the inventory and assessment, each Agency is responsible for developing a system replacement schedule to meet their needs.

(5) Other systems

OCIS staff will develop and implement a detailed work program illustrating how each of the other systems, not specifically addressed in this report, which require Year 2000 modifications, will be changed to meet the processing requirements of each system.

If there are potential resource conflicts, OCIS staff will formulate a proposal to resolve the resource conflict using outside services.

[ATTACHMENT C]

CITY OF OAKLAND
Agenda Report

TO: Office of the City Manager
ATTN: Craig G. Kocian, City Manager
FROM: Avon Manning, Director, Administrative Services Agency
DATE:December 10, 1996
RE: IMPLEMENTATION OF THE YEAR 2000 CONVERSION PROJECT

SUMMARY

On January 1, 2000, many information systems around the world will either fail or not function properly. This is not a trivial issue, but a serious problem which, by some estimates, will cost American businesses more than $200 billion over the next four years. This is an informational report intended to acquaint the Council with the year 2000 problem as it applies to the City's business systems and computer equipment.

BACKGROUND

The dilemma generated by the Year 2000 problem has three parts:

1. At the time many applications and systems were developed, computer storage was limited; therefore, dropping redundant data whenever possible saved valuable storage space. Consequently, the first two digits of the century designation were not included and many software programs currently in use assume that all dates begin with "19" and use only two digits to denote the year, such as "96" for the year 1996. Accordingly, the year 2000 will be interpreted by these programs as the year 1900.

2. Since systems developers did not anticipate that programs written in the 1960s, 1970s, or even the 1980s would still be in use as we enter the 21st century, some programs were purposely coded to interpret the numbers "99" and "00" in the year field as special control codes. In addition, some systems may not recognize the year 2000 as a leap year. As we move into a new century, use of the two-digit year, as found in many City systems will produce skewed data, generate unusable or unreadable screens and reports, or may cause systems to fail completely.

3. The final aspect of the Year 2000 problem exists at the personal computer (PC) level. Most PC's will have logic chip problems with the internally stored date when changing to the Year 2000. When the internal clock reaches 12:00 am on January 1, 2000, the system will erroneously reset to January 1, 1980 or January 3, 1982. This is true even for some PC's acquired earlier this year. A second PC problem is associated with the inability of PC software programs to properly handle dates after December 31, 1999. For example, LOTUS version 2.0 does not properly handle Year 2000 dates.

The overall impact of Year 2000 should not be underestimated. The City is challenged with meeting year 2000 compliance objectives while avoiding major system failures and the possibility of failed mission critical applications. Specifically, the most serious Year 2000 impact facing the City is that the Payroll/HR system can

not properly generate paychecks after DECEMBER 31, 1998, due to the programming issues previously identified. In addition, many other application software programs and the majority of the PC hardware currently in use will not be operable as we move into the new century, i.e., past December 31, 1999.

The Administrative Services Agency's Office of Communications and Information Services has completed an initial study of over 92 systems in use throughout the City. An interdepartmental team has been established to guide and direct the Year 2000 Conversion project to bring computer equipment, desktop software, and department applications into compliance with Year 2000 requirements.

A detailed report is attached for presentation to the Finance and Legislation Committee, recommending a course of action the goals and objectives of the Year 2000 Conversion. The plan includes cost projections for staffing, department applications replacement and modifications, and desktop software and hardware. This high priority, mandatory workload comes at a time when the information technology needs of the City are expanding and resources have been significantly reduced and stretched. Consequently, staff's ability to support new technology and systems required by agencies and departments will be severely limited at a critical time. Therefore, staff must be back filled and subsidized with contractors and consultants.

In addition, the financial and budget systems' (FMS/BDS) audit report for the fiscal year 1994–95 by Deloitte and Touche recommended its replacement to a fully integrated, centralized system. Consistent with the OCIS information technology model, the payroll/human resources application and FMS/BDS need to be implemented as an integrated package with a payroll interface. By combining their requirements processes and purchase an integrated package the City's can better meet its financial, payroll, and human resources systems needs. A combined Proof of Concept or Request for Proposal for a new comprehensive package gives the City strong leverage to drastically reduce the overall cost of the financial investment of required software.

RECOMMENDATION

No Council action is recommended at this time; this is an informational report.

Respectfully submitted,

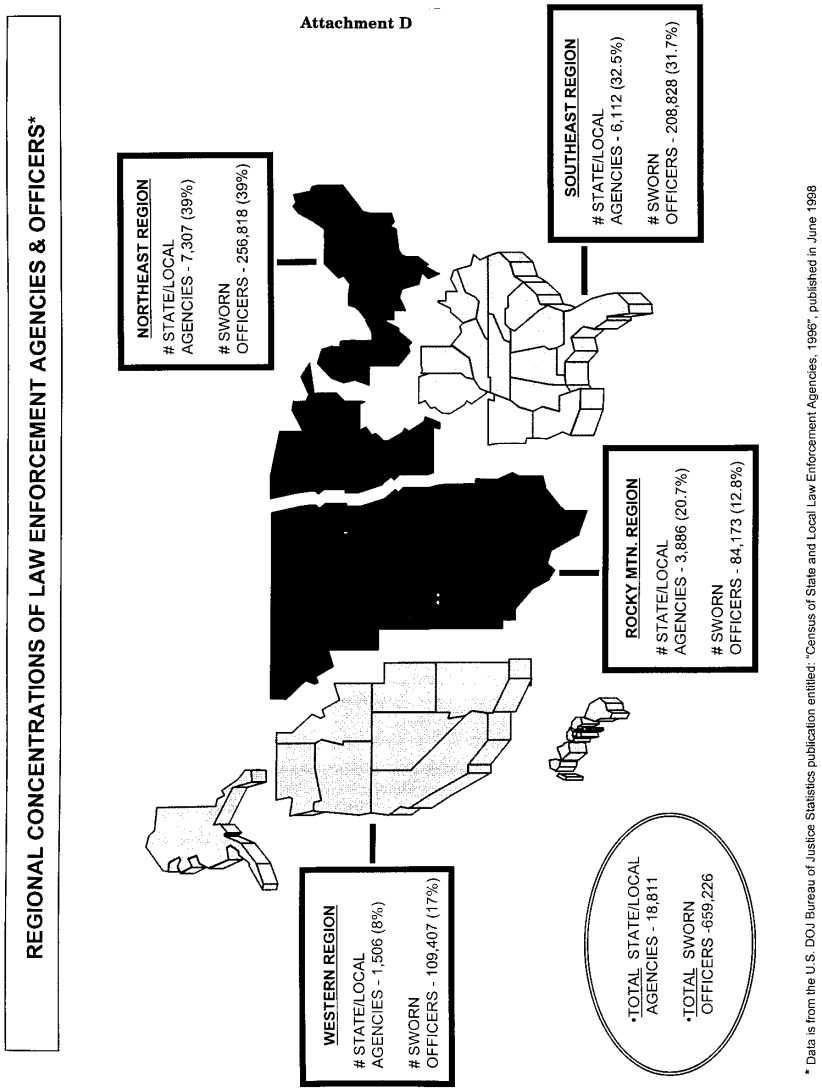
AVON G. MANNING,
Director Administrative Services Agency.

Prepared by:
MARILYN VARNADO,
Year 2000 Conversion Project Manager.

Approved for forwarding to the Finance & Legislation Committee:

———————————Office of the City Manager

Attachment D



STATEMENT OF ASSOCIATION OF PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-INTERNATIONAL

Founded in 1934, the Association of Public Safety Communications Officials-International, Inc. (APCO) is the world's oldest and largest public safety communications organization. Perhaps most widely known for standardizing, in 1936, the "10-codes" used by radio users for over 60 years, APCO is today recognized as the world's leading association on public safety communications issues. Most of its 13,000 individual members are state or local government employees involved in the management, design, and operation of police, fire, emergency management, emergency medical, local government, highway maintenance, forestry conservation, and other public safety communications systems. APCO serves as the Federal Communications Commis-

sion's (FCC) certified frequency coordinator for over 80 percent of the land mobile radio frequencies allocated for state/local government public safety use, and is the sole coordinator for public safety frequencies in the 800 MHz bands.

With the approach of the new millennium, attention from all sectors of business, industry and government has begun to focus on the Year 2000 (Y2K) Technology Problem. There are predictions of major catastrophes in everything from banks to electrical services. One area that cannot afford to have any type of system failure is this nation's public safety service providers. For this reason, APCO is committed to doing all that we can to assure that the public safety communications infrastructure this country depends upon will continue to function after December 31, 1999.

APCO has been working with the FCC to share our data and experiences regarding public safety communications and Y2K. APCO actively participated in the FCC's *Public Safety Year 2000 Roundtable* on June 1, 1998. We will be supplying the FCC with pertinent statistical data concerning the nation's over 20,000 Public Safety Answering Points (PSAP's) and Communications Centers in order to better coordinate the overall response to the Y2K issue.

Over the past few months APCO has done much to ensure that our members are aware of the potential problems that they could face due to Y2K. Each year, APCO hosts the world's largest Conference and Exposition devoted entirely to public safety communications. At this year's event held this past August in Albuquerque NM, seminars were conducted to address the myriad of Y2K issues facing public safety agencies to ensure consistent delivery of service. Our monthly publication The APCO Bulletin—*Public Safety Communications,* widely distributed within the public safety community, continues to publish articles describing Y2K problem identification and potential solutions. Copies of the articles *Protecting Public Safety Communications from the Year 2000* by FCC Commissioner Michael Powell and *Public Safety Preparation for the Year 2000: Dealing with the Y2K "Millennium Bug"* that appear in our October issue are attached. Special alerts and articles related to the Year 2000 problem have also been published in newsletters directed to APCO's leadership.

To further educate the public safety communications community, APCO has established a Y2K Forum on its Web site. This Forum is dedicated to allowing members to work together, sharing information and resources to help resolve their Y2K problems. APCO's web site can be found at: http://www.apcointl.org.

APCO is now designing a series of regional seminars specifically addressing Y2K to begin in early 1999. We are hoping to be able to conduct these seminars in conjunction with the National Institute of Justice and our sister public safety professional associations, targeting the chief officers and management level staff of law enforcement and other public safety first-responder agencies at the federal, state and local levels.

Public safety communications is the vital link between the public and those tasked to protect their lives and property; it is essential that this link remain functional. APCO is committed to ensuring that the delivery of public safety services is not disrupted by the Year 2000 Technology Problem.

CHRISTOPHER BEVEVINO, CAE,
Executive Director.

[From the APCO Bulletin, October 1998]

PROTECTING PUBLIC SAFETY COMMUNICATIONS FROM THE YEAR 2000

[By Michael K. Powell, FCC Commissioner]

In the last few months, much public attention has been drawn to the effects that the millennial date change will have on unprepared computers, intelligent systems, and microprocessor-controlled machines and appliances. At the Federal Communications Commission (FCC), we have been aware of the Year 2000 Problem or so-called "Millennium Bug" for several years because of our concern for the country's critical communications infrastructure.

We are particularly concerned about the integrity of the communications systems upon which police, fire, emergency medical and other public safety service providers rely to accomplish their all-important missions. Although it appears that conventional radios and radio systems are generally not at risk for Year 2000 failure, the same cannot be said of many computer-aided dispatch systems, records management systems, control systems, trunking systems, or electronic security systems. In addition, public safety agencies must be prepared for possible disruptions in transpor-

tation service and even electric power service to their agencies and in their communities that may occur at the turn of the century.

Many public safety service departments nationwide have already acted to prepare for the Year 2000 Problem. Yet, we are concerned that some public safety entities, particularly smaller or rural agencies without the personnel, technology and financial resources available to larger agencies, may not even now realize the seriousness of the problem and may not have begun taking the necessary steps to prevent system disruptions.

With fewer than 500 days to January 1, 2000, it is apparent that no public safety agency can afford to put off attending to this issue. Often we hear that Year 2000 remediation efforts are hindered by the notions that "it's someone else's problem," or that an eleventh-hour magic pill will be developed to fix the problem.

Unfortunately, there are no magic or universal solutions. America's public safety entities and the communications systems upon which they rely must not only make sure that they themselves will be ready for the year 2000, but must also be prepared to help others address the emergencies and public service disruptions that this problem may cause in their communities.

While the measures necessary to address the millennial date change problem (and other similar computer date change issues of which we are all becoming aware) frequently reach well beyond the communications jurisdiction of the FCC, we do take very seriously our responsibility to alert the entities we license and regulate to the various aspects of this problem and those interrelationships that can also affect other mission-critical aspects of public safety service providers.

As a consequence, we strongly encourage public safety service providers to use all available resources to develop a comprehensive picture of the potential impact of computer date change problems on every aspect of their operations. Many manufacturers have already done mass mailings to apprise customers of their Year 2000 efforts, have set up special Internet sites that list compliant and non-compliant products, and have created 24-hour telephone support hotlines.

Establishing an open dialogue with these, and other, equipment suppliers and manufacturers can be very helpful.

In addition to developing a comprehensive understanding of the effects of date-related changes on all of their operations, departments should also develop a readiness program to troubleshoot potential problems and examine all mission-critical systems. Such a readiness program should include complete audits of all critical systems, careful remediation of each problem identified, thorough testing of each solution, and the formulation of contingency plans that includes the acquisition of those resources that will be necessary to address the contingencies that have been identified.

The FCC has established a Year 2000 Task Force to coordinate internal Year 2000 compliance efforts and to assist the communications industry on this issue. The FCC's Year 2000 website at <www.fcc.gov/year2000/>, serves as an information resource on the Year 2000 Problem and telecommunications, including public safety communications. The FCC is also an active participant on the President's Council on Year 2000 Conversion. The efforts of this government-wide group are described in detail on the World Wide Web at <www.y2k.gov>.

Finally, the FCC is working closely with other Federal departments and agencies, including the Federal Emergency Management Agency (FEMA) and the U.S. Fire Administration (USFA). In that regard, the USFA has developed informational materials, along with a self-assessment process for determining if a computer system is Year 2000-ready, that is posted at <www.usfa.fema.gov/y2kfaq.htm> and <www.usfa.fema.gov/y2kcom.htm>, respectively.

The challenge of implementing public safety Year 2000-readiness rests with public safety managers and officers, including police, fire and emergency medical and emergency management departments, nationwide. Time is of the essence. We cannot extend the Year 2000 deadline. Our national well-being literally depends on the reliability of public safety services and the communications networks that support them.

The FCC is committed to taking whatever actions it can to assist public safety agencies across the country in this important effort.

[From the APCO Bulletin, October 1998]

DEALING WITH THE Y2K MILLENNIUM BUG

[By John Powell and David Buchanan]

If the predictions of computer system failures in everything from automobiles and ATM's to the IRS to traffic signal controls and a plethora of other systems that support everyday life are even partially realized, the overload on public safety services will be tremendous.

The "bug" is insidious, potentially impacting anything with a microcomputer chip—anything that has a keypad or timer, displays a date, stores numbers, or performs calculations. Consider for a moment the possible loss of a few personal items: digital clocks and wristwatch, automatic coffee maker, camcorder, home alarm system, pager, personal computer, radio, telephone, television, thermostats, VCR, and last (but certainly not least) access to ATM's, financial records, and retirement income (if you're lucky enough to have it)!

Couple these potential failures for millions of people with increased turn-of-the-millennia activity and the impact on public safety services could be crippling. The last thing public safety agencies will then want to contend with is problems with their own operational systems.

How big is the overall problem? After reviewing published documents and interviewing a number of Y2K experts, Silicon Valley Tech Week concluded in its April 13 issue: "None of the mission critical sectors in the U.S. are even close to being Y2K compliant, say the experts. Not the 9,000 electric utility plants. Not the 11,000 banks. Not the telecommunications companies. And certainly not the U.S. Government."

Tim May, the retired Intel physicist who discovered the damaging effects of nuclear radiation on computer chips, concluded, in the same issue of Silicon Valley Tech Week: "* * * financial collapse will occur when investors wake up and realize what's coming. July 1, 1999, is the start of the IRS fiscal year 2000. The IRS won't be able to process W2s and 1099s at that time. It has 100 million lines of code and isn't even awarding a Y2K conversion contract until October 1998. Jan. 1, 2000 may be an opportunity for terrorists, millennium fundamentalists, and others out to take advantage of a weakened infrastructure."

IRS Commissioner Charles Rossotti told the Wall Street Journal: "If we don't fix the century-date problem, we will have a situation scarier than the average disaster movie you might see on a Sunday night."

In the April 22 edition of the Wall Street Journal, Rossotti was quoted as saying, "Twenty-one months from now, there could be 90 million taxpayers who won't get their refunds, and 95 percent of the revenue stream of the United States could be jeopardized."

There are, however, other dates both before and after Jan. 1, 2000, that also must be considered. These include:

Jan. 1, 1999: Many spreadsheets and financial applications look forward during the current year and will see the next year ends in "00". Those functions that examine a date range may not be able to handle an ending date ("00") that is lower in value than the current date ("99").

Aug. 22, 1999: GPS rollover (reset to zero). GPS is now the most widely used system for public safety person/vehicle location applications. Beyond this fundamental application are other telecommunications uses, not the least of which is serving as the common time base for synchronizing transmitters in wide area simulcast systems, including most of the nations large commercial paging operations. In addition to geopositioning and telecommunications applications, GPS is used in major banks and thousands of financial institutions for accurate date and time recording and synchronization.

Sept. 9, 1999: "Nines end-of-file problem" in legacy systems using 9999 in the date field to denote "end-of-file" (EOF). Most of these programs are mainframe-based, written in high-level computer languages such as COBOL. Pubic safety applications include large Criminal Justice Information Systems and motor vehicle/drivers license systems.

Feb. 29, 2000: Not a normal leap year (rule: if the year is divisible by four but not divisible by 100, or if the year is divisible by 400, it is a leap year). Many computer programs perform the first two tests (divisible by four, but not divisible by 100) but do not include the last test. Those that do not will be off by 1 day from March 1 through Dec. 31, 2000.

Public safety decision makers need to begin planning for the potential problems that could be caused by major failures in electrical utilities, wireline and wireless telecommunications systems and financial institutions, among others. At the same

time, they need to ensure that their own critical systems will survive the Y2K date crisis and will remain operational despite failures of other major systems such as electrical utilities and the telecommunications infrastructure.

THE BOTTOM LINE

If there is the potential for everything else failing, then the one thing that absolutely cannot fail is the provision of public safety services. Key to the survival of public safety services is receiving emergency calls from the public and relaying those calls for service to units in the field.

THE PIECES TO THE PUZZLE

There are several levels of systems that are potentially impacted by the Y2K "bug." In general they are:

Legacy firmware-based systems: Difficult or impossible to upgrade, but probably not critical unless validating date ranges, these systems are extensively used in process control application, including traffic signal light controls, elevator controls, and stand-alone access control systems. Early stand alone systems (access control, for example) had sufficient read-only memory (ROM), but limited random access memory (RAM). Programmers went to great lengths to preserve RAM. Many such systems are still in use! Formats were designed to store dates in a manner that permitted rapid mathematical manipulation. The most common (YYDDD or YYMMDD) require 2 bytes (16 bits) for a 2-digit year code. Application and report generating programs using date ranges (for age, access card validity, etc) cannot function across a century boundary if they use a 2-digit year code.

Firmware-based systems also include most of the home electronic items mentioned at the start of this article: alarm systems, digital clocks, wristwatches, automatic coffee makers and similar appliances, automatic setback thermostats, pagers, radios, "smart" telephone sets, televisions, camcorders and VCRs.

Mainframes: Getting much of the attention, but usually programmed in higher level languages such as COBOL making updates easier, these systems include many federal/state CJIS-type databases.

Mini-computers: More difficult to update because code is often written in lower level languages such as C++ and optimized for speed, these systems include message switches and older and/or larger CAD/RMS systems.

Personal Computers: Finally, PC-based workstations are a common main-machine interface to many 9–1–1 and alarm reporting systems, computer aided dispatch (CAD), dispatch consoles, records management systems (RMS), telecommunications and trunked radio switches and a host of related systems. E-mail systems in LAN, Intranet, WAN and Internet applications link personnel and off-site facilities. Mobile data terminals (MDT's) are a thing of the past; the new game is mobile computing terminals (MCT's) based on PC architecture.

Within the personal computer, there are multiple levels to be addressed:

Hardware BIOS: More than 90 percent of PC's built before 1997 have a bios-level problem. Many of these should be easy to fix.

Operating Systems: Nearly all OS vendors are now addressing date handling problems with patches or the release of compliant upgrades.

Applications Software: Many software packages still have a two-digit date problem. A test of 5000 general software packages found 64 percent had some problem.

Data Within Single Application: Most databases and spreadsheet applications have 2-digit dates.

Data Shared Between Applications: Applications may make different "guesses" about the 4-digit year when encountering 2-digit year fields.

At least two software packages are available to evaluate Y2K date compatibility of personal computers. Y2000 is available for Internet download at no cost from National Software Testing Labs (www.nstl.com/downloads/y2000.exe). Y2000 downloads as a zip file containing the executable program and a Read me text documentation file. The program tests hardware and BIOS for proper Jan. 1, 2000 rollover; it also checks for proper leap year calculations for the years 2000 through 2010.

Another program, Check2000, is available at modest cost from most software suppliers. Check2000 performs similar hardware/bios testing to Y2000, but continues with more in-depth testing, reportedly checking some applications software as well.

PUBLIC SAFETY TELECOMMUNICATIONS

FCC Chairman William Kennard, being questioned by the U.S. Senate, concluded, "[I am] * * * concerned that the year 2000 problem has the potential of disrupting communications services worldwide * * * . Every sector of the communications in-

dustry—broadcast, cable, radio, satellite, and wireline and wireless telephony—could be affected."

Two "wakeup calls" this year highlight our dependence on these critical telecommunications services. During the week of April 13, AT&T lost its entire frame relay network for 24 hours. The failure was caused by a software glitch in a network circuit card that was being loaded with updated software while still connected to the network. 6600 customers, including major financial institutions and their ATM/credit card networks, lost service. Then on May 19, Hughes Corporation's Galaxy IV satellite failed, disrupting paging service to millions of paging receivers, including critical notification systems used by federal, state and local public safety agencies. Automated teller, point-of-sale and other VSAT-based services also were disrupted.

Recognizing these potential problems, FCC Commissioner Michael Powell convened a Public Safety Year 2000 Roundtable on June 1 in Washington, D.C. Panel members included a number of state/local public safety officials, as well as representatives from federal agencies, public safety equipment manufacturers, and consultants dealing with the Y2K problem.

Interestingly, all of the consultants agreed there is a quite straightforward process to be used for equipment evaluation. The recommended steps include: equipment inventory, analysis for problem potential, manufacturer/vendor inquiry and certification, testing (independent or in-house), correction or replacement of non-compliant systems, and re-testing. A critical recommendation was the testing of all components of a system operating together as a final test once corrections have been made. Use "IVE"—independent verification of everything!

The consultants further agreed that in some cases the cost, both in time (or lack thereof) and money, is leading agencies to replace systems rather than attempt to upgrade an existing investment. In fact, many agencies are using the Y2K bug as an opportunity to perform much needed replacements of outdated systems.

Equipment manufacturers present were primarily from the land mobile radio community. Several indicated their public safety equipment lines are so new that the problem was addressed in the initial design. Others, including Ericsson and Motorola, said they have some embedded equipment that may be impacted and offer information on determining Y2K compliance of their equipment on their Internet web sites. In particular, Motorola provides a search engine that allows access to information on Y2K compliance of their equipment in 3 categories: tested and passed, tested and did not pass (with additional information provided), and not yet tested. Unfortunately, Motorola has more recently stated some older equipment, primarily in the high-level encryption arena used by federal agencies, is not compliant and will not be updated.

The best general news from this Roundtable is the Y2K bug will not impact most conventional radio dispatch equipment (radio system infrastructure and field subscriber units). However, some radio system management equipment and software (report generators, etc) may need upgrades, particularly for trunked radio systems. Unfortunately, the same is not necessarily true of other critical public safety software such as computer aided dispatch (CAD) and records management (RMS) systems.

A CASE STUDY

San Bernardino County, California

San Bernardino County, California, encompassing 20,080 sq. miles, is the largest county in the continental United States. It has a resident population of 1.6 million people. The county contains the Mojave National Preserve, Joshua Tree National Park, the San Bernardino National Forest and many recreational areas along the Colorado River. The county also is home to the U.S. Army's National Training Center at Ft. Irvin and the Marines—29 Palms Air/Ground Training Center.

San Bernardino County's radio system is an 800 MHz integrated Motorola SmartNet II trunked/conventional system serving more than 130 public safety and public service agencies and departments. It provides interoperability with several state and federal government agencies. There are more than 10,000 mobile and portable radios on the system. Currently, 26 sites are used to provide coverage, with new sites being added each year.

The county's microwave system has four DS3 loops with many spur routes. This system supports data, radio and telephone transport throughout the San Bernardino County.

San Bernardino County also operates a 900 MHz paging system with 2900 pagers and 26 sites. This paging system is the primary fire dispatch alerting for many of

the county's fire agencies. It also provides administrative and operations paging for most county and city agencies.

San Bernardino County's Y2K Team developed a comprehensive test and evaluation plan. Similar to the steps recommended in the FCC's roundtable, the steps in their plan included:

—Completing an inventory of all models and versions of equipment used in radio, microwave and telephone systems.

—Evaluating equipment to deter mine which was not Y2K impacted (equipment without microprocessor chips, primarily older radio equipment).

—Contacting all manufacturers and asking for certifications of Y2K compliance. In some cases this was obtained from the Internet. The methodology that each manufacturer used to determine Y2K compliance was also solicited.

—Conducting in-house testing based on the manufacturer's methods and/or locally developed methods.

As a parallel effort, the county's information services is independently testing all PC's for Y2K compliance. Because all dispatch consoles are PC based, this is critical. There is a known problem with the Microsoft Windows NT operating system used in many of these applications. Microsoft has promised a fix within the next few months.

San Bernardino County's findings parallel those of the consultants and vendors who made presentations at the FCC roundtable. Generally, these are:

—All microwave equipment is Y2K compliant as there are no date specific functions in the firmware/programs.

—With the exception of the PC-based consoles mentioned earlier, nothing has been found with the radio system infrastructure or subscriber units that would disrupt system operation; however, system management functions will be impacted.

—Some radio system trunked management computer programs require an upgrade.

—Telephone systems are still under scrutiny and will probably require some upgrades.

As this article went to press, a detailed analysis of the San Bernardino County Sheriff's CAD system found major changes would be required to bring the software into compliance. It is probable that it will be most cost effective to replace the CAD system; this option is receiving careful consideration.

BE PREPARED!

As with any disaster, public safety personnel will only be effective if they have prepared themselves and their families in advance. Year 2000 is inevitable; personal preparation is essential. What can you as an individual do to prepare? Suggestions include:

IVE: Test all of your important home appliances by resetting the dates and allowing them to roll over the century and leap year dates. If you live by your PC as we do it should be at the top of the list, especially if you use it for on-line banking, financial management, or e-mail communications with your office. Consider buying a small electric generator to support critical home electrical needs if power fails; remember to stock up on fuel in approved storage containers during December 1999.

Banking and other financial services systems are linked in huge international networks where a single failure could cause network-wide problems. While the large banks, brokerage companies, mutual fund houses and stock markets state that they will be ready, smaller institutions without the fiscal and technical resources to properly address the problem may pose a higher risk. Correspond with your institutions and obtain written assurance that your data and your money will survive; then make sure you keep written copies of all account statements!

Credit card processing has already experienced snags as cards with expiration dates beyond 2000 encounter non-compliant processing equipment. Again, maintain copies of your account statements. Check them carefully and be prepared to dispute inaccurate bills.

Delays in clearing checks (including pay checks) are predicted. A number of Y2K "experts" are recommending keeping significant cash (up to two months worth) on hand as 2000 approaches.

Insurance policies and mortgage documents face similar problems. In both cases, obtain written documentation of coverage extending beyond 1999. For mortgages, it is important to obtain a lender-issued statement detailing payments (interest and principal) already made, as well as an amortization schedule showing payments during 2000 and beyond in case the lender's computer system is unable to issue payment coupons. Both institutions will still expect their payments to be sent!

Finally, but perhaps most importantly, is ensuring that you will continue to receive income from your employer or retirement system. Take an interest in your agency payroll systems and offer advice and assistance as appropriate; all of us are dealing with the same problem!

The Social Security Administration has been working on Y2K compliance for a number of years and should be ready for Y2K. Unfortunately, as stated above, some other federal government agencies (including the U.S. Treasury) that must work with Social Security are far behind. Since many public safety agencies participate in local or state retirement systems, it is important each maintain detailed records of our account(s) and be prepared for disruption in payments if you are fortunate enough to be retired.

CONCLUSIONS

Clearly the Y2K problem poses significant risk, both internal and external, to public safety agencies and to the general public. Furthermore, determining compliance can require significant time and resources. Correcting problem systems could require significant financial investment, up to the cost of replacing entire systems. Recommendations made at the FCC roundtable included:

—Encouraging all users to develop and implement identification and test procedures similar to those used by San Bernardino County.

—Thoroughly testing critical telecommunications systems off-line NOW. Take advantage of new/spare computers by copying current live data, and then resetting the date to observe the rollover.

—Encouraging manufacturers to develop web sites that list hardware and software (by version number) that have been tested and found to be compliant.

—Establishing an index on the FCC's web site with direct links to the manufacturer's Y2K web sites.

Finally, don't plan on getting any time off from work to celebrate the millennium!

PREPARED STATEMENT OF BRUCE ROMER

Good morning, Senator Bennett and members of the committee, I'm Bruce Romer, Chief Administrative Officer for Montgomery County, Maryland, and Chair of the Metropolitan Washington Council of Governments' CAOs Committee. I am here today, also representing the National Association of Counties (NACo). It is my privilege to meet with you today and thank you for the invitation.

Montgomery County, Maryland has a population of approximately 840,000 citizens and an annual operating budget of over $2 billion which ranks it sixth among the nation's counties in operating revenues. Montgomery County is one of three counties with a AAA bond rating from all three rating agencies. The County spends almost $100 million annually on technology, is highly invested in it and depends on technology to achieve its mission. Earlier this year the County was honored to accept the 1998 National Association of Counties (NACo) Annual Achievement Award for its Year 2000 program.

We in Montgomery County consider the coming of the Year 2000 as a very serious and significant problem. This so-called Year 2000 or "Y2K" Glitch when computers may fail to recognize "00" (zero-zero) as the Year 2000 is more than just a technology problem; we believe it constitutes a business management problem of enormous proportions competing for precious local government resources. If not fixed, this problem threatens public safety, emergency response, health and human services, finance, taxation, permitting, and even the operation of traffic management systems. In combination, problems in these areas could lead to challenges for public safety organizations, stoppage of critical services, loss of revenue, and enormous potential litigation costs.

In 1995–1996 Montgomery County formulated a plan to resolve its Y2K problem by December 31, 1998, with the entire calendar year 1999 reserved for contingency planning and testing. This included the establishment of a participative management and communications structure including a Project Office for a County-wide program in an otherwise independent and autonomous multi-agency enterprise. Montgomery County's agencies include general government, public schools, community college, parks and planning, water and sewer, revenue authority, and the Housing Authority. The County's Year 2000 Compliance Program Timeline is shown on Display #1 and is included in Attachment #1. The County's Year 2000 Decision Structure is shown on Display #2 and is included along with the County's website address in Attachment #2. We have been working diligently to manage the effects of the Year 2000 problem on the County and its citizens. In the process we have gained significant experience and knowledge which we have shared with other local

jurisdictions under the auspices of the Metropolitan Washington Council of Governments (COG). This information is contained in Year 2000 Best Practices Manuals (Attachment #3) produced by the COG's CAOs Committee of which I am the chair.

After almost two years of intense efforts, the County finds itself in a unique position. Through its comprehensive multi-agency, multi-phase, multi-platform effort, the County has identified over 200 systems that are the focus of its Y2K program. These systems—spread over seven agencies—were carefully assessed; prioritized through a rigorous triage process (see Attachment #4 for the County's triage process); are being remediated through repair, replacement, or retirement; tested; and must be certified to be ready to operate properly in the new millennium. For its Y2K efforts, the County has appropriated approximately $35 million to date, allocated significant staff resources, and passed special legislation to adopt fast-track administrative processes in areas such as procurement and budget. See Display #3 for the Appropriations Summary (Attachment #5).

The County's most recent list of projects identifies 204 registered projects as shown in Attachment #6. The categorization and status summary are regularly monitored. Examples of these projects are shown in Display #4 (also Attachment #4) which include E–911 Emergency Dispatch, traffic management, academic computing, building permitting systems, fueling systems and point-of-sale systems for the County's liquor sales. See Display #5 for a Systems Status Summary which is also shown in Attachment #7.

Recently, the County's program has expanded to four concurrent phases, namely: systems compliance and certification, business continuity assurance, contingency planning, and community outreach. (See Attachments 8, 9, 10 and 11, respectively, for documentation developed by the County for each of these phases). The community outreach program was most recently initiated when County government hosted all the County's municipal governments for a Y2K session (see Attachment #11). A meeting of the Chambers of Commerce is planned next. The County has also extended its previously strong regional role in emergency preparedness to Y2K. The County's Emergency Management Group (EMG) is expected to conduct a Y2K disaster exercise sometime in early December.

A continuous review of the program is conducted by committees of top managers from the Executive and Legislative Branches of government. See Display #6 for a Scorecard used by the County's Y2K Policy Committee to de-bottleneck projects. (See also Attachment #12 for a copy of the Scorecard and a sample internal memorandum dated October 22, 1997, from me to the County's Executive Branch department heads establishing Y2K responsibility and priority). All this is necessary in order to ensure that essential services will be available to our citizens in the coming months. Having done this much—and finding more to do everyday (such as embedded systems which are much more difficult to identify and assess)—I admit that this is a real strain on the $2 billion enterprise that is Montgomery County, Maryland. But any one municipality alone cannot assure the success of a region or the nation. NACo will continue to work with the counties to find appropriate remedies to assist them with their compliance efforts, meanwhile, this is a matter of grave concern to NACo and poses a major problem for the entire nation.

While the national media has done a good job of highlighting the challenge of remediating 7,343 critical Federal systems, the local challenge of addressing Year 2000 is less well understood. With local governments responsible for providing so many direct services to the nation's citizens, any failure of local government services will hit much closer to home for each of us.

As you may know, local government, in total, is larger and more dependent on information technology than the Federal government. Local Governments including municipalities, townships, school districts, and other jurisdictions, total as many as 87,259 in number. Federal government employment totals 4.2 million, while local government employs about 12 million people. Likewise information technology spending for the Federal government in 1997 was $28.6 billion compared to state and local government IT estimated spending of $41.9 billion. Clearly, while the Federal challenge for the Year 2000 is sizeable; the local governments' Year 2000 challenge is even greater.

How are we in the Washington region governments attempting to deal with Y2K related issues beyond our jurisdictional boundaries? The COG is providing regional leadership and coordination. COG's 17 member jurisdictions have identified the following six critical interlocking functions that must be assessed in order to codify region-wide contingency planning assumptions for Y2K preparedness: Utilities, Public Safety, Public Health, Transportation, Business/Commerce, and Communications. Through a division of labor, member jurisdictions are expected to complete an assessment of their assigned areas by January 1999. Utilizing the auspices of the COG will improve the quality of the information provided by those surveyed, assure

information confidentiality and improve the economy of effort through coordination. In many respects the COG and Montgomery County Y2K programs may potentially serve as models for the nation.

Problem solutions are normally preceded by a period of awareness, knowledge-transfer, discussion, and dialog. But that discussion and dialog must do more than just "admire the problem." We believe that five key elements, supported by Congress, could significantly enhance the Nation's understanding of, and attack on, Y2K. These are:

1. Establishment of a FEMA-like National Y2K Emergency Fund to help finance local governments' Y2K remediation and contingency planning efforts. The attached proposal (Attachment #13) recommends that Congress immediately appropriate $7.3 million to facilitate the efforts of the National Capital Region. If this region is not ready, the ability of Federal Government to function will be seriously impacted. The proposed Y2K fund will finance Y2K initiatives in each of the six functions identified by COG as listed above. This includes $5 million required immediately for the regional transportation infrastructure managed by WMATA and efforts to extend Montgomery County's Y2K disaster preparedness model to the National Capital Region.

Another $1.5 billion should be appropriated as seed funding for the other local governments to apply the best practices developed by the National Capital Region. The NACo through its Public Technologies, Inc. (PTI) relationship would serve as the vehicle for providing programmatic assistance to the nations 3,069 counties. At the same time NACo would assist the federal government by proposing application and eligibility rules for the Y2K fund.

2. Passage of immunizing legislation to allow known Y2K information to be shared without fear of lawsuit and to hold responsible public and private officials harmless against the threat of crippling litigation. Current efforts of the House of Representatives in this regard should be accelerated in order to encourage timely availability and sharing of objective information without fear of litigation. The immunizing legislation should not, however, relieve any party from negligence or deficient Y2K work quality.

3. Establishment of a National Y2K Program Office to complement the efforts of the President's Y2K Advisory Council. The focus of this office will serve to aggregate and disseminate information to local governments. It will also be key in providing national coordination to all regions while they plan for Y2K; it will also provide status reports on Federal efforts to mitigate Y2K risk to regional and local systems.

4. Formation of a National Y2K Help Desk available to all local municipalities for best practices and compliance information from nationally maintained databases and assistance regarding Y2K contingency planning.

5. Affirmation of continued Congressional leadership to highlight Y2K local government issues and solutions.

Other actions which Congress could take may include:

—Organizing and executing at least one National Y2K Day, where normal business is set aside as much as possible and Y2K solutions are tested, documented, and reported for the common good before January 1, 2000.

—Instituting a National Y2K Internet Web Site devoted to the responsible discussion of local Y2K issues and solutions thereby encouraging inter-governmental information exchange.

—Producing and promoting a series of professional, compelling, high-quality TV documentaries about local Y2K issues and solutions and their impact on local government services. This will supplement the work already done by NACo, ICMA, NLC and PTI in their program titled "Y2K and You." This would also supplement the proposed National teleconference seminar scheduled to air on October 7, 1998, to 47 local sites.

—Disseminating tool kits or "How To" manuals such as those published by the COG (see Attachment 3) which help local government officials identify the steps they need to take to address Y2K issues.

Looking at just one of the recommendations, a National Year 2000 Program Office, to complement the efforts of the President's Y2K Advisory Council, the Federal government can provide local government with much needed Y2K data aggregation and coordination. A large amount of data is being generated, but local governments need help in accumulating, analyzing, and understanding this data. As an example, using the information gathered for the 34 functional categories currently monitored by the Y2K Advisory Council, a National Year 2000 Program Office could assist each region in ascertaining the readiness of area hospitals. Providers of critical emergency medical equipment are known to be lagging in the Y2K race. This information is essential in operating our local emergency medical systems. It can assist

in projecting the necessity of the efforts of the national guard to assist state and local law enforcement agencies; and provide input to a national "disaster" exercise on Y2K much like the one Montgomery County has planned for December of this year. The most critical functions are the performance of the electric utilities and health care systems and providing information on risk assessment to local governments. An office of this nature would be instrumental in promoting dialog among the 87,259 jurisdictions in the nation.

To ensure a community's economic stability through this difficult period, each local community needs a Y2K business continuity program to assure that business partners, suppliers, contractors, and vendors will still be in business after 12/31/1999. Montgomery County has such a program and is sharing much of its information with regional governmental bodies and business entities but remains concerned about potential litigation should reliance be placed upon its disclosures. The immunizing legislation mentioned above would go a long way toward allowing those who have accumulated regional supplier information to share that knowledge without fear of retribution.

Montgomery County recognizes its obligation to the community, not only as the local governmental entity having the duty to inform and protect the citizens and businesses within its immediate boundaries, but also as a partner in a larger regional community. Y2K failure in any County's power, transportation, health care, or communications infrastructure will have tremendous rippling effects on all neighboring communities.

A county has the obligation to repair and test all critical systems and processes to ensure that it can continue to deliver services and that local businesses can continue to operate unimpaired. Montgomery County is committed to undertaking special efforts to minimize the risk of failure to its community but, at the same time, to plan for the most likely regional failures. This means government should prepare to be the direct provider of services in the event the business community is disabled, such as in the distribution of food or water, should the local supermarket be closed or overrun. Contracted service providers must be on standby. A community contingency plan is as important as those we are developing for our automated systems.

The potential effect of Y2K on county governments nationally requires the redirection of resources and manpower to ensure the health and safety of citizens, to maintain law and order, to initiate action plans for the restoration of business-as-usual, while minimizing negative impacts. Planning contingencies are essential in the event of power outages, failure in water and sewer systems, traffic controls, and telecommunications to note a few. Community health, safety, and welfare are County governments' highest priority, and potential Y2K impacts in this area must be identified and mitigated in short order. NACo is doing everything it can to ease the transition to the next century.

The nationwide extent of Y2K failure is still unknown. But whatever it is, it will affect everyone at the same time and some earlier. The Y2K deadline is immovable. No silver bullet solution will be found. As I stated earlier, while many of the Nation's local governments are engaged in Y2K assessment and repair, many are very late in starting. For many counties, local resources are scarce and funding is critical to the success of Y2K repair efforts. This may prove to be one of our biggest obstacles. Awareness must be increased and every community must plan now, because we are running out of runway.

Lessons learned by Montgomery County lead us to offer the following advice to those who are just starting:

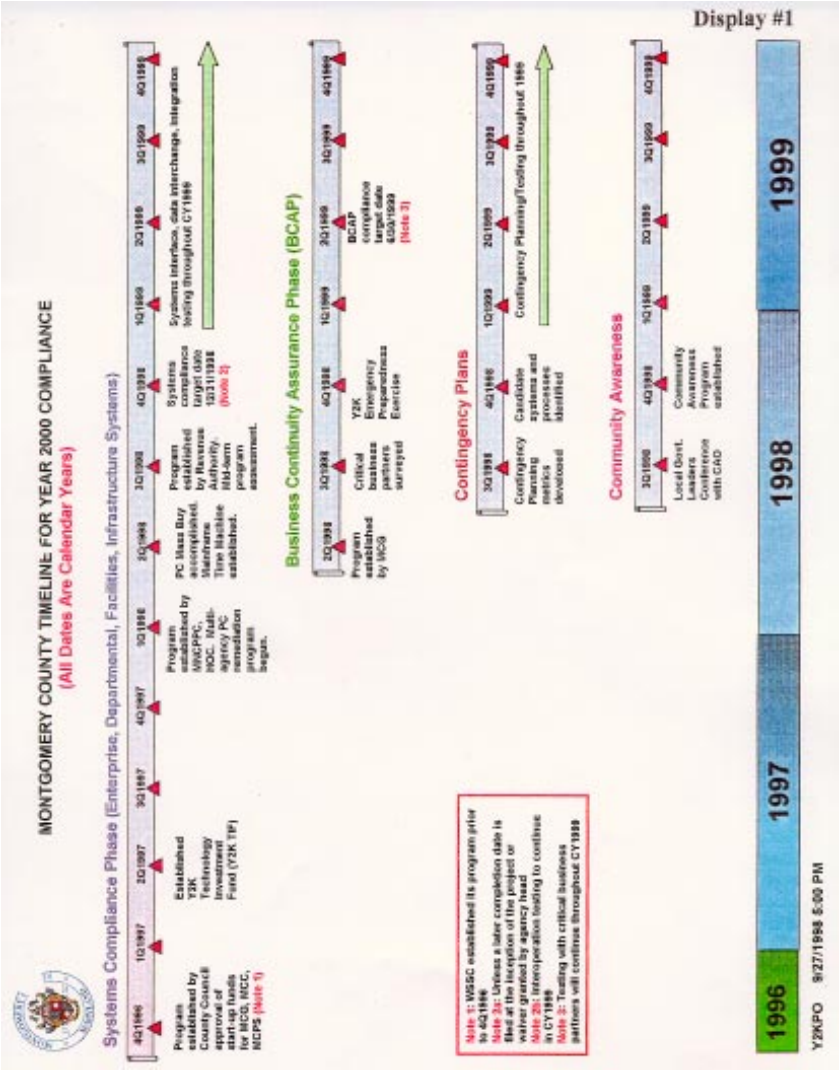
1. View Y2K as a business management problem, not a technical problem.
2. Insist on the highest level of executive leadership.
3. Make someone in your organization responsible for Y2K.
4. Consider suspending or postponing new, non-Y2K initiatives.
5. Make funding available; divert funds from current programs where possible; plan for uncertain buys.
6. Perform a full inventory, triage and prioritize.
7. Engender a sense of urgency; streamline procurement and budget processes.
8. Where possible, don't reinvent the wheel; adopt industry best practices such as those of the Metropolitan Washington COG.

Thank you, Senators, for your time and attention. I will be happy to answer any questions.

LIST OF DISPLAYS

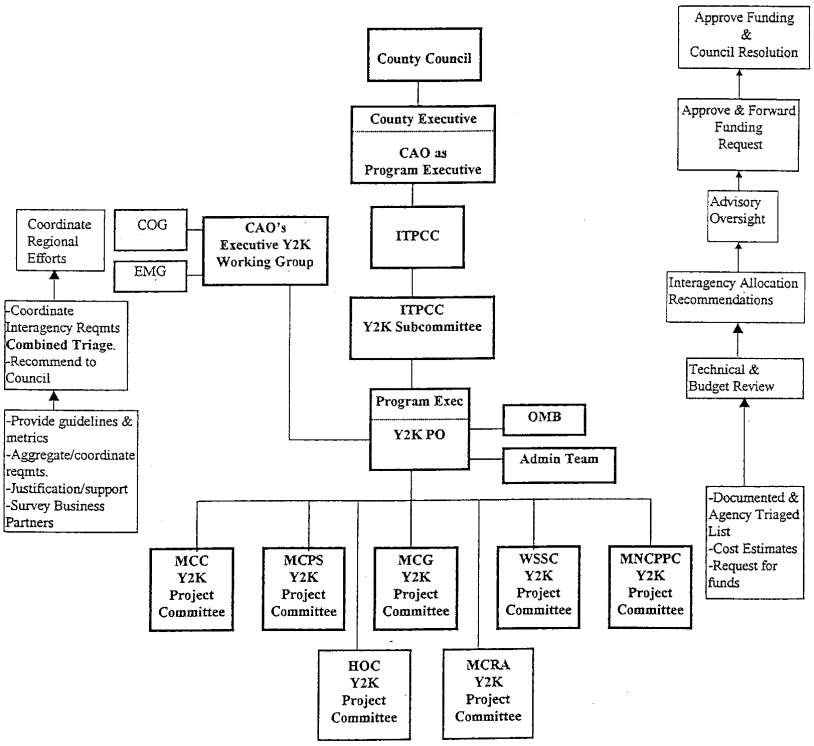
1. Montgomery County's Y2K Compliance Program Timeline
2. Montgomery County's Y2K Decision Structure

3. Montgomery County's Y2K Appropriations Summary
4. Examples of Montgomery County Projects by Categories
5. Montgomery County's Y2K Systems Status Summary
6. Montgomery County's Y2K Scorecard Report



Display #2

MONTGOMERY COUNTY, MARYLAND
YEAR 2000 DECISION STRUCTURE



Display #3

Montgomery County Year 2000 Program

Year 2000 Program Funding

(Appropriations - To Date)

Agency	Total ($ Million)
Y2KPO	3.0
MCG	6.7
MC	7.3
MCPS	15.8
MNCPPC	0.8
HOC	0.5
Total	34.3

Display #4

EXAMPLES OF MONTGOMERY COUNTY PROJECTS BY CATEGORIES

Y2K RISK RATING SCORE	CATEGORY	MONTGOMERY COUNTY EXAMPLES
45 points or greater	Highest-risk, mission-imperative	1) E-911 CAD Emergency Dispatch 2) Advanced Traffic Mgmt. System 3) Community College Academic Computing 4) Public Schools Student Info System
35 – 44 points	High-risk, mission-critical	1) Permits 2) Animal Control 3) Operating Budget/Capital Improve Process 4) PA/Bell/Fire Alarms
20 – 34 points	Medium risk, mission-essential	1) Security Systems 2) Inventory Control 3) Fuel Tracking
under 20 points	Lowest risk, mission-enabling	1) Road Inventory 2) Elevators 3) Air Quality

Display #5

Montgomery County Year 2000 Program

Systems Status Summary

	Assess	Remediate	Test	Implement	Complete	Total
Enterprise	10	20	6	4	10	50
Departmental	50	43	13	5	21	132
Infrastructure	2	1	1	3	3	10
Facilities/Fielded	4	2	1	3	2	12
Total	66	66	21	15	36	204

Display #6

MONTGOMERY COU' 'Y GOVERNMENT

Status of Year 2000 Projects

(with Report Validity Assessment)

Item # / Rank	System ID / Risk Rating	System Name	Project Status: Phase (Assess, Remediate, Test, Implement)	Project Status: Date Issues (Y=Minor Issues, R=Major Issues)	Project Status: Project % Complete (Last / Current)	Report Validity Assessment: Two Months Ago	Report Validity Assessment: One Month Ago	Report Validity Assessment: Current Month	Remarks
1 / 1	MCGE-0010e / 63	CAD	Remediate	Y	20% / 30%	5	5	5	Y2K test plan being developed.
2 / 2	MCGE-0010a / 62	E-911 ALERT SYSTEM	Remediate	Y	20% / 20%	5	4	4	Contractor test plan delayed to 9/18/1998.
3 / 2	MCGI-0006 / 63	EMERGENCY COMM CENTER	Implement	Y	90% / 90%	4	4	4	New PC delivered. Some new HW & SW still necessary. Completion date moved to 9/30/1998.
4 / 2	MCGO-0003 / 56	INDEPENDENT REVIEW & RISK ASSESSMENT	Assess	Y	9% / 9%	6	6	6	Contract negotiations aborted with vendor awardee due to differences in T & Cs. Negotiating with next rated vendor.
5 / 2	MCGO-0004 / 63	CONTINGENCY/BUSINESS CONTINUITY PLANNING	Assess	G	0% / 5%	0	0	0	New project established 8/1/1998.
6 / 2	MCGO-0005 / 65	INTERAGENCY Y2K EMERGENCY FUND	Assess	G	0% / 0%	0	0	6	TIF request submitted.
7 / 3	MCGE-0010b / 50	E-911 FALSE ALARMS	Remediate	G	27% / 27%	0	0	0	Servers & replacement PC hardware/software installed. Testing Kofax imaging cards. CACI test plan (timeline) submitted.
8 / 3	MCGE-0024 / 49	TAX ASSESSMENT	Complete	G	95% / 100%	0	0	0	DIST-MANAGED. Completed.
9 / 3	MCGE-0030a / 49	TAX RECEIVABLES-REPLACE	Remediate	Y	15% / 18%	0	0	0	DIST-MANAGED. 1st status meeting held. Tax Receivables system demo'd. Task Order RFP for project manager issued.
10 / 3	MCGE-0030b / 49	TAX RECEIVABLES-REPAIR	Assess	Y	3% / 5%	0	7	7	DIST-MANAGED. Contingency to MCGE-0030a. Contractor kick-off meeting held. Acceleration planned. Completion target date 12/31/98.
11 / 4	MCGD-0011 / 56	ATMS/COMTRAC	Implement	Y	50% / 88%	4	4	0	Contractor's report received, system certified. Integration in progress.
12 / 4	MCGD-0060 / 46	GENERAL PC REMEDIATION	Remediate	Y	25% / 27%	0	5	5	Cure letter sent to vendor. Diverting PCs from other programs.
13 / 4	MCGE-0032 / 47	3270 EMULATOR FOR WINDOWS	Assess	Y	3% / 10%	4	5	5	Testing done with compliant version of MEMO/Windows on September 3, 1998. Could not prove non-compliant.

Y2K PO 9/22/1998 8:29:03 PM NOTE: Some projects required to be held at 95% complete pending full integration (interface) testing.

LIST OF ATTACHMENTS—MONTGOMERY COUNTY, MARYLAND & METROPOLITAN WASHINGTON COUNCIL OF GOVERNMENTS [1]

YEAR 2000 PROGRAM—ILLUSTRATIONS & PROPOSAL

1. Montgomery County's Y2K Compliance Program Plan
2. Montgomery County's Y2K Decision Structure and Website Address
3. Metropolitan Washington Council of Government's Year 2000 Best Practices Manual
4. Montgomery County's Triage Process and Risk Rating Form
5. Montgomery County's Y2K Program Funding Summary
6. List of Montgomery County's Year 2000 projects
7. Montgomery County's Year 2000 Systems Status Summary
8. Montgomery County's How to Develop a Y2K Action Plan
9. Montgomery County's Business Continuity Assurance Planning Guidelines
10. Montgomery County's Contingency Plan Preparation Guidelines
11. Montgomery County's Session with its Municipalities
12. Montgomery County's Scorecard and (Internal) CAO's Responsibility Memorandum
13. Metropolitan Washington Council of Government's Funding Proposal for a National Y2K Emergency Fund.

[1] To obtain copies of these attachments please contact the Montgomery County, MD, Year 2000 Project Office.

PREPARED STATEMENT OF SENATOR GORDON SMITH

Thank you Mr. Chairman. I appreciate your leadership in preparing for today's hearing.

First, I would like to thank all the distinguished witnesses before us today for taking time to testify, and for helping us address the challenges facing the emergency services sector. You especially, along with many other leaders in this industry, are critical to ensuring the safety of our families as the year 2000 approaches.

I am also very pleased to see Mr. John Koskinen, the President's Special Assistant on the Year 2000 problem, here to testify again before the committee. Thank you Mr. Koskinen. I am particularly interested in hearing about the President's involvement in preparing our national emergency systems for the year 2000. As leaders of the free world, I hope we all continue to focus on the safety of America and make preparations to safeguard against worst case scenarios. Along with my interest on our domestic emergency preparedness, I am also interested in preparations being made on the international front.

After hearing from several agencies on this issue, it has become apparent that a priority must be placed on establishing a coordinated central Y2K emergency service center. It would make sense for every emergency program to dispatch from, and report to, a central Y2K emergency center when the average 300,000 9–1–1 calls a day increases into the millions on January 1, 2000? An emphasis should be placed on developing a response to all these worst case scenario emergencies. I look forward to hearing how these needs are being met and in what way our committee can help.

No one will know the impact of this problem until the beginning of the new millennium. I have heard the Y2K problem being characterized as anything from a simple bump in the road to the second coming of Christ. With only 456 days left, there is no more time for anyone to be dragging their feet or dodging this critical problem. We need to assure the American public that our emergency systems are prepared for any scenario that may arise.

In my state of Oregon, the Y2K issue has been made a top priority at every level of government. Local task forces are organized in every region, county, and city by private citizens who have volunteered their time. Every time I am back in Oregon, I make it a priority to participate with these task forces in as many local Y2K forums as possible, to learn more about the local problems and efforts going on in my state, and finding ways to help.

Information sharing has been extremely beneficial to everyone in Oregon, because we are working together to deal with the problem as a community. Working together prevents unnecessary panic, provides everyone an opportunity to understand the severity of the problem, and brings the community together as we work toward a common goal. Information sharing is working, as the citizens of may state are proving, and I hope we can continue the open, honest dialog today at this hearing, and in these final months to come.

Thank you Mr. Chairman, I look forward to learning more about the specific Y2K challenges facing our emergency services sector and the specific steps being taken to address them.

PREPARED STATEMENT OF LACY SUITER

Mr. Chairman and Members of the Committee: Good morning. I am Lacy Suiter, Executive Associate Director for Response and Recovery, Federal Emergency Management Agency. FEMA Director James Lee Witt has asked me to testify at this hearing on his behalf and I am pleased to have this opportunity to appear before you. 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 thirty-four sector coordinators supporting the President's Council on Y2K Conversion, chaired by Presidential Advisor, John A. Koskinen. 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 prevention or response to the causes of computer disruption. FEMA does not have authority or the technical expertise required to perform those types of missions.

The goal of the Emergency Services Sector is to facilitate efforts to ensure that all members of the nation's emergency services community will be able to operate normally through the Y2K conversion period. The other sectors are working toward the same assurances in their areas, with the shared goal being that Y2K disruptions will be of minimal consequence. The objectives of the Y2K Emergency Services Sector Working Group are to:

—Develop coordinated outreach plans and communications to State, local, and private sector groups in fire and emergency services (including the volunteer agency community);
—Monitor progress of the sector; and
—Prepare for inevitable disruptions.

BRIEF ASSESSMENT OF GOVERNMENT PREPAREDNESS FOR THE YEAR 2000

The Emergency Services Sector, which met most recently on September 16th, will be providing reports to the President's Council in the coming months on the readiness of the sector as a whole. Readiness assessments are being conducted throughout the 34 sectors on the Council.

At the Federal level, all of the agencies are in the process of increasing awareness and fostering readiness self-assessments among their stakeholders. These user communities cut broadly across the Nation's infrastructure, involving both the private and the public sector. And the agencies themselves must be ready to cross the year 2000 threshold with high confidence that their own systems will work well. To this end, FEMA and the other Federal agencies report directly to the Office of Management and Budget (OMB), on a monthly or quarterly basis, regarding the progress being made with their own systems.

OUTREACH TO THE EMERGENCY SERVICES SECTOR ON Y2K

FEMA is working with other agencies in the Emergency Services Sector to develop an outreach action plan. The action plan will include three categories of activity:

—Meetings on Y2K convened by Federal Agencies;
—Outside meetings which Federal officials will attend in order to spread the word about Y2K; and
—Other communications on Y2K, such as letters, public notices, web site information, and brochures.

FEMA plans to post this information on its Y2K web pages during the next month, and to make all of this information accessible through www.fema.gov, as it becomes available.

The 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, FEMA developed a list of frequently asked questions regarding Y2K and their 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 available for local distribution. 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. FEMA is currently in the process of direct-mailing the Y2K brochure along with a cover letter to each of the approximately 33,000 individual fire departments across the country.

The Y2K brochure also directs people to related web sites, including the USFA web site. The web site includes a Y2K section which provides general information, frequently asked questions and answers, as well as basic testing tips that individuals and organizations can apply to determine if their equipment and systems are Y2K compliant.

Over the next few months, the Fire Administration plans to enlist the aid of State Fire Marshals in determining local fire service readiness for the Year 2000. Throughout fiscal year 1999, 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 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 led a discussion of Y2K and identified it as a priority area for the coming year. In fact, NEMA has already initiated dialogue with its membership on Y2K, and has assigned the NEMA Preparedness, Training, and Exercises Committee to review and coordinate efforts with FEMA. Committee officials participated in discussions with FEMA's Associate Director for Preparedness, Training and Exercises, and the Presidents of NEMA and IAEM on the importance of developing emergency preparedness measures and guidance to deal with potential Y2K issues. As a result, FEMA will work in partnership with NEMA, IAEM, and other organizations over the next several months to develop emergency preparedness guidance for the entire emergency preparedness community. Information on model State and local Y2K programs and practices will also be collected and shared.

FEMA's Regional Directors have been asked to contact the State Emergency Management Directors in their region to support this effort. The personal contacts will

reinforce the importance of preparedness and compliance at the State level, emphasize the necessity of State outreach to local governments, and help to identify areas where additional specialized assistance is needed.

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. All students attending EMI resident classes receive copies of the Y2K brochure developed for the fire service community.

In November, FEMA's Associate Director for Preparedness, Training and Exercises will address the IAEM 46th Annual Conference in Norfolk, Virginia, to urge local emergency managers to participate in efforts to raise Y2K preparedness.

In February 1999, Director Witt will address the National Govemor's Association on the status of several FEMA initiatives, including Year 2000 outreach, and offer 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 I am responsible as Executive Associate Director of Response and Recovery, 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 is 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 assistance of 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 heath 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 the President's Council on Y2K Conversion is an authoritative source for information on this hazard.

The Council is scheduled to release a report later this year that narrows down the risks and describes a plausible worst-case scenario. John Koskinen, Chairman of the President's Council on Y2K Conversion, attended our August meeting of the

primary 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 believes that the basic infrastructure will work and that there will be no major nationwide catastrophic disruptions, but that there may be needs 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. 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.

As we wait for the official assessment from the President's Council, I am continuing my 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 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 millennium continues.

RESPONSES OF LACY SUITER TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Does FEMA plan to preposition any core reserves of personnel, supplies and equipment to aid local governments or is it planning to coordinate Federal Government and State government resources? Please explain.

Answer. At this point, FEMA does not plan to preposition personnel, supplies and equipment. We are planning to activate monitoring operations through the critical conversion period from December 29, 1999 through January 4, 2000. This includes activating the interagency Emergency Support Team at FEMA Headquarters and our 10 interagency Regional Operation Centers (ROCs) which will operate from each of the 10 FEMA Regional Offices. Appropriate Federal assets such as the Mobile Emergency Response Support Detachments will be placed on alert.

Question 2. Mr. Suiter, I would like to thank you for coming today's hearing. We realize that this is an incredibly busy time for FEMA. FEMA cannot deploy IT professionals to Y2K system failures. Unfortunately, our concern is that physical effects of computer problems could result in failed water systems, loss of power etc. which could be scattered so widely that States could become overwhelmed. What consideration has been given to how FEMA would respond to the request for help from multiple States (eight or more)?

Answer. The current Federal response structure as implemented through the Federal Response Plan is designed to provide assistance in response to emergencies and disasters in multiple locations throughout the United States and its territories when Federal assistance is deemed necessary. The Federal response structure relies heavily on its Federal regional response structure to deliver assistance to State and local communities.

Question 3. If a Governor were to seek, and the President were to issue, a declaration of emergency for a particular state or region as a result of major Y2K disruptions: What types of assistance might FEMA reasonably be able to make under current authorities? Would these requests all likely be made under the Stafford Act/Federal Response Plan, or would additional or alternative channels of relief potentially be available through other emergency preparedness authorities?

Answer. Upon a Presidential declaration of an emergency under the Stafford Act, FEMA may give mission assignments to other Federal departments and agencies that comport with their day to day missions to utilize their authorities and the resources granted under Federal law. Resources available include personnel, equipment, supplies, facilities, managerial, technical and advisory services. These assets are utilized to support State and local emergency assistance efforts to save lives, protect property and public health and safety, and lessen the threat of a catastrophe. Individual Federal agencies have their own statutory authorities through which they may provide Federal assistance to State and local governments that fall outside of the scope of the Stafford Act/Federal Response Plan.

Question 4. Mr. Suiter, how effective do you think a Y2K warning system would be? Would 17 hour advanced notice help FEMA response or preposition equipment?

Answer. Although FEMA agrees that a Y2K early alert system will be effective, it is premature to determine to what degree at this point. Effectiveness will depend on the nature of the emergencies and the type of Federal assistance that can be provided in a timely manner. The 17-hour advance notice will help FEMA assess the nature and characteristics of the Y2K-related emergencies and enhance our ability to relay to the public what types of emergencies are mostly likely to occur. At the same time, 17-hours advance notice may give us a better idea of the scope and order of magnitude of the emergencies that occur overseas. The extent to which the Federal Government's reaction will be enhanced is uncertain.

Question 5. I understand that FEMA is currently working on an appendix to the Federal Response Plan which will specifically deal with Y2K. Could you please elaborate on what this Y2K appendix will contain and when we might expect to see this document?

Answer. In January 1999, an outline of a Y2K Supplement to the Federal Response Plan will be developed based on input from the FRP agencies and their regional counterparts. Assessments from the Emergency Services Sector and the President's Council on Y2K Conversion will influence the content of the Supplement. At this point, we envision that the Supplement will include a Basic Plan and functional annexes for the appropriate Emergency Support Functions. We plan to develop, publish, and distribute the Supplement by July 1, 1999.

Question 6. The Federal Response Plan depends heavily upon the Federal Agencies such as the Department of Defense and the Department of Agriculture. How will FEMA cope if the supporting agencies have not considered their emergency response assets considered mission critical? Has FEMA received any indication that agencies are addressing this problem?

Answer. FEMA is hosting monthly meetings of the FRP Primary Agencies to collect and track information on the progress of the Y2K compliance status of the 12 Emergency Support Functions. This information will be used to conduct a vulnerability assessment of the interoperability gaps that may arise as a result of Y2K operational issues and shortfalls. Planning is underway to conduct a national level seminar or tabletop exercise in the May/June timeframe to run through an operational simulation of our response to a Y2K related emergency. A national level exercise enables us to work with the FRP agencies and to examine the interoperability shortfalls among the FRP agencies so that back-up systems can be put into place by December 31, 1999.

Today, I cannot determine that all of the 28 signatory agencies to the Federal Response Plan will be Y2K compliant by March 31, 1999. Based on responses FEMA has received from the FRP Primary Agencies in response to an Emergency Services Sector Y2K Standard Questionnaire, a number of agencies will not be Y2K compliant by March 31, 1999. However, no agency has reported that it will not be Y2K compliant before December 31, 1999.

Question 7. Has FEMA tried to ascertain the types of relief that states might need, and consider which of the 12 Emergency Support Functions it would most likely need to activate in response to Y2K-related emergencies?

Answer. FEMA is in the process of planning a series of regional tabletop exercises to ascertain the needs of the States resulting from a Y2K-related emergency. Although the Y2K Supplement to the FRP will detail the special operations and preparedness measures, it has been our experience that consequences requiring 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 FRP is robust , flexible and 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.

Question 8. What are the thresholds and guidelines that would govern FEMA's involvement in managing consequences of primary failures of critical infrastructure services. What criteria would be applied to determine the conditions under which relief or aid would be afforded?

Answer. From a technical viewpoint, FEMA may not be able to respond to requests for technology support. However, we can use the Federal response system to provide a backup network to ensure that requests from State and local governments are referred to the appropriate public/private coordination channels that have been established through the President's Council on Y2K Conversion. From a consequence management perspective, our primary operational objective and criteria will be to respond to physical consequences on lives, property, and public health and safety as a result of a Presidential declaration of an emergency or major disaster. This is in accordance with the Robert T. Stafford Disaster Relief and Emergency Assistance (Stafford) Act.

Question 9. Existing authority appears to permit FEMA, under appropriate circumstances, to preposition key assets in anticipation of a major disaster or emergency. Which of these authorities might be relevant to pre-positioning the resources most likely to be in demand in the aftermath of widespread Y2K-related failure? What conditions must be met in order to allow the pre-positioning of these resources under these existing authorities?

Answer. In accordance with several federal laws and existing executive orders, each federal department and agency has assigned roles to fulfill emergency preparedness and planning. These statutory and presidential mandates require each department and agency to budget for its own preparedness and planning. Should there be an event resulting in a presidentially declared emergency or disaster, the operations of the agencies are funded from the President's Disaster Relief Fund unless other funds are available. Because of the geographic uncertainty with respect to Y2K, planning for pre-positioning is not being conducted by FEMA at this time.

Question 10. Existing authority may allow for the Director of FEMA to initiate non-conventional forms of pre-preparation, such as providing grants to states for emergency plan development and training, or requesting from States reports on State plans and operations for emergency preparedness. Has FEMA undertaken any efforts to make grants or other forms of funding available to the states, in advance, for specialized Y2K preparedness programs? Has it made any requests of the states to review Y2K-related plans? Are these authorities generally suited to this purpose? If not, would modifications be advisable?

Answer. FEMA did not request additional funds for Y2K planning and preparedness as part of our initial request for fiscal year 1999appropriations. Public Law 105–277, the Consolidated Omnibus and Emergency Supplemental Appropriations Act for fiscal year 1999, provided additional funds to the President for Y2K issues.

In general, FEMA gives maximum flexibility to the States relative to the use of the State and local assistance funding they are provided so that they can determine how best to meet their emergency management needs. If a State decides to do so, some of this funding could be used to help address Y2K issues. The existing authorities are sufficient to undertake Y2K preparedness activities at the State level.

As part of our preparedness efforts, FEMA has discussed the Y2K problem with the National Emergency Management Association (NEMA), which represents State emergency managers, and with the International Association of Emergency Managers (IAEM), which represents local emergency managers. Both groups have pledged to work in full partnership with FEMA to address the Y2K issue. In addition, the ten FEMA Regional Directors have been directed to personally discuss with the State Emergency Management Directors the Y2K situation in the States and local jurisdictions. The Regional Directors are to report the results of these meetings in mid-November and a summary assessment of the State and local preparedness will be provided to the President's Council on Year 2000 Conversion in December. Future actions and guidance will be based on the results of the State surveys by the Regional Directors.

Question 11. If there are widespread failures and substantial portions of a state's population is deprived of critical services, it is foreseeable that a large number of states may request some form of Federal assistance. Has FEMA planned for this possibility, and if so how will state requests be evaluated or prioritized? Are there any means by which the states may be able to notify FEMA of their anticipated needs in advance of the event?

Answer. The Catastrophic Disaster Response Group (CDRG) is a National-level coordinating group comprised of senior representatives from all the FRP signatory agencies. The CDRG has the primary operational mission of resolving policy, resource allocation and prioritization issues that cannot be resolved at the Federal regional level. This also includes resource and allocation issues that arise between Federal regions.

Under FEMA's leadership, the CDRG is addressing the potential impact that Y2K failures could have in responding to the consequences of Y2K failures. The Chair of the President's Council on Year 2000 Conversion has asked that FEMA co-sponsor with DOD a National Y2K Table Top Exercise to be held next spring. One of the goals of the exercise is to identify issues that that may impact the Federal Government's ability to manage the consequences of Y2K failures. Exercise activities will be held at the regional level with Federal and State level participants to help prepare for and address Y2K issues.

Other outreach to State and local jurisdictions is being conducted through the ten FEMA Regions to survey and assess State and local preparedness for the Y2K conversion. FEMA is coordinating and working with the National Emergency Management Association and the International Association of Emergency Managers to address Y2K issues and to identify areas in which State and local jurisdictions may need assistance. Through these State and local contacts it may be possible to identify anticipated needs in advance of the event. As part of these outreach efforts, preparedness, training, and exercise assistance and guidance will be provided as necessary to State and local jurisdictions to assist them in preparing for the Y2K conversion and to help mitigate anticipated problems.

Question 12. S. 2361, the Disaster Mitigation Act of 1998, will, if passed: (1) expand FEMA's pre-disaster mitigation authorities; (2) reduce the types of facilities and activities that can receive Federal assistance following from a disaster; and (3) modify current cost-sharing arrangements pertaining to disaster relief and emergency assistance. How will this bill, if passed, impact FEMA and the Federal Government's ability to address foreseeable Y2K-related requests for relief and assistance? Are there some portions of this legislation that might be more applicable than others and that might be considered for expedited treatment?

Answer. The primary purpose of S. 2361, the Disaster Mitigation Act of 1998, was to promote mitigation; that is, to reduce loss of life and property from natural hazards both before and after disasters strike. It also proposed some changes to FEMA's disaster recovery programs to facilitate a more efficient recovery and to meet the needs of both public and individual disaster victims better. The amendments were not drafted with the Y2K-related requests for disaster relief in mind. Had the Disaster Mitigation Act of 1998 passed, we do not believe that it would have impacted FEMA's and the Federal government's ability to address foreseeable Y2K-related requests for relief and assistance.

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

STATEMENT OF R. MICHAEL AMYX, EXECUTIVE DIRECTOR, VIRGINIA MUNICIPAL LEAGUE, ON BEHALF OF THE NATIONAL LEAGUE OF CITIES

My name is R. Michael Amyx and I am the Executive Director of the Virginia Municipal League. I am pleased to be able to submit this testimony on behalf of the National League of Cities. The Virginia Municipal League is a statewide, non profit, non partisan association of city, town and county governments established in 1905 to improve and assist local governments through legislative advocacy, research, education and other services. The membership includes all 40 cities in the state, 155 towns and 15 urban counties. As Executive Director, I serve as the CEO of the Virginia Municipal Liability Pool and the Virginia Municipal Group Self Insurance Association. These organizations provide low cost insurance to municipalities.

NLC was founded in 1924 by state municipal leagues that sought national representation before Congress on municipal issues. NLC is the largest and oldest national organization representing municipalities and their elected officials. NLC represents 135,000 mayors and council members from municipalities across the country. Over 75 percent of NLC's members are from small cities and towns with populations of less than 50,000. A significant number of small cities and towns are in the Commonwealth of Virginia.

First, I am grateful to Chairman Bennett and the members of the Senate's Special Committee on the Year 2000 Technology Problem for their leadership role in drafting and efforts made towards the passage of The Year 2000 Information and Readiness Disclosure Act (S. 2392). NLC thanks the Special Committee for the opportunity to provide input during the drafting process regarding the needs of municipalities. Our nation's cities and towns consider the millennium bug to be a very serious matter with potentially dire consequences. Many applications and systems in local communities are not Year 2000 compliant today. Critical systems including E–911 services, water and wastewater, traffic signals, electric and communications, if disrupted, could cause severe problems for citizens who rely on these vital services

The Year 2000 Information and Readiness Disclosure Act will allow companies and municipalities to disclose and share information that will help to avert major system failures brought about by the millennium bug. It is critical that cities and towns know what measures are being taken by the computer industry and state and federal governments to avoid Year 2000 problems and what methods are working well. We hope that the House of Representatives will follow suit and pass this bill in the coming week.

There are several other crucial areas of concern to cities and towns where assistance from Congress is desired. We are willing to work with you to see to it that cities and towns are doing all that is necessary to avert a major crisis.

First, we need legislation requiring insurance companies to disclose how they plan to respond to Year 2000 claims. To date, the industry as a whole has kept its cards close to the vest causing much uncertainty with respect to coverage and defense costs in the event claims are filed. Cities and towns could lose millions of dollars in costs to fix equipment. Of equal concern is the fact that cities and towns could be sued for failing to adequately deal with the Year 2000 problem in liability lawsuits ranging from public safety issues to the issuing of welfare checks.

Second, we are concerned that small cities and towns do not have the information, resources, awareness, and time left to implement compliance programs. Many of these small cities are already struggling financially and they do not have the infrastructure resources that larger cities have. We need help with disseminating information to them about the Year 2000, assisting them with their compliance efforts, and helping them to pay for this process.

Third, despite the successful efforts of the Senate to address information disclosure, liability remains a concern of our nations cities and towns. Frankly, even with preparations and test runs, we still do not have the answer on whether all municipal systems will work within a city on January 1, 2000. This presents a challenge

for cities and towns because we are responsible for public safety. If a large number of lawsuits are brought against cities on the grounds of failure to provide adequate public safety due to such things as glitches on ambulances, fire trucks, global positioning systems, or electronic communications related to saving lives, we believe that cities will be faced with budget deficits. Even more chilling is the possibility that the fear of liability will manifest in a reluctance on the part of cities and towns to respond to disasters and routine emergencies. We would like to work with you to address this concern for both our citizens' lives and the fiscal future of our cities and towns.

The Virginia Municipal League has conducted some research that indicates that local governments are aware of the problem and of the potentially severe consequences of not solving it. Many local governments, in particular small to medium sized jurisdictions, do not have the internal expertise necessary to move forward and are, to some extent, relying on outside vendors to achieve compliance. Some cities and towns are way ahead of others. Limited resources and increased demand for services continue to make funding an issue. We are confident that most local governments will be ready when we reach January 1, 2000. However, invariably some applications and systems will not be compliant. Local governments are prioritizing systems for scrutiny, and we hope that disruptions will be minimal.

At this point the Virginia Municipal League is in the process of educating Virginia's cities and towns on the Year 2000 issues. It is no secret that while most cities and towns are dealing with the problems, information, and resources are beyond the reach of small cities. We have a seminar planned for next week at our annual conference to explore the liability issues for municipalities associated with Y2K and also to explore the scope of the problem. Within the 49 state municipal leagues, the National League of Cities, and the members of the Big 7 state and local government interest groups a network exists to provide information directly to cities and towns. Unfortunately, there is no single prescribed cure for this problem, and the costs of addressing the problem are well beyond the reach of many small cities and towns.

From a municipal perspective, cities and towns have multiple software and hardware vendors which have been used for numerous years. Cities and towns rely on these businesses for solutions to software and hardware dilemmas, but we cannot control the outcome. Further, some of these vendors are already out of business, and the vulnerability of those still in business is great. Additionally, electronic chips and devices embedded into machinery may suffer from the Y2K problem—imagine all of the public works equipment that may be effected by this.

NLC's Local Officials Guide *The Year 2000 Problem * * * When the Clock Turns Be Ready!*, addresses the problem for municipalities and the steps to take to implement a plan. This publication says that our nation's cities and towns face the following threats if we do not fix or are unsuccessful at fixing theY2K problem:

—Threats to human life and safety are likely to occur if systems fail to alert authorities to crisis situations or provide incorrect information about the nature or local of a crisis;

—Sharp increases in local taxes may be needed to defray Y2K expenses, including the litigation expenses which may continue for more than a decade into the new century;

—Elected and appointed city officials may be held personally liable for violation of fiduciary responsibility, breach of expressed or implied warranty, errors and omissions, or malpractice; and

—Extensive amounts of computer programmer time for both implementation of a plan and data repair costs, especially for data intensive agencies.

I think that all of the state and local government witnesses testifying here today can agree that the longer we delay, the greater the cost will be, more normal processes will be disrupted, and the less likely we are to be able to solve problems as time runs out. Cities and towns can prepare for the Year 2000, but we need help getting the right information and the resources. NLC and the state leagues can serve as a repository of information for cities, but we need to ensure that the information out there is correct.

LEGISLATION

At the state level, we are pursuing legislation that would extend sovereign immunity to local governments for liability arising out of the Year 2000 issue. Several states have passed such legislation (Nevada, Florida, Georgia, Iowa, and New Jersey) and others are currently considering similar bills (California, Hawaii, Illinois, Minnesota, New Hampshire, Pennsylvania, South Carolina, and Utah).

The Virginia General Assembly passed legislation during the 1998 session extending such immunity to the Commonwealth, but did not include local governments.

It is our view that local taxpayers deserve to be protected from unpredictable financial impact which could be catastrophic. This is particularly true if insurance companies do not step forward to provide funding for defense of claims and claim payments as required. Cities and towns need advance warnings to arrange for other coverages or potentially increased expenses. The 32 local government insurance pools that participate in the NLC—RISC (Risk Information Sharing Consortium) and primarily represent small cities that otherwise would have problems finding affordable insurance have looked to proactively address this problem, but need the information from insurance companies too.

THREAT TO EMERGENCY SERVICES

Arlington County, Virginia has one of the most advanced emergency preparedness programs in effect to date. Arlington County has set up an emergency management team whose function is to simulate all types of "what if" emergency situations, including systems failures due to Y2K problems. Emergency drills are performed regularly and are sometimes performed in conjunction with other local jurisdictions. There are two major areas of focus—information systems, which encompasses traditional computer hardware and software problems, and embedded chips, which comprises on-board systems in ambulances and police cars. To give the Committee an idea of the cost of implementation of a top-notch program, Arlington County has allocated $15.5 million just on the information systems portion of Y2K preparedness. This figure does not include monies for embedded chips issues or traffic signals, and is expected to increase drastically due to the sheer magnitude of the Y2K preparedness undertaking.

Currently, Arlington County has utilized Y2K coordinators who are looking to identify where the Y2K bug may occur. With respect to the embedded chips issue, assessments and inventories are conducted and each department is required to come up with contingency plans, even if the Y2K-compliant systems fail. Deadlines have been established both for conducting the inventories and for designing and testing contingency plans.

Despite the care taken by Arlington County to effectively complete its Y2K emergency preparedness efforts it, along with other local jurisdictions faces three major concerns. First, no matter what local governments do to prepare internally for Y2K, many critical governmental functions are tied to the private sector and are only viable if the private sector is ready for Y2K too. For example, a municipalities' E–911 response system may be Y2K compliant, but if the local hospital's systems are not Y2K compliant, there will be problems. Second, local governments must respond to emergencies caused by outside entities when there's a systems failure. For example, local police will be summoned if burglar alarm companies are not Y2K compliant and homeowner alarm systems go off en masse. Third, the fiscal impact upon local governments in the event of Y2K systems failures in the private section cannot be underestimated. If a local business goes out of business due to Y2K problems, that business is not paying taxes to the local government.

One way to help with solutions to these problems raised by Arlington County, but also applicable to local jurisdictions, is for Congress to focus on providing more resources to help coordinate Y2K preparedness on the local level. Whether this is better accomplished by federal involvement in increasing manpower at the local level or by simply providing more funding at the federal level is not known. What is known is that the federal government must become involved in some meaningful way. Even the most prepared local governments are worried about the ability of the private sector to adequately prepare for Y2K emergencies and the impact that this will have on local governments. We believe that some compliance accountability standards are needed to provide reassurance to local governments that all will be ready on January 1, 2000.

NLC ACTION

The National League of Cities has assisted in disseminating important information to local governments with Public Technology Inc., the International City/County Management Association, and the National Association of Counties. These organizations have mounted a national campaign to raise awareness and provide resources and other tools to local governments because of the serious impact that the Y2K problem could have on local governments. Most recently, NLC distributed over 6,000 copies of the "Y2K and YOU Information Kit" developed by these organizations. These kits will be disseminated through state leagues at annual conventions, state league special meetings focusing on Y2K, and sent to member local governments of these organizations. The Virginia Municipal League plans to distribute this kit to all members of our insurance program, which numbers about 500 cities and towns.

"Y2K and YOU" provides the tools necessary for cities and towns to develop remediation strategies. The kit contains best practices that cities have implemented, information on helpful organizations, Y2K do's and don'ts, and a checklist for coping with the Y2K problem. The intent of this kit is to avert potential problems that have the potential of crippling local economies, compromising public safety and health, and stifling local government revenues. Additionally, a video is included in this kit that highlights the steps necessary to implement a plan to address the Y2K problem.

Though the kit provides a good deal of useful help and guidance, local governments still have to contend with the high costs of addressing the Y2K problem proactively, finding the right information and solutions, and finding the actual manpower and technical expertise needed to avert a potential problem. The first step is helping local governments recognize that Y2Kis an issue that they must confront. Cities and towns across the country are all over the map when it comes to assessing what kinds of systems have been put in place to avert a problem.

STATE MUNICIPAL LEAGUES

From my perspective, state municipal leagues are at a distinct advantage in disseminating and sharing information on Y2K remediation. At this point, many leagues have begun programs that give local governments the tools to get started at a local level on addressing potential Y2K problems.

My colleague, Jim Miller, the Executive Director of the League of Minnesota Cities has convened a task force within the Minnesota League that is addressing Y2K. The League of Minnesota Cities will be conducting several regional meetings in the coming two weeks that will assist cities in addressing things like what do to do if wastewater treatment and emergency services are effected by the problem and how to plan to prevent problems. Additionally, The Minnesota League has developed its Minnesota specific Action Guide that outlines the necessary steps, samples of tools and important documents for planning, and checklists for issues to address.

While the Minnesota League has taken many steps and began this process relatively early, one of the things that Mr. Miller noted was that he wished that they had begun the process earlier, because the League keeps learning about new issues and new concerns. More than half of the counties in Minnesota have populations of less than 10,000. Community hospitals, utility commissions, and wastewater commissions just don't know where to turn to for help.

CITY EXAMPLES

In my testimony today, I can tell you about some great things that cities and towns are implementing, but I cannot tell you about who is not complying and what is not being done. We frankly have no foolproof way of determining which cities and towns have not developed and implemented effective compliance programs for Y2K. Further, the information that we do know is coming from large cities that have the revenue and access to information and technology that compares to Fortune 500 companies. The information is not out there with regard to those small cities and towns who don't know about the problem and who have not addressed it. We are concerned that these cities and towns will be forgotten. They need help, or they are likely to have catastrophic failures that compromise public safety and life as well as their town's economic survival.

While the concern remains for the cities that have not yet acted, I do want to tell you about some of the innovative things that are being done.

—The City of Plano, Texas' (Population 128,713) purchasing division required a "Year 2000 Compliance" warranty from vendors providing the City with hardware and software products. Vendors must sign the document guaranteeing that their products can accurately process date between the 20th and 21st centuries.

—The City of San Diego, California (Population 1,110,550) formed a team that began addressing Y2K issues in 1995. The focus of their attack is the City's internal software and assessing off-the-shelf software problems.

—Albuquerque, New Mexico (Population 384,736) developed a process to identify and remediate those things adversely effected by Y2K problems. The city's Information Systems Division reorganized to three interrelated teams—City Services, Finance, and Public Safety. These teams will address the needs of programming and infrastructure during the process and also plans to hire five additional contract programmers for the effort.

—Seattle, Washington (Population 516,259) plans to spend more that $50 million to reprogram major applications affected by the problem and plans to replace the city's accounting system.

Thank you again on behalf of the NLC for providing us the opportunity to present our views to the Committee.