S. HRG. 105–692

TELECOMMUNICATIONS AND Y2K: COMMUNICATING THE CHALLENGE OF THE YEAR 2000

HEARING

BEFORE THE

SPECIAL COMMITTEE ON THE YEAR 2000 TECHNOLOGY PROBLEM UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

ON

GETTING TELECOMMUNICATIONS READY FOR THE YEAR 2000

JULY 31, 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

50-323 CC WASHINGTON : 1998

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*
ANDREW LOWENTHAL, *Acting Minority Staff Director*

(II)

CONTENTS

OPENING STATEMENT BY COMMITTEE MEMBERS

CHRONOLOGICAL ORDER OF WITNESSES

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

TELECOMMUNICATIONS AND Y2K: COMMUNICATING THE CHALLENGE OF THE YEAR 2000

FRIDAY, JULY 31, 1998

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

The committee met, pursuant to notice, at 9:33 a.m., in Room 192, Dirksen Senate Office Building, Hon. Robert F. Bennett (chairman of the committee), presiding.

Present: Senators Bennett, Collins, Smith, Dodd, and Bingaman.

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

Chairman BENNETT. The committee will come to order. We wish you good morning, and welcome to the fifth hearing of the Year 2000 technology problem. To date, we have held hearings on the energy utilities, financial services industry, and health care. Those who follow the committee's activities know that our future hearings will include transportation, general government services, and general business issues.

I am gratified to be able to report that the previous hearings have produced some results. For example, last week's hearing, which was on health care issues, exposed the fact that many manufacturers of health care instruments have been derelict in their reports to various government agencies, and between last week and this week, there have been a deluge of such reports. Apparently, we got some people's attention and that is one of the main purposes of the committee and the hearings. We hope that some beneficial results will come out of today's hearing on the global telecommunications infrastructure.

Let me begin the hearing by noting that this global infrastructure is the central nervous system of modern society. Daily, 270 million Americans depend upon this complex web of voice, data, and video services that enable their telephones, radios, fax machines, computer networks, and televisions and other information appliances, including the pagers that call the Members of the House of Representatives to come vote. We had a failure in that system a little bit ago and the House was forced to go back to systems of bells and hand signals and they, frankly, did not quite

know how to react. I am not sure the Senate would do any better if our pagers were to go down.

Major national and international enterprises, such as emergency response, national security, finance, transportation, health care, government, energy distribution, and others are critically dependent on reliable, 24-hour-a-day, 7-day-a-week telecommunications. That is why this hearing is so important.

Without these services, our ability to receive, gather, and respond to information would be as limited as it was for our forbearers before Alexander Graham Bell invented the telephone. Some critical enterprises which depend upon telecommunications services include the National Weather Service, the Department of Defense, the Federal Reserve System and Wall Street, the National Airspace System, the American Red Cross's blood service and the United Network for Organ Sharing, as well as the national electric power grid. I can go on and on, but I think I have made the point.

I have great concerns that our global telecommunications infrastructure can ride out the millennium date change without significant disruptions for three reasons. First, it is a highly complex system of systems. The opportunity for a breakdown in one place to ricochet around through other places is very, very high.

Second is the fact that there is no identifiable U.S. public or private body taking the lead on the global aspects of Y2K telecommunications problems. Not only is it a complex system of systems, it is multifaceted in its regulatory and ownership structure.

And finally, the fact that to have successful communications, both parties must be able to send and receive information. It is not enough just to be ready yourself. So the solution to this problem for those who are working on it depends upon cooperation from others.

Now, with regard to the complexity of global telecommunications, the sheer number of players illustrates the problem. Today in the United States, there are five long distance carriers, not including the growing number of long distance resellers, five major national television broadcasters, six Regional Bell Operating Companies, more than 1,000 small telephone companies, 16 communications satellite providers, more than 4,500 Internet service providers, hundreds of cellular phone companies, thousands of broadcast radio stations, and over 11,000 cable service companies. This just captures the infrastructure in the United States. It does not include the thousands of large and small communications equipment manufacturers.

Finally, it must be pointed out that this infrastructure relies on hundreds of millions of lines of computer code. It is too great a leap of faith to believe that all the elements of an endeavor this complex will be ready at the stroke of midnight just 17 months from today, especially in light of the limited readiness the industry has shown to this committee so far.

As for coordination and oversight of telecommunications, let me note something from a 1995 National Research Council report, and I am quoting, "In 1984, it was clear what the telecommunications information infrastructure was and who defined it. It was, in essence, the telephone and broadcast networks. The defining players were AT&T, the Federal Communications Commission, and the

broadcasters. You got only the connectivity and services that were offered; compared with what is available today, it was not much.''

''All of this has changed radically. Instead of being defined by monopoly suppliers and regulators, the telecommunications infrastructure has become more closely defined by both market demand and an explosion of supporting technologies that have been brought to the market by myriad suppliers. There has been much movement away from a supplier-defined infrastructure to a user-and market-defined infrastructure.''

In this new world of telecommunications which has given rise to a revolution of new services, no one party is charged with the task of assuring the reliability and interoperability of the entire network, and this is what has made the millennium bug a much harder beast to squash, as it only has to show up in one link in a communications chain to cause mayhem.

Finally, let me return to the two-way nature of telecommunications. Simply put, if the long distance carrier is up and running but the regional carrier is down, the long distance call does not go through. If the Internet backbones are working but the local Internet service provider is off-line, the World Wide Web is inaccessible to the user. And if a financial payment can be received in New York but cannot be sent from overseas, the transaction will not occur.

Like it or not, there is a link-to-link connectivity that starts locally, goes regionally, continues on nationally, and finally ends internationally in this network upon which telecommunications and the enterprises supported by telecommunications critically depend. I am expecting today's panel to tell us how they are going to take charge and address this challenge. Getting telecommunications ready for the Year 2000 is a massive task that will require tremendous cooperation and coordination, but it is a task we must complete.

I am informed that Senator Dodd is tied up in D.C. traffic. I am sure the telecommunications industry controlling traffic lights by satellite had nothing whatever to do with his problem and that he will be here shortly and we will look forward to his opening statement when he arrives.

We will go ahead with our first witness. We are beginning with a staff presentation on the complexity and interdependencies of global communication.

Senator Bingaman, I apologize. I was so wrapped up in my own rhetoric, I did not see you come in. [Laughter.]

Senator BINGAMAN. I am sure that we all were, Mr. Chairman. [Laughter.]

Chairman BENNETT. I am sure that has never happened to any other chairman before.

Senator, we welcome you this morning and would be happy to have you make an opening statement.

OPENING STATEMENT OF HON. JEFF BINGAMAN, A U.S. SENATOR FROM NEW MEXICO

Senator BINGAMAN. Mr. Chairman, you have made a very excellent opening statement and I will just briefly say, I think this is a very important hearing. I believe there are a great many com-

plexities that I do not begin to understand about the telecommunications infrastructure that we all depend upon for national security needs as well as our economic welfare. I hope that this hearing will help to elucidate some of that and I hope it will also help us to sort out who is doing what to ensure that the system continues to function properly after the first of January of the Year 2000. So thank you for scheduling the hearing and I look forward to the witnesses.

Chairman BENNETT. Thank you.

We will begin with a staff presentation on the complexity and interdependencies of global telecommunications. Dr. Judith List, vice president of Y2K Programs at Bellcore, a leading supplier of telecommunications software and engineering services, will describe the scope of the Y2K problem in the context of the national and global telecommunications infrastructure and she will identify specific vulnerabilities facing the industry.

STATEMENT OF JUDITH LIST, PH.D., VICE PRESIDENT AND GENERAL MANAGER, INTEGRATED TECHNOLOGY SOLUTIONS BUSINESS UNIT, BELLCORE

Ms. LIST. Thank you, Senator Bennett, Senator Bingaman, for inviting me to testify on how telecommunications networks could be affected by the Year 2000 technology problem. I am Judy List, vice president and general manager of Integrated Technology Solutions for Bellcore.

Bellcore, an SAIC company headquartered in Morristown, NJ, is a leading provider of communications software, engineering, consulting, and training services based on world class research. Our customers include major telecommunications carriers as well as telecom companies of all sizes, both in the United States and abroad. The business I head for Bellcore provides Year 2000 services primarily in the telecommunications industry, carriers and suppliers, financial institutions, and power utilities.

In response to your request, I will focus today on what Bellcore is doing for the industry concerning Year 2000 on elements of telecommunications networks that could be impacted by the Year 2000 problem, on the challenges of testing, on the outlook for the problem as I see it, and on what positive steps can be taken to help with the problem. I would be happy to answer your questions during my briefing.

To set the stage, let me say that Bellcore has been working on the Year 2000 problem since 1993, with concerted effort beginning in 1995. Bellcore currently supports approximately 150 software system products that are installed in the networks or operations of its licensed customer users. Those users include top tier local exchange carriers, among others. The software systems products include operation support systems and network system that support provisioning, maintenance, and other management functions for local telephone services. All Bellcore-supported software system products either are now, or will be by the end of 1998, Year 2000 functional.

We have also been actively providing our licensees and other customers with Year 2000 information through information kits, our website, and through customer meetings and forums. Bellcore also worked with telecommunications carriers and equipment suppliers

to develop a set of generic requirements for Year 2000 functionality. Bellcore's GR–2945 was available to the industry on January 1, 1997.

In both private and public networks, as in software and hardware computing systems, Year 2000 impacts are possible at every layer of the computing infrastructure. That is, Year 2000 problems can be found in applications, operating systems, databases, file systems, protocols, middleware, and hardware platforms, as well as in the interfaces between interconnected systems.

I would like to turn your attention to the chart at the side of the room so that I can describe how calls are processed through our communications network as a means of illustrating where Year 2000 vulnerabilities are and where they are not.

Networks are large distributed computing environments. The point that I would like to leave you with before I go through the chart is that where we see Year 2000 vulnerabilities in the network is not in the fundamental call processing and data routing of information through the network. Rather, the vulnerabilities are largely in the operations, administration, and maintenance functions that support that fundamental call processing, and I hope that by going through this chart and following the path of a telephone call through the network that you will understand that point.

Senator BINGAMAN. Could I ask you to be a little more specific? Are you saying that the calls will continue to go through but the ability of companies to track what they are doing and all is what is in danger? They are not going to be able to send accurate bills out and that sort of thing afterwards?

Ms. LIST. Right. To set up a telephone call, from the time somebody picks up a receiver on one end until it is connected on the other end through the various switches and other network equipment across various telephone carriers, carries very little date information that is processed in order to set up that call and establish that connection. The date-sensitive processing that goes on is largely for billing purposes, to provision the service, to maintain services so that you can detect faults and alarms in the network.

Problems in those functions could ultimately impact the ability to provide service. So, for example, if there is an alarm condition in a switch and it is unable to be detected because a technician cannot get into an administrative system to look at the error log because passwords have aged, could ultimately impact the ability for the switch to function. But in terms of the actual setup of a call, from the time somebody picks up a telephone until it is connected on the other end, there is very little date-sensitive information that is processed to set up that call.

Senator BINGAMAN. So you are saying that you do not expect an interruption in the ability to use the telecommunications system on the first of January of the Year 2000. What you do think is that some of these embedded problems may cause the system to deteriorate over a period after that, is that right?

Ms. LIST. That is the more likely scenario.

Senator BINGAMAN. Thank you, Mr. Chairman.

Ms. LIST. Thank you. Let me just orient you to the chart initially. There are two large ovals that represent local exchange carrier networks. In between them is an interexchange carrier net-

work, and I am primarily addressing a domestic telecommunications network, although the points are applicable to an international carrier, as well. In addition, we have represented a competitive local exchange carrier in yellow that we are representing as a wireless carrier.

On the top, in the light purple shading, are many of the administrations and operations functions of a network—service activation, the service ordering process, service assurance, detecting faults and troubles and sending technicians out to them, billing processes, a lot of the network management kinds of capabilities.

On the far right, we have represented a portion of a large commercial enterprise. This is not a complete private network. What it represents is a call center network, where customer service representatives might be taking calls, and in the example that I will use, you could imagine this might be a large mail order catalog company that is receiving a variety of customer calls from customers and they are being routed to different service representatives.

Chairman BENNETT. Could we consider the pink portion the U.S. Senate with all of its telephone calls?

Ms. LIST. Absolutely.

Chairman BENNETT. OK. That will help us understand what disaster awaits us.

Ms. LIST. There you go. The red boxes inside of the network elements and the red lines between network elements indicate where there is date-sensitive processing in the telecommunications network. Analyses that we have done for our customers indicate that 75 percent of voice networking devices have date-sensitive processing in them. About 25 to 35 percent of data networking devices have date processing in them. And almost 100 percent of the network management devices have date-sensitive processing in them. The question is, what do those dates do?

What I would like to do is walk you through an 800 call through the network so that you can see how calls are processed through the network and where date-sensitive information comes into play. In many ways, an 800 call is like a typical telephone call. There is a little bit of added complexity to an 800 call because of the nature of that call that I will explain in just a moment.

Let us say that the scenario is that a caller wants to place a call to a mail order catalog or perhaps they are trying to call into the Senate offices. The person picks up the telephone. What happens is the switch detects that someone has picked up the telephone and sends a dial tone to that telephone. It happens in milliseconds. The person dials the telephone number. Those tones are received by the switch and the switch recognizes that this is an 800 call and that it needs to do some special processing on the 800 call.

At that point, it sends a question or a query up to a service control point, or an SCP. The SCP's function is to take the 800 number and translate it into an actual destination telephone number. Let us say that they are calling into Washington and the actual destination is Washington, D.C., or a mail order catalog company in Idaho, for example. It sends that actual destination telephone number back down to the switch. That is the special processing that goes on in an 800 call.

At that point, the call is treated very much like any other telephone call. The switch knows, based on the area code and the three-digit exchange, which end office switch to route the call to across the network. Let us assume that it is a long distance call. It goes through a local tandem to an access tandem. The access tandem hands off the call to an interexchange carrier. The interexchange carrier then hands off to a local exchange carrier on the other end, back through again an access tandem, a local tandem, to an end office switch, and ultimately terminates at a private branch exchange, which is a small private switch at the end user's site, whether it is the catalog company or in the Senate offices.

The information that is used to set up that call is the telephone number of the person who is calling, the telephone number of the person who is being called, and there is date and time information in that call setup message, primarily for billing purposes. It is not used to actually establish the call.

Where we see date processing is in the support functions for the network, and these support functions may sometimes be in the network equipment themselves, in the switches, the boxes in the local exchange network where you see red marks, or it may be in the support systems, the purple shaded areas as well as the other green rectangles at the top, that support those functions.

Let me again use 800 service. Eight-hundred service has a service management system where when a large mail order catalog orders service, they call into the telephone company and they say, "I want to get an 800 number." That order is processed through a customer negotiation system service order and then that service is entered into the service management system.

The kinds of things that are entered, an 800 telephone number is reserved. It is reserved for a certain period of time. Activation of that service may be scheduled for a future date. All of that is date-related information that is important in the support and providing 800 service, but it is not directly involved in the processing of an 800 call itself.

In another instance, a billing example, for example, telephone companies use date and time information to provide detailed records to customers of their calling, as well as in some instances to time the amount of the call or to use different rates for daytime versus evening or weekends, et cetera.

Senator BINGAMAN. I was just going to ask, taking the example you are using, a 1–800 number that is reserved for a period of time to a particular customer, if the system reflects or does not accurately register the fact that you are now in the Year 2000 and you are still within the right period of time, would the customer's ability to use that 1–800 number be lost?

Ms. LIST. That is a possible scenario. It is a 6-month window that an 800 number can be reserved or scheduled up to be activated within 6 months. If that 6-month period covers the boundary over the millennium rollover, it is a possible scenario if there is a Year 2000 problem that it could not recognize—it may decide that that time period has expired. It may not recognize that, in fact, the service should be activated after that window.

I have discussed service activation processes as well as billing processes. Another example is service assurance. If there is a prob-

lem with a network element, it will detect that problem and report it into a fault management system. The fault management system does root cause analysis to determine the cause of the problem and date and time information is passed with that reporting of the trouble so that the network can establish when the trouble was first detected. It then has a trouble ticket issued.

All of those dates and times are important, for example, in addressing service agreements that carriers may have with their customers where they have to provide rebates if they do not recover service within a particular period of time. So dates and times are used in the fault management and network management service assurance part of the network for those kinds of purposes.

There also are scheduling dates and times that are used in the service assurance part of the support systems. So, for example, if a technician is required to go out and fix a problem with some lines that are out in the field or at a customer's premises, those technicians are scheduled and there is date and time information that is involved in scheduling technicians for resolution of those problems.

Finally, let me turn to E–911 service, which I am sure is of particular interest. E–911 services are provided, in many ways, very much like a regular telephone call. Somebody picks up the phone to place an E–911 service. It is routed to the end office switch. The switch recognizes that it is an E–911 call, sends it out over special dedicated lines to an E–911 tandem, and the E–911 tandem, which is a switch, then routes the call to the appropriate public safety answering point, or PSAP. PSAP's may be in county offices, they may be in police departments, they may be in local fire departments.

Again, date and time information is passed along with the E–911 call, primarily for record keeping in the call, not for actual setup of that call. However, date and time information is very important for the PSAP's because they date and time stamp the record of when the call came in and maintain those records on tape, primarily for emergency response recovery time, as well as for legal reasons to have a record of the date and time that an emergency call came in. So the PSAP equipment has date and time stamping information that is important in it. But the calls will terminate in much the same way that a regular telephone call would flow through the network.

I hope this discussion has helped you to see where the Year 2000 vulnerabilities are in communications networks. So while I indicated that a large proportion of network devices have date-sensitive processing in them, that processing is primarily in the operations, administration, and maintenance functions of the equipment, not in the call processing or data routing capabilities. However, if Year 2000 problems are not found and fixed in these operations, administration, and maintenance functions, they could impact service.

Bellcore has conducted assessments of network equipment in a number of major domestic and international carrier networks, as well as risk assessments of the networks of a number of Fortune 50 companies. These analyses we have conducted on the Year 2000 issues in network equipment have covered thousands of voice and data products manufactured by hundreds of United States and international companies. We have analyzed the data gathered from a variety of sources, including manufacturers' responses to ques-

tionnaires, information available on manufacturer websites, and other publicly available sources. We have gathered and analyzed this information in support of our customers. We have not embarked on a comprehensive survey of all carriers, large enterprises, or equipment manufacturers.

The charts at the side of the room summarize our analyses of these data based on our experience, but they have not been independently verified. The first chart covers voice network products and shows for each quarter the percentage of manufacturers who plan to have their equipment Year 2000 functional in that quarter. Combining the data from the third and fourth quarters of 1998, 87 percent of the products we surveyed are planned to be Year 2000 functional by the end of 1998. An additional 5 percent are planned to be Year 2000 functional by the end of first quarter 1999. Of the remaining 8 percent, there are 5 percent of those products that will never be made Year 2000 functional, largely because they are manufacturer discontinued products. The additional 3 percent will be made Year 2000 functional sometime during or after the second quarter of 1999.

The second chart refers to information on data network products. Again, of the products for which we have collected data, if we combine the first 2 bars, 91 percent of the products are planned to be Year 2000 functional by the end of this year. An additional 5 percent are planned to be Year 2000 functional by the end of the first quarter of 1999. And of the remaining 4 percent, there are 3 percent of the products that will not be made Year 2000 functional and 1 percent are planned to be Year 2000 functional sometime during or after 1999.

Senator BINGAMAN. Could I ask, now, are these charts indicating that that percentage of the products being produced and sold are Year 2000 functional or that that percentage of products in use are Year 2000 functional?

Ms. LIST. It is the percent of products of the manufacturers that we have surveyed. So they are products that are currently in the inventories of a number of domestic and international carriers as well as a number of Fortune 50 companies.

Senator BINGAMAN. So you are actually talking about the percentage of the equipment that is being used as part of the infrastructure right now?

Ms. LIST. That is correct, the things that are currently being used. But, for example, for equipment that is manufacturer discontinued, if, in fact, it has Year 2000 vulnerabilities, it will need to be replaced in the network or retired if the functionality can be provided by another piece of equipment.

Chairman BENNETT. Thank you, Dr. List. This has been very helpful. Your full statement will be included in the record.

Just to reinforce a few things, on your first chart, everything that has red in it has a date-sensitive problem?

Ms. LIST. Yes.

Chairman BENNETT. So the deterioration that you talk about over time could occur at any one of those points?

Ms. LIST. Potentially, yes.

Chairman BENNETT. Potentially. So we know that problems are everywhere.

Ms. LIST. Right. The data that we have says that about 75 percent of voice networking devices have date-sensitive information in them.

Chairman BENNETT. Seventy-five percent, if I got it from your statement, of voice networking equipment is date-sensitive, 25 to 35 percent of the data networking equipment, and 100 percent of the network management services.

Ms. LIST. Close to 100 percent, correct.

Chairman BENNETT. So it could strike anywhere. Now, I think, given the size and complexity of the problems, it is critical that contingency planning and disaster recovery be implemented. You mentioned that in your statement. I understand that, statistically, for every 4.5 code corrections that are made in the telecommunications software code, one new error occurs.

Ms. LIST. According to the Software Engineering Institute, it is not just the telecommunications industry, it is software development in general.

Chairman BENNETT. Software in general?

Ms. LIST. Yes.

Chairman BENNETT. That emphasizes the importance of testing——

Ms. LIST. Absolutely.

Chairman BENNETT [continuing]. To find those errors. Nobody deliberately puts an error in every 4.5 lines of code. But simply opening it up and fixing the code, you could go 30 lines of code and have no errors, and then you could go two lines of code and produce two or three errors, and statistically, it works out that for every 4.5 lines of code that are fixed, there is an error.

So while your second chart was encouraging, the number of people who expect to have things compliant at a relatively early date, the question that I have to raise is, do we have enough time for testing? Could you address that before you are through?

Ms. LIST. Certainly. The testing, manufacturers have different definitions of what it means to be Year 2000 functional. I will talk about what Bellcore's approach is for Year 2000 functionality just to give you a sense of what that means for us.

We consider a product to be Year 2000 functional when we have completed unit testing of the particular part of the software code that has been changed, multiunit testing, so looking at different modules of the software that need to work together. We then do a product test in a clock rollover environment, where we actually roll the clock over, the millennium date, the leap year, a variety of other dates, and then we do a capability test between our systems that interact with one another in order to test those interfaces.

So when we say a system is Year 2000 functional, it has gone through an extensive program of testing in order to understand whether, in fact, we have addressed the Year 2000 problem in our software and whether there have been other issues that have been introduced as a result of those fixes. So testing is very important.

Ideally, you would like to test everything that you could test, but that is not feasible, nor does it necessarily make good business sense. It is a risk-benefit issue that needs to be addressed. There is not enough time nor resource to test everything. Even if we had

started many years ago, there is not enough time or resource to address everything.

What most companies are doing is addressing the most critical systems first and then working through their inventory and doing various kinds of testing, depending on how much risk is presented by various pieces of equipment. Things that are critical to the network, large network elements that provide switching capability, for example, many companies are relying on vendor testing, they are doing their own testing once they get the equipment, they are doing interoperability testing to make sure that the interconnections between that equipment and other pieces of equipment are, in fact, functional, whereas other types of equipment that may serve a much smaller role in the network and may not be as critically involved in the provision of services may not go through such an extensive type of testing.

Chairman BENNETT. Let me raise one more issue with you and then we will turn to Senator Dodd. One of the areas where the Year 2000 problem has already hit us is credit cards. In the Christmas buying season last year, December 1997, people would have credit cards that would have an expiration date of 00 or 01 and they would be rejected as having been 98 years out of date.

I have talked with American Express, who has an obvious interest in seeing that this gets fixed, and they said, we are moving rapidly towards fixing the point-of-sale device—you swipe the credit card in the point-of-sale device and it works—and fixing our receiving device where that information comes in and says, no, this really is a current credit card, so we get that to work. But we cannot test the system, running a credit card here and making sure it works there, until the telecommunications system is up to Y2K standards because that is the link between A and B, and even though we can certify that A is Y2K-compliant and B is Y2K-compliant and the telecommunications systems say the link is Y2K-compliant, we are still not sure the system is going to work because the three fixes might not talk to each other.

So it becomes imperative from their point of view that the telecommunications system not only be Y2K-compliant by December of 1999, but that it be compliant much earlier than that so they can run their own tests on it to see to it that the whole system works. Do you have a comment on that challenge?

Ms. LIST. Well, in your particular example, they are really passing data over a telecommunications transmission facility and they can do that today. If they have a Year 2000-compliant device on one end and a Year 2000-compliant device on the other end and they want to pass the information about the credit card number and the expiration date——

Chairman BENNETT. They can do the passing, but they cannot do the hookup test to see to it that the way you, and by you, I mean generically telecommunications, not you, Judith List, the way you have hooked up your device is, in fact, going to work with the way they have hooked up their device, because we go back to this chart. There is a red square virtually at every step along the way that may or may not hook up correctly with their red square.

Ms. LIST. Right. But in trying to send this information through the telecommunications network, nothing is done with the date in-

formation that is being sent by the credit card company to—from the point-of-sale terminal to the credit card company. It is simply a set of bits that are being passed through the telecommunications network.

In terms of the connections through the network, as I have mentioned, the call processing part of the network has very little date-sensitive processing in it. The carriers do need to worry about the operations, administration, and maintenance functions, but that is not directly involved in the point-of-sale terminal sending that data to the credit card company.

Chairman BENNETT. OK, fine. Thank you.

Senator Dodd?

Vice Chairman DODD. Thank you very much, Mr. Chairman. Let me first of all, apologize to you and others for being a few minutes late coming in, and thanking our witnesses and particularly thanking our colleague, Senator Bingaman. He and his staff have done a terrific job in putting this part of our overall set of hearings together here and focusing it.

I have a statement I want to make, but let me just ask you something quickly, Ms. List. We have had a number of different witnesses and trying to get sort of a set of common usages of words or common language in this discussion is not an insignificant problem. I have heard people talk about being Y2K compliant, Y2K ready. You have repeatedly used the word "functional" in lieu of the words "ready" and "compliant". Should I read something different in the word. Are functional and compliant synonymous?

Ms. LIST. People have varying definitions of compliance and it has been used so broadly within the industry that there is confusion about what compliant means. So Bellcore has chosen to be very specific in what it means about being Year 2000 functional, which is the definition I provided in my testimony, in order to make sure that it is clear what we are referring to when we say a system and we warrant our systems as being Year 2000 functional.

Vice Chairman DODD. Can something be functional and non-compliant?

Ms. LIST. Well, it depends on what your definition of compliant is. I mean, therein lies the problem. [Laughter.]

I mean, that is the problem. There are various definitions and there are no standard definitions of what it means to be——

Vice Chairman DODD. Could you be compliant and non-functional?

Ms. LIST. It is possible, depending on what your definition of compliance is.

Vice Chairman DODD. OK. That is very helpful. [Laughter.]

I appreciate that very much.

Senator BINGAMAN. You ought to pursue a career in politics. [Laughter.]

Vice Chairman DODD. Maybe she already has. [Laughter.]

OPENING 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. Let me just make a couple of observations if I could, Mr. Chairman. Again, I thank you immensely. These have been so important, these hearings, and I think shedding a lot of light on what needs to be done and really pointing out the importance of these issues.

One of the reasons I was a little late getting in here this morning was because of some traffic congestion all related to, and I know everyone in this room and across the country feels as strongly as all of us in this building do about the very sad loss a week ago today of Officer Gibson and Officer J.J. Chestnut, and this morning, as the chairman knows and Senator Bingaman knows, there is a funeral for J.J. Chestnut. Again, all of us, while we are having this hearing here and we are focusing on this issue, all of us are very mindful, as well, of the significant loss that all of us suffered last week with the senseless killing of these two officers.

Second, Mr. Chairman, and I gather you mentioned this, we had a pretty good hearing here a week or so ago on the medical implications of the Y2K issue. I thought it might be worthwhile just to sort of take a minute and bring you up to date on where we are with all of that.

Chairman BENNETT. I did mention it, but I think it would be helpful if you have some specifics.

Vice Chairman DODD. As you know, the chairman, as well as myself, expressed our disappointment with the medical device manufacturers who had chosen not to comply with either the Food and Drug Administration's request for information or the request from the Veterans Administration regarding these medical devices and medical equipment.

In particular, Dr. Kaiser of the Veterans Administration testified that there were 233 manufacturers who had failed to respond to their requests for information about this medical equipment. However, we have been informed, the chairman and I have, that after he returned to the VA from this very hearing room, his phone started ringing off the hook, and as of today, the list of 233 has been reduced to a list of 99.

I also want to tell you, Mr. Chairman, that I met, as well as you did, with the senior officials from the Health Industry Manufacturers Association earlier this week, and at that meeting, HIMA, as it is called, told us that they are going to reverse their policy of non-cooperating with the Food and Drug Administration's requests for information and they are going to issue a letter early next week urging their 800 members to cooperate with all requests for information.

There are a lot of other medical devices, but there are 2,700 manufacturers that may have Year 2000 complications. HIMA represents 800 of that 2,700, so it is not all inclusive, but they are urging very strongly their members to cooperate fully with the requests from the Food and Drug Adminstration and from hospitals and clinics around the country.

We have, after much unnecessary obstruction, I might point out, from the Health and Human Services Agency, obtained from the

FDA the list of the 2,200 manufacturers of computerized medical devices that have not responded to their June 29 letter. We are going to guard it closely right here for a few weeks. I said I would earlier release that this week if people did not start complying. They have, and we will wait another couple of weeks to see whether or not the progress on that is as good as it has been in the first week. If it is not, then my intention would be to release the list of companies that are not responding to these basic requests for information about their equipment.

Chairman BENNETT. They are not compliant or they are not functional or they are not ready.

Vice Chairman DODD. Well, maybe neither in this case. It is hard enough to fix these issues and talk about them, but if the companies are not letting the agencies know and the Veterans Administration know whether or not their equipment is going to work or not, that is just pretty standard stuff, if you cannot even communicate with them. So we will see how it progresses here over the next couple of weeks.

On this issue here, just very briefly, when it comes to telecommunications, I guess the bottom line in some ways is that the telecommunications industry will be collectively calling, I guess, sort of 911, and if we do not deal with this problem effectively, they could end up with a busy signal there come January 1 and that is the reason for getting into all of this issue this morning.

I will reserve, Mr. Chairman, the balance of the statement for the record.

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

Vice Chairman DODD. I just would raise a couple of questions here. One is, this is a unique problem in the sense, and the chairman has already addressed it in part, in that everyone else we have talked to gets a period for testing. We have talked to people who say, well, we are going to do it on weekends. There will be holidays when the businesses are down. We can bring people in. We can spend a couple of days and really run the traps on this. The problem in the sense of telecommunications is there are no weekends off. There is no holiday in which you can sort of take a break from all of this and run systems to see how well they work. I am very interested in pursuing the testing element of all of this and the contingency ideas.

Second, I wonder if you might address the global questions here, as well. As I understand it, this chart here represents domestic systems, and that what you have not included here or we have not included is the global communications. We have done a lot of work on financial services, but utilizing global telecommunications as a way of transmissions of major monetary denominations and securities and the like, it seems to me, is critical, and obviously, our systems link up—I presume they do—with international communications systems.

If you had to take this chart and add a new egg, or whatever you want to call those round pieces here, and put the international quotient in there, how many red boxes would we, to put it very sort of non-technically here, how many red boxes would we see had we

had an international communications function included in this graph?

Ms. LIST. I would be happy to address both of those questions. First, the testing one. You are absolutely right. One of the challenges with telecommunications networks is you cannot take them off-line to do testing and you do not want to do testing in a live network. So the challenge is to find enough facilities between various laboratories the carriers may have, the suppliers may have, that other service providers may have in order to do both standalone testing as well as interoperability testing, because you not only want to test individual networks, obviously, this is a complex interconnected system and there is a need to do interoperability testing between those systems.

I believe some of my esteemed colleagues on the industry panel later on will be addressing some of their efforts with regard to doing that kind of interoperability testing, but it does pose a particular challenge for the telecommunications industry.

With regard to international issues, the networks of international carriers and of telephone companies within particular countries do not look vastly different than the interexchange carrier picture here or the local exchange carrier picture in the sort of aqua shading in terms of the ways in which those networks are configured. They have switches. They have tandems. They have other network elements that provide service. So they do not look terribly different.

There are different equipment manufacturers who are represented largely in the international marketplace versus some of the equipment manufacturers that are represented domestically, but much of the functionality is the same. And the way in which calls are processed also is very much paralleled by the domestic picture that I have provided here.

So, again, in terms of actually setting up a call, there is not a lot of date-sensitive processing that goes on in that call setup. My concerns have to do with the general lack of attention to Year 2000 in some parts of the world. It is not just the telecommunications industry, it is the financial industry, it is the bank, it is the public utilities, and that those may have an impact on the ability of a telecommunications carrier in another part of the world to be able to continue to be operational, because they may have extended power outages or they may not be able to pay their employees or collect revenues and that may impact our ability to originate or terminate calls in those parts of the world.

Vice Chairman DODD. Just last on that, at some point here, we joke about it a little bit, but we have got to have some clarity here on the definition of terms. I tease a bit about it, but I am not terribly comfortable with the notion that the word "functional" that is being used here and what we mean by "compliant" and "ready" and what you mean by "functional" or what others mean by "functional" is disconcerting to this one member. Maybe I am the only one, but it is troubling to me that you have got a distinction between the words "functional" and "compliant".

Ms. LIST. It is really just a clarification issue. I mean, if you read the definition, the definition says that our systems will process dates in the same manner before the Year 2000 as after the Year

2000 and that they will process dates over the leap year rollover. We also are very clear about what our testing strategy is and the extent of the testing that we do on our products before we will call them Year 2000 functional.

Our concern really is that there are very various definitions of compliance, many of which we do not believe go as far as our definition of functional does.

Vice Chairman DODD. Is this the legal department that came up with that word?

Ms. LIST. Of course. [Laughter.]

And it is better than Year 2000 hopeful. [Laughter.]

Chairman BENNETT. Thank you. It is, indeed. It is, indeed.

Ms. LIST. I am waiting for people to start using that term.

Chairman BENNETT. Senator Collins, we welcome you.

Senator COLLINS. Thank you very much, Mr. Chairman. I have an opening statement that I would request be submitted for the record.

Chairman BENNETT. Without objection.

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

Senator COLLINS. I apologize for being unable to be here earlier. I have reviewed the testimony of Dr. List and I appreciate her being with us this morning.

Dr. List, in your written testimony, you talked about large corporations being more attentive to the Y2K problems than are small Main Street businesses. Now, obviously, a lot of the telecommunications network is controlled by large corporations, but certainly small businesses also have their own internal systems. Could you comment and expand on your comment on what the impact on small businesses will be with regard to the telecommunications Y2K problem?

Ms. LIST. Yes. It really depends on what their own internal network looks like. Many small businesses rely on the public switch carriers to provide their telecommunications services for them, in which case many of the things that I have discussed in terms of the public switch network would address the kinds of services that they can expect to receive after the turn of the century.

Some small companies, though, do have some of their own private equipment. They may buy or lease a private branch exchange, which is simply a kind of switching system that allows you to do four-digit dialing inside the office and those kinds of things. They may have an automatic call distribution system. For example, I would imagine the Senate does. When calls come in, they may be routed automatically to different Representatives who are service providers, who may be able to answer questions or those kinds of things.

Those pieces of equipment do have some date-sensitive information in them. For the private branch exchange, the small switch, it is very similar to what a larger switch has. So it may do some date and time stamping so that they can keep records of when calls came in, how long they lasted, how quickly they were answered. It may also do some administration and maintenance functions on a scheduled basis that would carry date and time information, and they would want to know that the manufacturer who produced that

equipment, if they bought it, or the company who is leasing it to them is addressing the Year 2000 issues in that equipment so that it will continue to perform those functions.

Automatic call distribution equipment is of particular interest because there are automatic call distribution pieces of equipment that do schedule changes of routing over time. Let me give you an example. This is really for a larger company, but I think the example may be applicable to smaller ones.

Some companies that provide customer service want to do it on a 24-by-seven basis, so 7 days a week, 24 hours a day, they want to be able to provide services, or they want you to be able to order from their catalog anytime you want to. In order to do that, they very often have call centers that are in different time zones, and this automatic call distribution equipment routes the calls depending on the time of day, day of the week. That is date-sensitive information and that routing, if the Year 2000 issues are not addressed, may not work effectively when the rollover of the millennium happens.

The other places that you see date-sensitive information are in voice mail systems. So, again, date and time stamping of when messages are left, as well as in some of the routine maintenance and operations functions.

Small businesses really need to be aware that there are Year 2000 issues and work with their suppliers, whether it is a supplier of public switch service, whether it is a supplier of a piece of equipment, either on a purchased or leased basis, in order to assess and address any Year 2000 problems they may have.

Senator COLLINS. Is the telecommunications industry making an effort to reach out to smaller businesses? Are suppliers of the automatic call distribution equipment, for example, contacting their customers to let them know that there may be these problems?

I am fairly confident that large corporations are going to be able to solve the Y2K problem, but I am very concerned about small businesses that may be linked to larger companies and what the impact will be on them. It seems to me there is some obligation on larger companies, the suppliers in the telecommunications industry, to do affirmative outreach. I do not know whether a lot of small companies would even realize they were vulnerable in exactly the way that you very articulately explained.

Ms. LIST. Yes. I cannot really say whether, across the board, companies are doing that. I think some of the members of one of the later panels might be able to address the activities that they have in place in that regard.

I can tell you that for our company, we are proactively contacting our customers to let them know about the state of readiness of our systems, our products, as well as to advise them of some of the consulting services that we provide for them, that they need to address Year 2000 issues in networks that they are putting in place and those sorts of things.

Senator COLLINS. Thank you, Dr. List.

Thank you, Mr. Chairman.

Chairman BENNETT. Thank you. We appreciate your presentation. We anticipated that it would be a brief scene setting and

the interest of the members of the committee have kept you here longer than you anticipated. We are grateful to you.

Ms. LIST. Thank you.

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

Chairman BENNETT. We now welcome the Honorable Michael Powell, Defense Commissioner of the FCC; Dr. Jack Edwards, speaking for the President's National Security Telecommunications Advisory Committee; and Ms. Diane Fountaine, Deputy Manager of the National Communications Systems.

We appreciate your being here. You have heard the testimony and the questions, so I think you have got a flavor now overall of the main concerns that we have on this committee.

Commissioner Powell, we will start with you and welcome you here to the committee. I will say that Commissioner Powell has been to see me privately in advance of this hearing and we have had conversations about this and he has made it clear the FCC is anxious to work on this issue and he himself is going to be available, and we are very grateful to you, sir, for that willingness to help.

STATEMENT OF MICHAEL K. POWELL, DEFENSE COMMISSIONER, FEDERAL COMMUNICATIONS COMMISSION

Mr. POWELL. Thank you, Mr. Chairman. It is a pleasure to be here, and Senator Dodd, it is good to see you. I have also met with you prior to the hearing. And Senator Collins, I hope to see you at some point at your desire.

I commend the Senate Special Committee on the Year 2000 Technology Problem for its active participation on this issue. I welcome this opportunity to share with you what the Federal Communications Commission has learned about industry efforts to address the Year 2000 problem and to discuss the fundamental importance of the national telecommunications infrastructure and the potential impact of the Year 2000 problem on embedded telecommunications networks and systems.

At the FCC, we are working to promote an effective public-private, mission-oriented, partnership to ensure that users of telecommunications services enjoy as close to the same level of quality and reliability on and after January 1, 2000, as they do today. We believe that the FCC can play an important role in facilitating the development and dissemination of critical information among carriers and to their key customers. Timely dissemination of information will increase the sharing of solutions, avoid duplicative testing, help companies spot undetected problems, and reduce customer uncertainty and anxiety.

We have developed and continue to work on strategies for outreach and advocacy to all the industries we regulate, including wireline and wireless telephony, cable, radio and television broadcasting. We also have been looking into ways to facilitate the development of effective contingency plans in the event that a major disruption to the network should occur under our authority and in cooperation with NCS.

Although we have Y2K programs for all the various telecommunications industries, my remarks today will focus mainly on

wireline telecommunications carriers, and Mr. Chairman, I would ask that my full statement be entered in the record.

Chairman BENNETT. Without objection.

Mr. POWELL. Thank you. As an initial matter, it is important to remember that no single entity owns or controls the public switched telephone network, and this is part of the challenge. In addition to the major telecommunications companies that provide service to the majority of the country, there are also 1,400 small to mid-size independent telephone companies that serve many rural and insular parts of the country, as well as U.S. territories and possessions. And each of these companies is only one in a long chain of interdependent companies required for the network to operate. Without a doubt, the telecommunications network is a tremendously complex and interdependent thing, and consists of millions of interconnected parts.

As a result, the ways in which the Year 2000 problem could affect telecommunications companies is almost unlimited. However, I believe that with time and greater knowledge of the scope of the problem and by maximizing the amount of information available to all companies facing the Year 2000 problem, we will be able to better predict where and how the problems in the network are likely to occur. In my role as Defense Commissioner, I plan to work closely with the industry, NCS, and the Network Reliability and Interoperability Council to help attack these problems.

We have sent over 200 letters to major companies and organizations in all sections of the telecommunications industry, asking them about their efforts to become Year 2000 ready. In June and July alone, we organized eight informational forums with representatives of different sectors of the industry to facilitate information sharing and learn how the FCC can further assist industry efforts to tackle this issue.

I also represent the Commission on the President's Council on Year 2000 Conversion and co-chair the Telecommunications Sector Group of that organization. In an attempt to better facilitate communication, I have asked also representatives from each of the communications industries to sit on that group.

Our general assessment of the telecommunications industry remains positive, much as Dr. List described. Our inquiry letters, for example, asked 20 wireline carriers, accounting for more than 97 percent of the country's access lines, to report on their critical systems. We learned that, generally, the carriers have completed their review of the inventory for these systems. They have completed assessing the impact of the Year 2000 problem on these systems and have set completion dates for remediation, testing, and integration by the second quarter of 1999.

The information we have received suggests that the major U.S. equipment manufacturers also will be able to meet projected demands for equipment. The manufacturers report that most of their software and hardware products are already Year 2000-ready and have been made available to customers. They have further targeted the end of this year and the first quarter of next for general availability of all their products.

The major carriers also are cooperating on integration and interoperability testing, as you heard. The Telco Year 2000 Forum has

contracted with Bellcore and is already performing integration testing on Year 2000-ready equipment. ATIS will conduct inter-network interoperability testing in January and February of 1999 and is also working with Bellcore.

The Network Reliability and Interoperability Council, NRIC, as it is called, will also play an oversight role with respect to testing. I would like to take this opportunity to announce that, at our request, Michael Armstrong, the Chairman and CEO of AT&T, has agreed to be the chair of NRIC. NRIC will play a central role in our Year 2000 effort. We believe that that organization will be invaluable in coordinating overall testing, collecting and disseminating information, and advising the FCC on the status of industry readiness, and assisting in the facilitation and development of contingency plans. A representative of NRIC will also sit on the Telecommunications Sector Group of the President's Council.

While we have programs in place to work this problem, all that we have observed is not comforting. With regard to the independent telephone companies, it is important to note there are some 1,400 of them that serve the rural and insular parts of our country. The Commission is working continuously to find ways to reach out to these companies and make sure that they are aware of the problems and are taking steps to address it.

But that pales in comparison to our concern about international telecommunications carriers. The United States, Canada, and the U.K. are forging ahead, but we have many profound concerns about carriers in other nations, especially those in developing countries, that have not yet taken necessary steps to prevent system failures. We have been working independently to address this issue, as well as monitoring the work of the International Telecommunication Union.

In my role as Defense Commissioner, I have endeavored to make sure that the FCC is ready to continue its own operations in the event of national emergency. In this regard, the FCC's Compliance and Information Bureau has been revising the agency's continuity of operations plan as well as a plan to maintain our ability to coordinate and grant special authority to help companies continue operating in time of emergency. With respect to national emergency plans, CIB is reviewing and are updating these now. I will work with NCS and the industry to continue to examine the appropriate role of the FCC in the event of an emergency.

Without a doubt, I should say, the legal liability issue which has been raised is a serious impediment and continues to impede the flow of timely and candid information. We support the efforts to pass legislation that would promote the exchange of information by limiting the way such information could be used against a company. I believe there is a significant role to be played by the Congress and the administration with regard to the legal liability issue and other barriers to information flow.

As we move closer to the millennium, all of our concerns, of course, become more acute. I believe that the FCC has begun to establish the kind of inter-company and private-public partnership that will facilitate the flow of information and get it to those who need it most. It will also permit the government to become aware of and respond to the needs of the industry as they arise. Our na-

tional well-being is dependent upon the reliability of the nation's telecommunications networks, and government and industry must work together to ensure that whatever disruptions occur do not lead to widespread outages and failures. To that end, the FCC is committed to taking whatever actions it can to facilitate the industry compliance efforts.

Thank you, Mr. Chairman, for the opportunity to be here and I am happy to answer any questions may have.

Chairman BENNETT. Thank you very much. We will get to the questions at the end of the panel.

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

Chairman BENNETT. Dr. Edwards, you may proceed.

STATEMENT OF JOHN S. EDWARDS, CO-CHAIR, NETWORK GROUP, THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE

Mr. EDWARDS. Thank you, Mr. Chairman, for the opportunity to testify here today on behalf of the President's National Security Telecommunications Advisory Committee, NSTAC. I am Jack Edwards, an Industry Executive Subcommittee member of the committee and chair of its Network Group.

For the past 16 years, the Committee has worked jointly with the National Communications System to advise the President on national security and emergency preparedness issues pertaining to the reliability and the security of telecommunications and information infrastructure, issues critical to national security and commercial interests. The Y2K changeover is an urgent matter, Mr. Chairman, and it is at the forefront of our effort.

In January 1998, the manager of the National Communications System asked the NSTAC to update the President on the telecommunications industry's actions to ensure continuity of service through the millennium change. In response to this request, the NSTAC's Network Group addressed the Y2K problem and is developing a report on the efforts to prepare the telecommunications infrastructure for Y2K, factors affecting these efforts, and possible implications if these efforts are not fully effective.

We broadly reviewed the telecommunications industry status by soliciting briefings from interchange carriers, local exchange carriers, switching system vendors, large-scale systems integrators, and Y2K risk assessment and remediation solution providers. We heard from all of these sectors. Representatives freely reported to us as NSTAC promised to use the information without attribution. Our report includes a consideration of the current Y2K readiness of the major telecommunications service providers and equipment vendors.

Efforts to make the telecom infrastructure Y2K ready are well underway. In fact, the major service providers and the vendors have been working on these issues for several years. Those who briefed the Network Group on their Y2K initiatives expect the majority of critical products and networking to be Y2K ready between late 1998 and early 1999.

However, in spite of the resources being devoted to this complex task, all agree that it is not possible to foresee and test for every

possible adverse interaction. Since Y2K readiness preparation is a massive software augmentation, even the most thorough, exhaustive efforts may fail to achieve 100 percent success.

No organization in private or government in its brief to the NSTAC's Network Group offered a guarantee of total Y2K eradication from its network, services, or systems. In addition, these organizations could not offer guarantees of the adequacy of the Y2K internetwork interoperability testing.

Compounding the problem, many felt that the millennium change was not a January 1, 2000 problem, but could begin before and extend well after that date.

The Network Group's Y2K report is pending final approval by the NSTAC, so I apologize for being unable to make specific comments on the Group's findings and recommendations at this time. However, I can say that our report will recommend actions for the President to enhance the Y2K readiness for national security and emergency preparedness telecommunications and to mitigate any impact of Y2K-induced service disruptions in the nation's security and emergency preparedness posture. Further, it recommends actions for the NSTAC to help the Government respond to Y2K-induced service disruptions. When approved, the recommendation will be forwarded to the President and subsequently made available to all interested parties.

We have also been asked to comment this morning on the NSTAC's 1997 report to the President addressing the probability of a widespread telecommunications outage. While this report preceded and is not directly connected to the NSTAC's current Y2K assessments, it is highlighted today to convey our understanding, contingency planning for, and recovery from a severe telecommunications outage, should one occur.

For the purposes of the report, NSTAC developed a definition of a widespread telecommunications outage. Specifically, a widespread outage would be a sustained interruption of telecommunications service. It would last for at least a significant portion of a business day, interrupt both local and long distance services in at least one region of the country and including at least one major metropolitan area, and significantly degrade the ability of other infrastructures to function.

While we determined the likelihood of a widespread telecommunications outage was low, the potential impact warrants careful consideration. Service availability and reliability are hallmarks of the telecom industry. With respect to internetwork connectivity, there are agreements in place amongst the carriers whereby, in the face of trouble, the local exchange carrier can redirect traffic to an alternative interexchange carrier. However, in the new regulatory environment, business restructuring to accommodate competition, the deployment of new technologies and the introduction of new services do create unknowns. In this environment, it is critically important to do nothing to increase the probability of a widespread outage. Continual attention needs to be placed to how these unknowns affect security requirements.

In all this, contingency planning is key. Recognizing there can be no ironclad guarantee against a widespread outage, the report offered several cost-effective recommendations for the President and

the NSTAC to further decrease the overall probability of a widespread outage and to improve recovery plans and procedures. These recommendations centered on the coordination amongst the operators, improvements of software integrity checking, and information sharing amongst the various entities.

Our critical national infrastructure relies on a growing and vital web of communications, computer, and associated information technologies. Furthermore, the gamut of threats, including those posed by Y2K, could disrupt critical infrastructures, for example, electric power, on which the infrastructure is highly dependent for sustained operation.

Understanding and addressing the interdependent nature of critical infrastructures are immensely important to protecting the Nation from unmanageable crises, such as a Y2K problem, and must not be overlooked.

The NSTAC believes the telecommunications infrastructure is robust and reliable, but even the most exhaustive efforts cannot guarantee total eradication of problems from the network services or systems. The NSTAC will continue to focus on national security and emergency preparedness communications problems and overall continuity of service in light of the Y2K problem.

We appreciate the opportunity to testify today. The NSTAC looks forward to sharing the results of the Y2K analysis with you pending final consideration and approval of this report. Thank you, Mr. Chairman.

Chairman BENNETT. Thank you, Dr. Edwards.

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

Chairman BENNETT. Ms. Fountaine, we appreciate your being here and look forward to your testimony.

STATEMENT OF DIANE FOUNTAINE, DEPUTY MANAGER, NATIONAL COMMUNICATIONS SYSTEM

Ms. FOUNTAINE. Thank you, Mr. Chairman. Good morning to you, Senator Collins, Senator Dodd, and Senator Bingaman. I appreciate the opportunity to address you on behalf of the National Communication System's Executive Agent, Defense Secretary Cohen, and its Manager, Lieutenant General Kelley, on the crucial role and initiatives that the National Communications System is taking to meet the Year 2000 challenge as it applies to national security and emergency preparedness telecommunications.

The National Communications System is a confederation of 23 agencies across the Federal Government tasked with ensuring the availability of a viable national security and emergency preparedness telecommunications infrastructure. National security emergency preparedness telecommunications are those emergency communications required by the Federal Government during the conduct of business under all conditions, including and ranging from peacetime to national emergencies to international crises or war.

The Manager, National Communications System, is also the designated Federal official for the National Security Telecommunications Advisory Committee, which was established in 1982 by President Reagan in anticipation of the divestiture of AT&T. The Committee is limited to 30 Presidentially-appointed senior execu-

tive industry leaders, often chief executive officers, who provide the President with a unique source of national security and emergency preparedness telecommunications policy expertise and advice.

Mr. Chairman, the Office of the Manager, National Communications System, shares in the concerns expressed by this committee relating to the Year 2000 compliance issue. In addressing the Year 2000 issue, we are focusing on three primary areas: First, on the national security emergency preparedness capabilities that we contract with the interexchange and local exchange carriers to develop and maintain in the commercial public networks; second, on the overall voice services in the public networks which are the primary foundation of national security emergency communications; third, on the contingency plans that we follow during a national security or emergency event.

First, let me address the unique capabilities that we have implemented in the commercial network for national security emergency telecommunications. We have contracted with the primary interexchange and local exchange carriers to develop and implement a capability in the public network to identify a priority national security or emergency call and then give that call priority treatment through the network. This Government emergency telecommunications service allows national security and emergency response users to use a dedicated area code, 710, to receive priority switched voice and voice band data service in the public switched network.

In addition, for a Federal user or a federally-sponsored user who requires priority restoration or activation of a telecommunications service for national security or emergency reasons, we have implemented the telecommunications service priority system. This system allows us to identify to the telecommunications companies the circuits which should be given priority during activation or restoration.

Testing of the telecommunications service priority system for Year 2000 compliance can be conducted independent of the live public network and has been completed. Minor problems were discovered which are being corrected. Because the Government emergency telecommunications service capabilities are internal to the operational switches in the networks, we will test those functions in a test network.

To achieve this, we are collaborating with the Alliance for Telecommunications Industry Solutions, which is establishing a Year 2000 test network that will emulate major portions of the public switched network. The Government emergency telecommunications service testing requirements were outlined at the last meeting of the Alliance's network testing committee, which was held in June. They accepted the proposed scenario for Government emergency telecommunications service testing and requested further details to include a draft test script and an implementation summary, which we will present at their next meeting in August. Bellcore is assisting us in this effort and this testing should be completed in March of 1999.

Specific testing will include the ability to recognize the 710 area code and successfully complete priority calls end-to-end over local and interexchange carrier networks. While the scope of this government emergency telecommunications service testing is limited, it

does provide us with a single test bed of our major service providers and the benefits gained from internetwork testing among several major carriers in the U.S. telecommunications infrastructure are substantial.

To assess the overall voice services required for national security telecommunications, the Manager requested that the National Security Telecommunications Advisory Committee focus on the Year 2000 issue as it relates specifically to national security, emergency preparedness, and the national telecommunications infrastructure. The committee's Network Group has completed the initial assessment of this subject, as you have heard from Dr. Edwards, who is the Network Group's chair. This report will be reviewed by the National Security Telecommunications Advisory Committee principals at their upcoming meeting on September 10.

As I indicated earlier, in implementing special national security emergency capabilities in the public network, we chose the major interexchange service providers and the primary local exchange companies.

Based on information gathered by the National Security Telecommunications Advisory Committee Network Group and discussion with individual companies, we believe that there will be little or no interruption of service from these major service providers due to the Year 2000. While the individual companies are conducting extensive network element testing and intranetwork interoperability testing, the biggest challenge, we believe, for all of these companies will be the testing of their networks' external interfaces, both domestic and international. Ensuring the interoperability of these various solutions is critical, particularly in a system as complex as the U.S. telecommunications infrastructure, and this is why the Alliance for Telecommunications Industry Solutions internetwork testing is so important.

Even though we do not expect a major telecommunications service interruption resulting from Year 2000, we are putting a great deal of emphasis on proper planning for a contingency in this area. In 1983, we established an operations center, staffed by both government and industry personnel, for the coordination of telecommunications required during a national security or emergency event. The National Coordinating Center for Telecommunications is reviewing current operational response procedures and the existing national telecommunications coordinating network, looking for variations to current process or backup connectivity that might be peculiar to the Year 2000 problem. For example, we may add connections to software experts from the telecommunications switch manufacturers which, up until now, we have not done.

Since 1992, we have had a system for communications with key telecommunications locations that is independent from the public network and we use primarily high-frequency radio capabilities. We are now augmenting that capability with additional non-public network and satellite communications connectivity among critical national security emergency preparedness operational sites, major service providers and equipment manufacturers. This additional connectivity will allow us to coordinate with the telecommunications industry and key Federal operations centers in the event of service disruption resulting from Year 2000 complications.

Additionally, we are adding a state-of-the-art capability to cross-connect various communications media that will be available in the coordinating center by the end of this Year. This capability will extend to our continuity of operations site in the event relocation out of this area becomes necessary.

In conclusion, Mr. Chairman, we are working with the National Communications System Federal agencies and departments and the National Security Telecommunications Advisory Committee member companies to provide continuous national security, emergency preparedness telecommunications services prior to, through, and beyond the millennium change. While we have accomplished a lot, there is still much to be done, particularly regarding internetwork Year 2000 testing and contingency planning. I would urge the committee to support the efforts underway in the telecommunications industry and continue to stress the importance of internetwork interoperability testing as this work progresses.

Mr. Chairman, this concludes my statement on our efforts toward solving the Y2K problem and I would be happy to take any questions that you have at this time.

Chairman BENNETT. Thank you very much.

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

Chairman BENNETT. We have had so far today a picture that is basically reassuring. That is, yes, that this is a serious problem. Yes, it is very complicated and very complex, but we are pretty much on top of it and we are going along just fine and, basically, we are going to be all right.

I hope that is true, but I have to share with you before I get to specific questions some of the reactions of people outside looking in on the telecommunications challenge. In an earlier hearing by this committee on financial services, one of the witnesses, Tanya Bader, who is a principal in the Capital Markets Advisors Financial Group, said, and I quote, ''Most large financial firms conduct 80 percent of their transactions electronically and 25 percent or more of their transactions in the inter-bank market. To summarize the remarks that many Y2K chiefs have in this area, 'We do not have a clue.' This leads me to conclude that reliability in telecommunications is a Y2K wild card.''

Now, I have to add that Ms. Bader was one of the more thoughtful and well-versed witnesses that we had appear before this committee. I hope she is listening to this and I hope she will be reassured by this panel that that demonstrates that there is at least that aspect outside the telecommunications industry that is concerned.

Now, another one from overseas. This comes from the Year 2000 task force chairman in the United Kingdom named Ron Balls, addressed to our committee staff. He says, ''Further to our discussion, please find associated a copy of the ITU questionnaire. As you can see, this was sent out on April 17 with a request for information by May 25. Responses from the USA have been poor so far in terms of the number received and the reference to the legal position. I would like the FCC to take an active role in assuring that we receive quality responses from, (A) U.S.-based carriers, (B) U.S.-based regional operators, or RBOCs, and to consider how best to

deal with the USA local operators. The intent is to publicize the general position of each operator on the ITU external web site within the next 2 weeks and continue to update this as more information is received. I hope this assists," signed by Ron Balls.

There is a little bit of a disconnect here, of the perception outside of the telecommunications industry and the rather rosy picture we have received today. So against that backdrop, let me say, Commissioner Powell, you mentioned in your statement that the FCC had sent out letters of inquiry to 200 major companies and organizations, asking them about their efforts to become Year 2000-compliant. Can you tell us when you sent those letters out and how many of those 200 organizations that responded?

Mr. POWELL. Senator, it has been a rolling process, but the vast majority of the letters went out in May and the beginning of the summer. Let me break them down for you, because that 200 covers all the industries we regulate.

With respect to wireline carriers, we sent out 20 letters to the top carriers that cover more than 97 percent of the country's total access lines, and one thing I am pleased to report is we have a 100 percent response rate from that category, so we have received letters from all 20.

Other areas are not as responsive, but somewhat encouraging. With respect to mass media, which is broadcasting properties, television and radio, we have about a 31 percent response rate. With respect to wireless telecommunications systems, which would include about 53 wireless commercial and private entities, and another segment which we worry about quite a bit, the public safety community, we sent another 55 letters. With respect to the commercial and private wireless, we received to date only 11 responses. With respect to——

Chairman BENNETT. Eleven out of how many?

Mr. POWELL. Fifty-three. Wireless is one of our areas of concern, for obvious reasons.

Chairman BENNETT. So that is about 20 percent.

Mr. POWELL. Yes. Public safety is even of greater concern. This is not an entity we specifically regulate, but it is an area we are concerned about because they operate a lot of privately-held wireless equipment. This is fire departments, police departments. We got 1 response out of 55.

What this helps us do is understand where there needs to be a much more dramatic outreach effort. We tend to see that, often, lack of responses is a result of lack of awareness and lack of understanding of how to respond, so we are going to try to do something to ramp up our efforts with regard to that last segment.

Chairman BENNETT. Thank you. I will reserve my time and we will go to Senator Bingaman, who has made this something of a specialty, and we are grateful to him for his expertise on this.

Senator BINGAMAN. I do not claim any expertise, Mr. Chairman. I have an interest.

Let me ask about the extent of the interoperability testing. I think the previous witness testified that this was very important and we needed to have more interoperability testing. I think that was one of the recommendations that Bellcore has made. How ex-

tensive is this testing at the present time? Who should I ask that to, Dr. Edwards?

Mr. EDWARDS. Thank you, Senator Bingaman. In our information gathering in the Network Group, we had occasion to hear from several interested parties and one of the things that comes to mind earlier in remarks, contrasted—taking systems off-line and testing them in the telephone industry, you do not have that luxury. There are two things that come to my mind.

One is that the telecommunications business is—the programs are complex, but they are very single-minded and the main function is to make phone calls happen. Changes come rather slowly by comparison to changes in other kinds of programs that you might buy commercially.

We had testimony or a report in our group from a corporation which was doing Y2K remediation testing in the non-telecom market. They indicated a difficulty because when they went to test the systems, the systems owners and operators really did not know what they had because they had been modified over the years. Things had been added, features had been changed and modulated.

In the telecom industry, features are added very carefully and tested very carefully. We do a complete regression testing, where we have a set of test conditions and if you change something in the program, you have to repeat the test over the total path of this. Consequently, all of the people that came to our committee told us how much resource was devoted to just sheer testing, because once the systems are returning to the service, you do not have the luxury of turning them off and trying it again, so the testing is terribly important, as you will hear from the next succeeding panel. They will go into that in great detail, I am sure.

But there is a very good contrast between the telecom example and the non-telecom example in that the first step they had to do in the non-telecom example is to find out exactly what they had, to develop a regression test, because it is one thing to fix the Y2K and get that right, but you may change something else. The comment about the errors, the errors that you introduce are not always in the code you are changing. You can introduce an error which shows up over someplace else, and unless you test the entire system when you are done, you cannot be sure. It may be Y2K-compliant, but it may fail for some other reason later on because you introduced a spurious error. So testing is terribly complicated and has to be done with the entire system under test.

Senator BINGAMAN. What I am trying to figure out is how much of this interoperability testing ought to occur and how much of it has occurred or is occurring? I mean, have we done 10 percent of what ought to be done? Have we done 90 percent of what ought to be done? I guess that is where I trying to——

Mr. EDWARDS. As you will hear from the next two panels, the Y2K Forum people and the ATIS people both came to our group, testing is proceeding this fall up through February.

Senator BINGAMAN. Now, ATIS, I was led to believe, only involves a very few companies. Am I wrong about that?

Mr. EDWARDS. Well, the testing is interoperability testing amongst the local exchanges and interexchange carriers.

Senator BINGAMAN. I will wait and hear from the Commissioner. Mr. Powell, did you want to say something?

Mr. POWELL. Yes, just to help clarify a little bit. There really are two testing forums. There is the Telco Year 2000 Forum, which is a coalition of the major local exchange carriers. This would be Bell Atlantic, Ameritech, the sort of large local exchange carriers, and they are primarily focusing their testing efforts—and they are here on the second panel and you can ask them with specificity—they are testing the components and the intra-network operations. And then, essentially, there is sort of this roll-up to the interoperability testing, which is being facilitated by the ATIS forum.

The Telco Year 2000 Forum's testing efforts are presently underway and will continue, I think, for the rest of this year, and then that will turn to the interoperability testing phase with ATIS beginning in January and hopefully concluding in February.

ATIS is an extensive organization. It includes not only local exchange carriers to some degree but it also includes the majority of the long distance carriers. It includes equipment manufacturers. Believe it or not, it also in some respects has other kinds of service providers, like cable representatives, et cetera. It is a very—a pretty extensive organization, the interoperability testing element.

Senator BINGAMAN. Let me ask Dr. Edwards one other issue here. In the recommendations that NSTAC makes, you have one in here, the second one, I believe, to remove the legal and regulatory obstacles for widespread outage recovery, and underneath that you say it was recommended that the President encourage the FCC to guard against premature implementation of unseasoned technologies that might contribute to the possibility of a widespread outage.

Does the FCC have the authority and the capability to guard against the implementation of unseasoned technologies? That seems like a pretty tall order, to me.

Mr. EDWARDS. Yes.

Senator BINGAMAN. Yes, they have got the authority, or yes, it is a tall order?

Mr. EDWARDS. Yes, it is a tall order. [Laughter.]

What we were trying to do there is concerned with how new technologies and new entrants come into the business, and I think it is more at that level. As competition arises, we are concerned that it be expanded in a careful, rational method and the possibility for entrants into the marketplace that are not careful, that bring in untested technologies, is one that could cause some concern to us, and that is the reason for the recommendation.

Senator BINGAMAN. I can share the concern. I guess I just have never thought the FCC was staffed and equipped to perform that function. Commissioner Powell?

Mr. EDWARDS. I think we hope that the NRIC will help provide some rationalization in that area, not the FCC itself, necessarily, but the FCC with the help from the NRIC, which is looking into security issues and robustness issues.

Senator BINGAMAN. Let me just ask Commissioner Powell, is there any capability to do this in the FCC or anywhere else that you know of? Is there any governmental entity that is taking on

the job of guarding against premature implementation of unseasoned technologies? That is an interesting concept.

Mr. POWELL. Yes, Senator. Candidly, not really, in the sense that there is little in our economic regulatory authority that allows us to prevent the introduction of new technologies by private carriers in a competitive environment, and the strain is even greater as we implement the Telecommunications Act of 1996, which expressly contemplates, as the will of Congress, the sort of greater increased deregulation and lesser input on the business decisions about the deployment of technologies. So we, as a large measure, have a technology-neutral policy, and even if we did not, we would have an incredibly limited ability to prevent the introduction of new goods and services in the market.

I would also say I am not so sure you would always want to do that. A lot of the new and advanced technologies that are bringing great benefits to consumers also potentially provide new solutions to problems that might be more acute in the legacy systems.

I think the concern is a valid one, though. That is, we want to be sensitive to the hastiness that sometimes excitement about new competition can bring. But beyond articulating the concern, I have a hard time understanding practically how the FCC could sort of execute that recommendation.

Senator BINGAMAN. Let me ask one other question of you, Commissioner Powell. You are the Defense Commissioner, correct?

Mr. POWELL. Yes.

Senator BINGAMAN. Could you tell me what authority that office carries with it? I mean, what can you do as the Defense Commissioner that another FCC commissioner could not do?

Mr. POWELL. It is a fair question. It is evolving, to some degree. But, essentially, what it does is that there has been a clear recognition that the national security and emergency preparedness apparatus of the United States in the execution of their operations have a real-time need for a single point of contact in the Federal independent regulatory agency simply because we are the steward of the legal and regulatory regime that can influence or impede the ability to sort of reach certain national objectives.

So in large measure, I serve as that single point of contact at the Federal Communications Commission for that apparatus. So, in a sense, it is a point of contact role. It is a coordination role. But there are some limited circumstances under which, in the execution of continuity of operations plans, I have some authority to take action on behalf of the Commission without needing the vote of the full Commission.

If the President—you know, I do not want to go through them in complete detail in this open forum, but if the President were to declare a national emergency and execute his authorities under that regard, there would be certain steps that I had the authority to take and would not have to call a meeting and get the majority vote of three of the five.

So that is largely what it has been, and it has been natural to use that position—that is how I sort of got into being the principal representative of the Commission on efforts like this, when the White House is looking for someone who oversees those sorts of issues.

Senator BINGAMAN. Thank you, Mr. Chairman.

Chairman BENNETT. Thank you. Senator Dodd.

Vice Chairman DODD. Thank you very much, Mr. Chairman, and I thank all of you for being here, and Mr. Powell, thank you, as well, for coming by the office a few weeks ago and bringing us up to date on your efforts.

I want to sort of pick up on, I think it was the lead question the chairman had, and this is sort of a theme we are working through these issues as they come before us. As I said earlier, there is a tendency, and I think it is true of any institution, obviously, to try and put the best foot forward in public hearings like this, and yet I think it is important for us to also gather information from outside to determine whether or not we are moving as aggressively and as thoroughly as could be the case.

In addition to the comments at an earlier hearing that this committee had in New York that the chairman quoted from one of the witnesses, and the letter from ITU in London regarding the response of companies, and we will get to some of those questions, I suppose, when the industry panel appears, but Commissioner Powell, I do not know if you are aware or not, but the Federal Reserve Board Governor Edward Kelly testified in April to the Senate Commerce Committee here regarding the telecommunications industry.

He said in that hearing, and I am quoting him here, "We are particularly sensitive to telecommunications, an essential infrastructure element, and our ability to maintain a satisfactorily high level of financial and business services. We have been working with our financial institutions and our telecommunications servicers to find ways to facilitate preparations that will ensure Y2K readiness. Nonetheless"—this is the important part of this—"nonetheless, this is an area that many financial institutions regard as needing attention."

Now, I do not know how many of you are aware of Fedspeak, but let me translate that last sentence in Fedspeak. "Houston, we have got a problem," is sort of how I would translate that line, and that is just adding an element to this here. When the Federal Reserve Board begins to raise concerns and questions—now, this was April, late April. I wonder if you maybe could just pick up even further on the comments of the chairman about this as to sort of where are we in all of this. That is April 28.

Mr. POWELL. The first thing I would say is, particularly with respect to Senator Bennett's suggestion that our comments are rosy, let me assure you, I do not think it is rosy at all. What I am confident about is that we have a system and a process to work. I do not express any rosiness about whether they will get there, only that I think I have some confidence that we have the instruments, and some indications of the level of effort that give one reason to have some confidence that we may, with the little remaining time, be able to successfully navigate these waters.

It is not surprising for me to hear the concerns from the outside community seeming to be at odds with our own. I hear it, as well. I meet with these groups quite frequently. I have met often with the banking community, and, indeed, a few weeks ago spent 3 or

4 hours at the Federal Reserve briefing people by video on the efforts of the telecommunications industry.

I would offer this, which I think helps understand this. There are sort of in my mind three levels of concern. The first kind of concern is concern about telecommunications because you ought to be. It is a critical infrastructure and that is a kind of concern that we should have all the way through the date and long after, because we understand that while the probabilities may be low, consequences are dramatic and no one can rest with respect to that concern. I would say that energy and other critical infrastructures have the same kind of component.

The second kind of concern is concern because you do not know. Now, what I have tended to find is that what we are finding with a lot of critical users, like the Federal Reserve and others, is that the anxiety is not that they see things that suggest failure, but they are not getting information that gives them confidence, either. This is the barrier to information problem.

When I took over these responsibilities in May—that is not an attempt to hide from what was going on in April—we made it a critical component of what we thought we could do, is to help facilitate and improve that level of anxiety, and I can say a little bit more about that in a minute.

The third level, I think, is that you see and you do not like what you see. That is, you are beginning to get information and the information is disturbing.

I think part of the disconnect is that the three of us, at least, have had a lot more opportunity to see, and what I am happy to say is that the more I did, while I do find new things to be concerned, my confidence improves rather than falls. The key is to make sure that we proselytize that, make sure that the Fed and other people are getting what they need to have their own confidence or make their own decisions about what contingencies. That is a cornerstone of our efforts to try to fix that problem. We are doing it both through the surveys and figuring out how to cull information and then disseminate it to key users.

Our forums have been particularly helpful. When I hold a forum with the wireline carriers, I have the carriers at the table, I have the equipment manufacturers at the table, I have the industry groups that represent them at the table, and I have major end user groups. I have the Fed. I have had Sears. I have had UPS. I have had any number of people who can speak to the problems. And when they are talking right in front of us, we try to serve as sort of a tough referee to pry out the problems, and I think legal concerns have been a big part of why companies have not told their story more fully, and so we are just trying to work through that.

Vice Chairman DODD. I think that is a very good analysis of the three areas of concern. I was pleased to hear you announce that the chairman of AT&T will be the chairperson of this NRIC group, but speaking to the very set of issues you just raised and identified in the three categories: First, because you ought to; second, because of what you do not know; and third, because of what you do know, we have 17 months left, about 520 days. This is not a question where we get it done this month, next month, there is some give. In Washington, typically, things can be delayed. We are on a real

clock here, and, obviously, things have to happen before January 1, 2000.

Chairman Kennard promised back in April that there would be the NRIC organization up and moving. It is 3 months, and I am pleased to hear the announcement today. I do not want to sound like I am being a nit-picker here, but every day that goes by gets really problematic. When it takes 3 months to get something up and going and announce a chairman, it is disconcerting and maybe fall under that second category or third category here for me.

I would hope we might get some sense of what the timeframe is now for NRIC to respond to these and give us some sense of where this is going and a broader sense of the problem that we have. Do you have any idea of that at all? Is there a time table? Have you insisted, or has the Commissioner insisted on the chairman getting back in a very time certain period with information?

Mr. POWELL. First of all, to clarify some misunderstanding about that, I am disappointed, too. I have the same sense, that every day is a day lost and we were probably slower than we should have to get that operating. But I will say, it was in operation. The key is that it did not have a chairman, which is normally a CEO, because the previous chairman had elapsed, but the NRIC operation has been in effect all of that time and what we have been doing is making sure that the vast majority of its mission, which is not exclusively Y2K, it is network reliability in general, that the vast majority of its mission was redirected to be exclusively about Y2K.

The other thing that has really been difficult, which has been part of my challenge, is sometimes there are too many cooks in the kitchen. NRIC will be important, but it is one of many, many organizations worrying about telecom. I mean, three of them are right here and that does not even hardly scratch the surface. So I would say that there have been a number of people trying to do monitoring and assessment of the telecommunication industry from different venues.

To me, when you have an urgent situation in terms of time, efficiency becomes really important, and what really becomes important is getting an effort that is relatively coordinated so people do not ask Bell Atlantic ten times the same question, that we have some way to bring some efficiency into that response.

The key to the NRIC effort is not that I am going to turn the job over to them, and so, in a sense, there is not this, they will get back to me on this date sort of thing. They are part of my process which I personally intend to try to drive. That is, they sit at the table of the Telecommunications Sector Group. They report back to us. We talk to them almost daily with respect to the kinds of things that we would hope that we do. We have already had one significant opening meeting with their presence this month, earlier this month, and I intend to put that on an almost monthly update basis in that we will develop in that group specific taskings with specific times for responses to them.

But what we do not want to do is drive in and try to quash really good efforts underway. It would be, in my opinion, not a good use of NRIC to tell them to buffalo into the Telco Year 2000 Forum and start changing the great efforts that they have undertaken with respect to testing.

So I hope that is a satisfactory answer to the question, but I assure you, we are taking that urgency seriously.

Vice Chairman DODD. At some point, we would like to know who the lead chef is.

If the chairman would yield for just one question, because this ties in with this.

Chairman BENNETT. Surely.

Vice Chairman DODD. First of all, I am very heartened by the good response you have had from a number of companies, and I had earlier sort of prepared a question to ask you about the 911 issue. In fact, I used the 911 analogy and talked about what can happen here. For a lot of folks out there, this is a very personally critically issue. The other stuff we talk about, financial services will impact them, maybe directly, maybe indirectly, more likely indirectly. But the 911 issue is one that has a very direct impact.

You mentioned only about 1 out of 55 wireless companies that are heavily involved now in this area have responded to inquiries. I would——

Mr. POWELL. Public safety. If I could correct, the public safety community.

Vice Chairman DODD. The public safety community. I think it might be helpful if you could provide this committee with a list of those companies and we will add that to our group of companies that we would make in a very public setting here today, saying you have got a couple of weeks. We are going to be calling Commissioner Powell back and asking him whether or not you have responded to these letters, and if you have not, I am going to add you to that public notice about companies that are not doing their job in responding to this problem.

So I will make a formal request of you that we have a list of those companies. We will keep it confidential, I hope, Mr. Chairman, in the committee——

Chairman BENNETT. Yes. Yes.

Vice Chairman DODD [continuing]. And we will call you back in a couple of weeks and find out whether or not they have been more responsive.

Mr. POWELL. Absolutely.

Vice Chairman DODD. And if they have not, I will let you know today, be prepared to read your names and hear about them in a very public setting.

I thank the chair.

Chairman BENNETT. Thank you. Senator Smith?

Senator SMITH. Thank you, Mr. Chairman. I apologize for being late. I was in the Judiciary Committee giving testimony on the issue of assisted suicide, which affects my State a great deal. On the way over here, I was wondering if we are not in a different context talking about assisted suicide on Y2K.

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

Senator SMITH. I apologize if I am plowing old ground, but with Senator Dodd, I serve on the Foreign Relations Committee and I am very interested in how well prepared the rest of the world is. That clearly may affect some political stability around the world and certainly has an impact on our country. I wonder, is there an

international organization that is helping on this issue? Are we doing anything to provide that leadership internationally? Any of you can speak to that.

Mr. POWELL. Senator, I can offer a little bit on that. There are any number of people trying to work on the issue on the international front, but let me point out what I think are some of the critical forums.

First of all, there are regional organizations. The European Union has its own Y2K operation. There are other regional operations. But the one to my mind that is probably playing the most critical role and the most umbrella role is the International Telecommunication Union, which meets frequently and is part of—it historically is part of an effort that coordinates international telecommunications generally. You know, we share spectrum around the world. People have to figure out how to do that, and so they are a very fundamental player in that.

That is chaired by an individual named Ron Ball, who is from Britain, who is an extremely gifted individual and I am personally very heartened that he is chairing that effort over others.

They have been engaged in an effort to do monitoring and assessment much like we do domestically and have sent out a significant number of surveys around the world to try to get detailed responses and it is pretty dismal. Senator Bennett was right in his assessment of how that has gone, and the United States is a little vulnerable on this, as well, and we are doing stuff to make sure that gets fixed. So that is part of their effort.

They have deputized what they call ''Y2K Ambassadors.'' That is, they are individuals or institutions that are responsible for particular parts of the world, sort of in an effort to delegate some responsibilities across the board.

The State Department has been engaged in an effort through state-to-state contacts to raise the profile of the issue through its ambassadors. I know it has dispatched communications to the field in that regard.

Indeed, the President raised this as part of the G–8 summit, again, another interaction that was not heartening. We sat—not me, personally, but the United States sat at that table with an extensive amount of materials, I think, prepared to begin working on that issue in a much more serious way. The vast majority of people had nothing to hand out and barely want to talk about the problem. There are others. I mean, there are other forums being put together and being worked on.

One of the things I do is lean heavily on American companies who I think have the contacts that matter. State-to-state contact is useful, but the truth to it is, you have got to talk to Deutsche Telecom. You have got to talk to the companies. You have got to talk to KDD and NTT and Singapore Telecommunications. The AT&Ts of the world do that frequently, and if they are taking the problem seriously, everyone they interact with should be taking the problem seriously.

As I understand it, for example, a company like British Telecom begins to now have important contract provisions and an insistence that we are going to look for new relationships if you cannot give me some assurances you are working on the problem.

So that is some of the effort that is underway, but you point out rightfully what concerns me. Thankfully, in the United States, for the most part, there are not a ton of things competing for national attention with regard to this issue. But when I talked, for example, to the president of Deutsche Telecom, I said, what about the Year 2000 problem? He said, "I have two of them, the euro and this." There are an extraordinary amount of world events that are competing for attention. One gets concerned about how those priorities are assessed.

Japan has a "right now" problem, and the notion that they, sort of as a national priority, have this at the top of this, it worries me that they do not.

Indonesia, significant parts of the world who are critical to the international payment system, very critical to other things that we rely on, are sort of in woeful straits in that regard.

So the bottom line, to tie your comment together with Senator Dodd's, is that there cannot be an interaction in which this issue is not raised. I think if any government official or any private sector individual who has an interaction with a foreign carrier, foreign government, does not raise Y2K every time they run into someone, they have made a substantial error.

Senator SMITH. Is the United Nations doing anything on this?

Mr. POWELL. I am not personally aware of the extent of the United Nations' involvement. I thought that I understood, and I would have to verify that there were some resolutions that either were passed or were pending, but I am not specifically aware of it. I do not think the ITU is an element of the United Nations, or has a component of the United Nations, but I stand to be corrected on that.

Senator SMITH. Does this have any implications for—it seems apparent to me that it does—for the Aura, that transition? This is occurring simultaneously with it. I would think that would greatly complicate their financial system.

Mr. POWELL. It is huge. Put simply, it is huge. Next to Y2K remediation, I cannot imagine a more complex transition than changing your currency. I have had some discussions with presidents of foreign carriers and the kinds of things they have to work through are astonishing, where the commas go in terms of the bills, what systems have to be reprogrammed, the training of employees.

I am not one to tell Europe what to do, and in a sense in this regard, they are way too far down the road, but I think what everyone needs to do throughout the world is understand what things are not essential to happen now. This one has to happen now. You do not have a choice. Other things do not. I think nations, including this one, need to make some national priorities about what things can be put on the back burner as we hit the red zone to make sure that we do not blow this deadline.

Senator SMITH. Thank you, Mr. Chairman.

Chairman BENNETT. Thank you, Senator.

I would point out, I have met with Ambassador Kamal, who is head of the Informatics Committee at the United Nations. He and I have appeared on common speakers' platforms and we are in touch with this committee. He has described his relationship to the United Nations as much the same as my relationship to the Con-

gress, somebody who is trying to get everybody interested when they have other things on their minds.

Thank you all. One last comment, Commissioner Powell. With respect to the announcement you made today of the appointment of a chairman of this group, I would hope that the group would formalize some kind of link to the staff of this committee so that there could be an exchange of information.

This committee is performing, I think, a serious function in that we are becoming the repository of information. There does not seem to be any other place where information on Y2K across the spectrum of industries, States, government agencies, and so on is accumulating other than this committee, and I think your group would benefit from that context, and, frankly, so would we if, in performing this role as the repository of that information, we had a conduit of connection. So I would appreciate if it you would take the charge to see to it that that conduit is created and the opening is made.

Mr. POWELL. Senator, I will, and I would also issue a standing invitation to anyone on the Hill, your staff, in particular, to ever attend any of these telecommunications working groups. I would be more than happy to have them there. We will make sure that they know about them, when they are occurring.

Chairman BENNETT. Thank you. That is very much appreciated and I am sure someone will attend.

Thank you all. We appreciate your being here.

Chairman BENNETT. We will move now to the final panel. We appreciate this final panel. I have to make an editorial comment. Those that are worried about the lateness of the hour, it is unusual on a Friday morning after a recess has started with no votes on the Senate floor for as many Senators to attend a committee meeting as have come to this one and as have stayed. Senator Stevens has told me he is still coming. He has a number of other pressures on him as chairman of the Appropriations Committee.

So it is a testimony to the importance of the issue that we are going as late as we are and that you do not usually get left solely to the tender mercies of the chairman, that other members of the committee have shown up and demonstrated an interest and continued to question. That is why we have gone on as long as we have.

Our first witness will be Joseph Castellano, president of Network and Corporate Systems at Bell Atlantic. He is representing the efforts underway and difficulties facing the local and long distance common carriers.

He will be followed by Gerry Roth, vice president for Technology and Systems at GTE, who is representing the TELCO 2000 Forum, an organization of telecommunications companies established explicitly to focus on testing common carrier interoperability.

He will be followed by Ramu Potarazu, vice president and chief information officer of INTELSAT, a leading provider of commercial communications satellite services.

Our final speaker will be Gary Beach, publisher of CIO Magazine, a bimonthly publication reaching over 125,000 IT and business executives.

We will have other telecommunications experts who are providing statements for the record.

[The prepared statements can be found in the appendix.]

Chairman BENNETT. Gentlemen, we appreciate your being here. I make one comment, highlighting what Commissioner Powell said. If we are going to get the international problem under some degree of control, it is going to be more company-to-company conversations than it is government-to-government conversations. We are sorry to have to put that big a burden on you, but the nature of this particular problem simply requires it. So that is why we are delighted to have you here and delighted to have the level of interest that your presence here represents.

Vice Chairman DODD. Mr. Chairman, just before they start, I want to thank all of them, as well. I have a flight problem that is going to cause me to leave, but I wanted to apologize in advance to the witnesses. It is my fault. We went on with some of these other panelists a little longer than the chairman probably anticipated. But I appreciate immensely your presence here today.

I just would like to pick up on the comment we made earlier, and this is a group that can really be of help to us and I suspect, based on Commissioner Powell's response, that we are not talking about anyone here at this table, in terms of just keeping communication lines and responding to these inquiries that come from the FCC.

But if you would use your good offices, particularly you, Mr. Beach, in having the advantage of reaching a lot of people out here. how important it is that that information that is being requested be provided. I have no desire to get into the business of releasing the lists of companies who are not responding, but I do not know of any way to get attention. What I try to do is announce that we are going to do it, give plenty of time for people to know that I am not doing it today or tomorrow or next week, but at some point, you are going to provoke me into saying, look, I will use the bully pulpit of the U.S. Senate to do so. So I would hope that we might get that message out to people. It is in their interest. It is in all of our interest that they respond.

I apologize, Mr. Chairman, but I may not have a chance to raise that with you by the time you complete your testimony, so I just wanted to raise it here before we started.

Chairman BENNETT. Thank you. We all understand about airplane problems.

Mr. Castellano.

STATEMENT OF JOSEPH CASTELLANO, PRESIDENT, NETWORK AND CORPORATE SYSTEMS, BELL ATLANTIC

Mr. CASTELLANO. Good morning, Chairman Bennett and members of the committee. I appreciate being invited to address you on the Year 2000 issue. My name is Joseph Castellano and I am the president of Network and Corporate Systems for the Bell Atlantic Corp. I am also the officer responsible for leading the company's Year 2000 program. In that capacity, I chair Bell Atlantic's Year 2000 steering committee.

Bell Atlantic is a communications and information company with more than 41 million telephone access lines and 6.7 million wireless customers worldwide. I have been asked to offer testimony today about the Year 2000 vulnerabilities facing telecommunications carriers and the legal complexities of information sharing.

As you are aware, the Year 2000 challenge is to ensure that information technology accurately processes data into the Year 2000. For the telecommunications industry, this is a significant challenge and one we must meet in order for our communications networks and services to continue to perform as our customers expect. Communications networks are comprised of a number of computer-controlled network elements which operate together to allow voice and data to be transported and switched. Bringing all of these network elements into Year 2000 compliance is the goal of the telecommunications industry.

To understand the vulnerabilities facing our industry, it is helpful to consider the scope of the effort that is required in order to insure that carriers' communications networks are Year 2000-compliant.

In addition to the industry-wide activities discussed by others here today, each telecommunications carrier must undertake its own effort to identify Year 2000 concerns in its operations and to devise a plan to address each concern. The first step in this effort is to inventory all of the network elements, information systems, and computers that could possibly be affected by the century change.

To give the committee an idea of the size of this effort, Bell Atlantic's inventory includes the following: Over 350 types of network elements which Bell Atlantic has deployed tens of thousands of times in its network; more than 1,200 software applications with over 250 million lines of computer code, which support Bell Atlantic's business processes; approximately 88,000 personal computers, 800 mid-range computers, 40 mainframe computers, and hundreds of supporting software products; hundreds of unique security access, air conditioning, elevator control, and similar systems servicing thousands of buildings, garages, and other facilities.

Once inventoried, each type of network element and computer in each information system must be assessed to determine if it is Year 2000-compliant, and if not, when and how it would most likely fail. Knowing when a component may fail is important because this will influence the sequence and prioritization for correcting that component. Because telecommunications carriers purchase the vast majority of their network elements, information systems, and computers from others, an extensive program of equipment vendor communication at this stage and throughout the process is necessary. The carriers must know what steps an equipment vendor is taking to make its products Year 2000-compliant.

Detailed planning follows assessment. In this phase, plans are developed for the remediation or replacement of each type of network element and computer and for each information system. Even components found to be compliant during assessment will require testing or verification to validate manufacturer-provided information. For those components evaluated as non-compliant, we must determine if they should be fixed or replaced. Detailed plans must include all activities required to insure that the particular components within a carrier's network will operate correctly.

The next stage of a Year 2000 plan consists of testing compliant components, remediating and testing non-compliant components that will be retained, and replacing those components that will be

retired. This is the stage most carriers are at currently, and it is by far the most complex. During this phase, new and remediated network elements, computers, and information systems are comprehensively tested. Once network elements, computers, and information systems are fully tested, they can be deployed. Deployment for most companies has begun and will continue through early 1999, with some additional deployment occurring after that.

It is also important for carriers to develop comprehensive contingency plans. These plans should address actions required in the event that scheduled activities, such as the replacement of a particular software application, do not occur on time, as well as planning for possible failures. A contingency plan should also include the establishment of internal, industry, and customer command structures to effectively manage critical situations.

In general, the performance and integrity of the worldwide telecommunications network is primarily dependent upon three factors: First, the performance of the various network components and software manufactured by numerous equipment vendors; second, the integration of these network components by telecommunications carriers within their networks; and third, the interoperability of the separate networks owned and managed by numerous telecommunication carriers throughout the world and their customers.

If an equipment vendor is not able to provide functional Year 2000-compliant replacements or upgrades, that failure will likely have a material adverse impact on the carrier's Year 2000 efforts. Likewise, if the carrier fails to properly address its Year 2000 issues and a service disruption occurs, not only will that carrier's customers be affected, any interconnecting network operated by another carrier might also feel consequences.

Given this interdependency, it is critical that each equipment vendor and each carrier properly address its own Year 2000 issues and that equipment vendors and carriers work cooperatively to ensure a seamless, uninterrupted operation of the global network. Information sharing among carriers and between carriers and their equipment vendors is, therefore, essential in the successful implementation of any Year 2000 plan. Likewise, information sharing between carriers and their customers is equally critical to enable customers to understand and address their Year 2000 requirements.

This is an area in which government can help private industry. Our experience has been that liability concerns have had an adverse impact on the free exchanges of Year 2000-related information among businesses. These concerns affect not only the level or content of disclosure, but also the timing of the information exchange.

Given the compelling need to share Year 2000 information within the telecommunications industry, legislative action is needed to reduce liability concerns among companies. That is why we support legislation such as the proposed Year 2000 Information Disclosure Act to facilitate a more open and timely disclosure of Year 2000 information, and we urge the members of this committee to support its passage, as well.

In addition, Federal and State regulatory agencies are in the process of gathering as much information as possible from the entities within their jurisdiction in an effort to understand the issues, problems, and progress on Year 2000 matters. While we applaud and encourage these efforts, we believe that consideration should be given to the development of a more uniform approach to information gathering from the telecommunications industry. Such a uniform approach to information gathering would improve the usefulness of the information provided and minimize the impact of these requests on personnel working to address the Year 2000 problem.

I thank the committee for allowing me to address the Year 2000 issues facing the telecommunications industry and I stand prepared to answer any questions the members of the committee may have.

Chairman BENNETT. Thank you very much.

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

Chairman BENNETT. Mr. Roth, we thank you and appreciate your being here.

STATEMENT OF A. GERARD ROTH, VICE PRESIDENT, TECHNOLOGY AND SYSTEMS, GTE, ON BEHALF OF THE TELCO YEAR 2000 FORUM

Mr. ROTH. Thank you, Senator. Chairman Bennett, members of the committee, my name is Gerry Roth. I am responsible for GTE's Year 2000 program, but today, I am here to represent the Year 2000 TELCO Forum. We have submitted a written testimony, but with your permission and in the interest of time, I would like to summarize those remarks, sir.

Chairman BENNETT. By all means.

Mr. ROTH. The TELCO Forum is a voluntary, self-funded group formally established in 1997 to address Year 2000 issues potentially impacting the telephone industry. Its membership consists of Ameritech, Bell Atlantic, Bell South, Cincinnati Bell, GTE, SBC, Southern New England Telephone, and U.S. West. Additionally, AT&T, Worldcom/MCI, Sprint, and USTA have been invited to participate as full or supporting members.

The Year 2000 Forum is chartered by the Council of Telephone Company CIO's to address the potential impact of the Year 2000 on the telecommunications industry. Major priorities for 1998 and 1999 include information and best practices sharing in all areas of Y2K, network interoperability testing for Y2K compliance, and contingency planning, to include command structure planning for network coordination efforts across our industry.

The TELCO Year 2000 Forum initiated a concept for interoperability testing with three important goals: First, to minimize the risk of network failures; second, to minimize the risk of service failures; and third, to ensure functionality of date-and time-sensitive operations is not adversely affected by Year 2000. This intranetwork interoperability component testing includes tests of robust interactions between network elements, data transport systems, operational support systems, and the network elements that they support.

Our service cluster approach includes testing essential features of the public switch network, such as the public safety and emergency services systems, such as E–911, basic enhanced and intelligent network services, network management systems, and data network services.

Some of the characteristics of our testing include 16 separate configurations for network element and data testing and 40 separate network management configurations which span all service clusters. Testing is being conducted in five separate laboratories established across the United States in members' facilities, using 82 common communications products from 21 suppliers. This equipment comprises the major components of the standard North American suite of equipment and systems in use in the public switch network. In addition, four members have compiled and assessed product information on 93 other vendors with 470 separate products.

Information sharing is certainly an extremely important issue for the Forum and for the public, as we have heard here today. It has always been the intention of the TELCO Forum to make available the scope, the plans, and the outcome of our Year 2000 testing. As the committee is aware, several issues remain unanswered about either the advisability or the appropriateness of some aspects of this general information sharing. Nevertheless the Forum will continue to make this information available to the maximum extent possible in light of those issues.

Our network interoperability testing began on July 6 with operational support systems and network element management testing. This was followed on July 13 with the start of testing for data transport systems. Network element testing is planned to begin the first week of August. All testing to date has been successfully executed and testing is proceeding according to schedule. Test completion is planned in December 1998, with a final report being submitted on the first week of January 1999.

In an affiliated activity, the Forum is actively working to establish a plan for interoperability testing with a similar Canadian Year 2000 Forum, and we have begun discussions with the ITU concerning international interoperability test support.

I would like to spend a minute to discuss the relationship of these network testing activities that you have heard about. In previous testimony, you heard discussions of at least two major related Y2K interoperability test activities, the TELCO Year 2000 Forum and the Alliance for Telecommunications Industry Solutions, or ATIS. Although these groups operate independently, all members of the TELCO Year 2000 Forum are members of ATIS. The co-chair of the ATIS network test committee is also in the Year 2000 Forum. And the Forum will be represented in the ATIS network test committee as a separate entity. Year 2000 test planning for both the TELCO Forum and ATIS are intentionally complimentary.

After each company and/or supplier has completed Year 2000 remediation and tested at that level, the next step is to test component interoperability between companies and products. The last leg of that testing, then, is network interoperability testing, which stresses network features and services in an operational test environment.

The TELCO Year 2000 Forum testing, the intranetwork testing, is being conducted in late 1998. This is the first leg of testing which assesses network component interoperability, basically answering the question, "Do the major network support and management elements continue to operate appropriately among and between carriers in a Year 2000 environment?" An example of this is the 800 number data base support services.

This is then followed by the ATIS testing, or the internetwork testing, in early 1999. Internetwork testing will assess network interoperability with respect to service and operations once component interoperability has been demonstrated. This testing deals with such issues as potential network congestion on December, 31 1999, or January 1, 2000, time zone transition issues, Year 2000 impacts on local number portability enhancements, voice and data transmission between local and interexchange carriers, and real-time network management and control.

We have often been asked about our concerns about interoperability, which is a expressed concern of this committee. We have every reason to believe that the U.S. public switch network will continue to operate with no major service disruptions due to the Year 2000. However, full international interoperability is of concern due to many late starts and the uncertain program status in many countries.

The Year 2000 brings a unique and unprecedented potential for network stresses for several reasons. The anticipated increases in call volume crossing multiple time zones, increased international telecommunications interactions to usher in the new millennium, and then, due to the high profile of the Year 2000 as both a technology challenge and a new millennium, network security concerns will also be at peak because everyone out there is not just "calling to say they love you."

Any Year 2000 glitch which may appear at this otherwise teeming confluence of unique events would certainly exacerbate any performance issues.

We have been asked by Congress and others, what could others do to help our efforts, and some suggestions would include support of good Samaritan legislation, such as the Year 2000 Information Disclosure Act; work to remove the specter of antitrust claims against companies which cooperate in good faith on Year 2000 remediation; continued awareness campaigns through hearings like this; work to support efforts to enhance international interoperability; and finally, work with other government agencies to consolidate queries and streamline information sharing to prevent unessential duplication of effort.

In conclusion, the members of the TELCO 2000 Forum believe that this cooperative, voluntary testing effort will go a long way toward removing public anxiety over the Year 2000 status of the public switch network in the United States. Despite the fact that the live network cannot be 100 percent tested in advance of the Year 2000, we believe our individual and collective actions in Year 2000 remediation and subsequent tests and validation provide a basis for sustaining public confidence that the telephone and data networks will continue to operate in the Year 2000 and will continue to provide the outstanding services we have come to expect.

Mr. Chairman, I thank you for this opportunity to testify on behalf of the Year 2000 Forum.

Chairman BENNETT. Thank you very much.

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

Chairman BENNETT. Mr. Potarazu.

STATEMENT OF RAMU POTARAZU, VICE PRESIDENT AND CHIEF INFORMATION OFFICER, INTELSAT

Mr. POTARAZU. Good morning, Mr. Chairman, members of the committee. My name is Ramu Potarazu. I am the Vice President and Chief Information Officer of INTELSAT, the international telecommunications satellite organization.

I appreciate the opportunity to testify before you today on the important issues raised by Year 2000. I also wish to thank Chairman Bennett and the committee for your leadership in addressing such a complex and global problem.

This morning, I will concentrate on what INTELSAT is doing to address the Year 2000 issues. In fact, we calculate that we have 370 business days left before the Year 2000 is upon us.

Let me begin with a brief history of INTELSAT. INTELSAT was established in 1964 as a global commercial cooperative on the initiative of the United States. INTELSAT's main mission is to provide the space segment for public satellite communications services throughout the world on a non-discriminatory basis. Today, INTELSAT has 143 member countries and connects virtually every country and territory in the world. INTELSAT provides international, domestic, and regional satellite communications, services such as telephone, television, Internet, and data.

INTELSAT began its official Year 2000 program several years ago to make sure that we are ready for this challenge. In preparation for today's hearing I was asked to address several specific questions. The first question asked was, how does the Year 2000 problem affect satellite communications? I would like to spend a few moments to explain the four basic elements of the INTELSAT global system.

The first part is the satellites. Behind Senator Bingaman is a picture of a satellite located 23,000 miles above the equator in geosynchronous orbit. INTELSAT maintains a fleet of satellites in geosynchronous orbit which together provide global coverage, meaning we reach every person in the world.

The second part is the INTELSAT control system which is pictured to the chairman's right. The satellite control facility allows us to control and monitor our satellites, parts of which are located throughout the world.

The third part is the customers' earth stations, consisting of satellite dishes and other equipment.

The fourth part is essentially our entire user community—the local phone companies, broadcasters, business networks, Internet service providers, and other end users.

I will first explain what INTELSAT is doing with the satellites. Our satellite manufacturers have advised us that there are no known Year 2000 problems on our satellites. typically, a communications satellite does not use a time and a date. It uses a satellite

reference, what we commonly refer to as satellite local time. This is a reference to the sun, and when there is a reference to the sun, there is usually no reference to a specific year.

INTELSAT's own analysis and testing will seek to confirm this information. At this time, however, we believe that our INTELSAT satellites have no Year 2000 issues, but satellites are only one piece of the INTELSAT system.

For the INTELSAT control system, which are the systems that allow us to control and monitor our satellites, we have adopted a five-step approach to resolving our Year 2000 issues.

The first step is the preliminary assessment phase, where inventory for software and hardware is done.

The second step is the analysis and plan phase where the inventory is analyzed and a remediation plan is established.

The third step is the remediation phase, where the actual hardware and software is fixed.

The fourth phase is the test phase. As stated earlier by Senator Dodd, this phase is the most difficult. At INTELSAT, we are not a 9-to-5 business. We are a global business that must serve the world 24 hours per day, 365 days per year. We simply cannot shut down our daily operations to test hardware and software. Therefore, new test facilities have to be set up in temporary locations. We are currently preparing to conduct such tests as soon as the software remediation is complete.

The fifth and final phase is the deployment phase, where systems are put into production and operation. INTELSAT's Year 2000 program has primarily focused on our ground systems that fly, command, control, and monitor our satellites.

Now let me turn to your next question. What are INTELSAT's concerns about international communications? This, quite frankly, is INTELSAT's biggest concern and is the one that is mostly out of our control. The customer satellite dishes and the local phone companies, broadcasters, business networks, and other end users are the biggest challenge in addressing the Year 2000 issue. Because these entities are out of our control, our emphasis has been on education. Many of the customer stations throughout the world have several hundred pieces of computer equipment from various manufacturers that control their ability to send and receive telecommunications information.

For example, if the antenna control unit fails at the customer location, this failure could cause complete loss of pointing to the INTELSAT satellites by the antenna, and no information could be sent or received, even though INTELSAT's portion of the communications link is compliant.

Perhaps I can use an illustration to demonstrate INTELSAT's concern and those raised earlier by the chairman about Year 2000 issues affecting international satellite communications. A significant percentage of INTELSAT's international traffic is two-way communication links that use an INTELSAT satellite between country A and country B. Suppose country A's ground network is Year 2000-compliant. INTELSAT, being the supply chain in the middle, is also compliant. And suppose further that country B's ground network is not Year 2000-compliant. The result is that you have a failure of the complete chain. This is why INTELSAT has

some concerns about the Year 2000 compliance of all international communications.

To this end, INTELSAT has been proactive in working with our customers and our owners and other international organizations to exchange and gather information relevant to Year 2000 issues. INTELSAT has also teamed up with the World Bank and the International Telecommunication Union on several initiatives to promote the awareness of the Year 2000 problem throughout the world via seminars and the use of INTELSAT capacity on a no-charge basis for promotion of the Year 2000 issues.

In closing, INTELSAT has a plan in place to address the INTELSAT satellites and the INTELSAT control systems. We are confident that we will be ready in the new millennium. Our main concern is with our customers' satellite dishes and all of the business entities at both ends of the supply chain. It is important that we all continue our education efforts in this area throughout the world.

We need the ability to share information relating to the Year 2000 issue. We urge the administration and Congress to work together to allow us to share information more freely so that the Year 2000 problem can be resolved in an expeditious manner. Thank you very much.

Chairman BENNETT. Thank you.

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

Chairman BENNETT. Mr. Beach, you get to be the clean-up hitter here.

Mr. BEACH. I hope I can hit a home run.

Chairman BENNETT. Please do.

Mr. BEACH. No pressure here. [Laughter.]

STATEMENT OF GARY BEACH, PUBLISHER, CIO MAGAZINE

Mr. BEACH. Mr. Chairman, Senator Bingaman, my name is Gary Beach. I am publisher of CIO magazine, a magazine written for chief information officers who are responsible for building the largest information technology infrastructures here in America. These are the people, Mr. Chairman, that you were mentioning who are responsible for the company-to-company communication that is going on.

I feel a special akin to the Year 2000 problem, having been publisher of Computer World in September 1993, when Peter Deyager wrote the famous article that brought this problem to many people's attention. While I was not as smart as Peter to become a consultant back at that time on Year 2000, my conversations with users and chief executive officers of several large telecommunications companies this spring led me on June 15 to the write the following in the pages of CIO.

"The Year 2000 safety net for the telecommunications industry, our nation's backbone for voice, data, and Internet transmission, is nonexistent, will never be built, and as such, presents the global economy with its most significant Year 2000 problem."

I would paraphrase Senator Dodd's comments of a moment ago, "Houston, no, you do not have a problem. Planet Earth, we have a problem."

Here is why I feel this way. It has been an incredible 3 years for users in large, medium, and small companies. At once, the most diligent of them have addressed the Year 2000 problem, but as we said earlier this morning, some of that testing will be done erroneously.

On top of that, an issue that we have not talked about today at all that is compounding not only the time problem is the labor problem. Here in America and around the world, we have a critical shortage of information technology workers, men and women who could address this issue.

At the same time in the last 3 years, another technology phenomena, the World Wide Web, has expanded the dependence of companies on telecommunications, linking customers, partners, and suppliers in global networks.

Mr. Chairman, have you ever played dominoes? No? Well, one of my favorite games of dominoes, not particularly the game but setting them all up and hitting that first domino and watching them all fall down, the single effect theory.

As you were mentioning aptly this morning, we live in a system of systems, an interdependent world, and we have seen examples of how a single event can impact us all. Just in the last year, the UPS strike crippled many in the industry. In the spring, the PanAm satellite interrupted pager transmission. And just this week, we saw the conclusion of the General Motors strike, in which a single event in Flint brought that company to its knees.

The major fear of CIO's is this. While they may be compliant with Year 2000, their partners, their suppliers, their customers, all linked in this food chain, may not be and their non-compliance could in that domino effect impact their company.

Some companies have extraordinarily large food chains. General Motors, the company I just mentioned, has 35,000 partners. Again, as Senator Dodd was talking about this morning with Judith List, it is my opinion some of those 35,000 partners will be Year 2000 functional, some will be Year 2000-compliant, and many will be Year 2000 dysfunctional.

As Commissioner Powell talked about in terms of the legality issues, this is an incredible challenge, preventing many companies from fully declaring their Year 2000 operability. As several members of this panel and before have aired, I strongly support the administration and the Congressional efforts to get the Year 2000 Information Disclosure Act passed and passed fast.

CIO's express a particular concern, and we have heard this morning Senator Collins and others, about small companies. There are 23 million small companies in America. Wells Fargo Bank just this week released a report where they interviewed 500 small companies, those who have 100 or fewer employees, and found 50 percent are planning to ignore the Year 2000 entirely.

We have talked about the global issues. The World Bank in March of 1998 released the results of a survey it did among 128 borrowing nations. Seventy-one percent did not even know what the Year 2000 problem was.

The telecommunications industry in America, while many are familiar with the names on this panel, is really made up of many, many small companies. The United States Telephone Association

has 1,100 members. There are 4,500 members, as you mentioned earlier, Mr. Chairman, who are Internet service providers. I am concerned about the readiness of this sector of the telecommunications industry.

While the United States Telephone Association does a fine job managing its members, last evening, I went on their website and I challenge anybody to go on that website and find right up front information about the Year 2000.

ISP's, Internet service providers, who is even monitoring them?

So, in essence, the telecommunications industry faces what I call a great paradox. If the system works as advertised, as we have heard here this morning, then the global infrastructure will act as a massive conduit, spreading Year 2000 problems, not theirs, but from partners and suppliers in their information food chains. If it does not work, we all know where that is going to lead.

I have several recommendations. First, I would encourage this committee to raise the awareness of the Year 2000 challenge with small independent telephone companies and small internet service providers while abating the potential for panic.

Second, I would encourage all sectors of the telecommunications industry to follow the example of the TELCO Year 2000 Forum and expand their efforts as they have in an invitation to long distance carriers, competitive LEC's, et cetera. This is critical.

Third, I would encourage Commissioner Powell and the FCC to put enforceable Year 2000 compliance policies in place immediately for all groups it monitors, plus hold the chief executive officers and board directors of those companies personally responsible for Year 2000 compliance statements they share and file with the FCC. We need an independent verification process.

Fourth, I would recommend that the FCC impose immediate moratorium on telecommunications mergers and acquisitions. Why? The FCC needs to focus its finite resources on issues of national, not corporate, interest.

Fifth, I would consider the formation of a Year 2000 information center across America to inform consumers not only of the likely impacts on communications but the services they will purchase from banks and utilities. CIO magazine surveyed in May 400 households. Four out of ten Americans are totally unaware of the Year 2000 problem.

Sixth, I would mobilize millions of Americans to join a grassroots volunteer effort to help solve the problem. That same survey found 45 percent of Americans willing to serve if asked. I applaud the President for his efforts on July 14 to encourage retired Federal workers to come back, but more could be done. Possibly, we could follow the example of President Roosevelt and create a digital Civilian Conservation Corps.

I would challenge the telecommunications industry to report back to this committee with in-depth contingency plans on what happens if the network goes down, particularly in rural parts of America.

I would encourage you, Mr. Chairman, to talk to Ambassador Kamal, who headed the Informatics Committee, and possibly have a summit at the United Nations this fall.

So my basic report is this. I am concerned. I am close to this issue. When someone asked me the other day, what am I going to

do with my money, I do not know, but we all have to work on this together. We should prepare for the worst, pray for the best, and hope between now and the Year 2000, everything we do can bolster those dominoes so when one of them falls, and one of them is going to fall, all the rest do not fall. Thank you.

Chairman BENNETT. Thank you very much.

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

Chairman BENNETT. I gather from your presentation, Mr. Beach, that you agree with my concern that things as presented earlier were a little too rosy. Is that an understatement of where you are?

Mr. BEACH. No, that is an affirmative.

Chairman BENNETT. Thank you. Given the hour, I have a whole series of things I want to get into, but let me focus on just a few.

You have all talked about the need for legislation. Senator Dodd and I have introduced by request the administration's bill as it was presented to us. For those of you who are not following the committee's activities, I will tell you that I have given the assignment to work on this legislation to Senator Kyl. Senator Kyl is chairman of the Subcommittee on Technology in the Judiciary Committee, so there is a nice fit here. Since this committee has no legislative authority, the committee with legislative jurisdiction probably would be the Judiciary Committee and Senator Kyl is going to work with his staff, the Judiciary Committee staff, and our committee staff through August to try to have something for us to consider in September.

I am convinced that it must be passed in this session of Congress, that we cannot wait until next Year on this one. We are trying to draft a careful bill. We will use the administration draft as a beginning point, but we have had a number of people say that the administration draft is inadequate in a variety of ways and we will do our best to try to see to it that it gets improved.

I would like you briefly to comment what you would see life like a Year from now, in, say, summer of the Year 1999, if this legislation is passed. What do you see the impact of this producing in the next 12 months? Mr. Beach?

Mr. BEACH. I would just like to comment that while I support the legislation and the goals of it, it can be difficult to have companies share best practices, particularly in a very competitive environment. So I would only caution. I applaud the goals and the spirit of the law. In reality, companies may not share as much as they should.

Chairman BENNETT. Does anyone else have a comment, specifically on the President's legislation, because you have not seen the draft that we will inevitably come up with?

Mr. CASTELLANO. Chairman Bennett, I think that as a result of the legislation, we will see a better flow of information between suppliers and customers at all levels. I think that is very important to address some of the comments that were made earlier about the concerns people have about not knowing what the status of things are and I think the legislation would improve that tremendously. Also in the working relationships between the various firms, it would facilitate coming to conclusions on how to fix the problem.

Chairman BENNETT. Senator Bingaman, you have a strong interest in this. We will go to you now and I will reserve the balance of my time.

Senator BINGAMAN. Thank you, Mr. Chairman. It seems to me we have got sort of two schools of thought presented today. Mr. Beach may represent one of those.

I noticed in the testimony that Ms. Fountaine gave us from the National Communications System, she says here, "In implementing special national security emergency preparedness capabilities in the public network, we chose the major interexchange service providers, as well as the primary local exchange companies." It says, "We believe, based on the information they gave us, we believe that there will be little or no interruption of service from these major service providers due to the Year 2000." I would be interested in Mr. Castellano's view as to whether he agrees with that.

Mr. CASTELLANO. I actually do, because we have been working very diligently, all of us, for several Years now and doing all of the steps that you need to do in order to be prepared, and I think we have reached the point where we are starting to feel confident that our own networks within individual companies will be ready and ready, willing, to begin the testing process between the networks to make sure they will be ready.

We feel for the most part that most of the problem will take place, if it takes place at all, towards the later half of next Year. We are aiming to be ready in the second quarter and we think we have some contingency time to do additional testing before the actual date. So I think our level of confidence with the major carriers is pretty high.

Senator BINGAMAN. Now, when you say the major carriers, one of the statistics we heard earlier was that 98 percent of the communication traffic is carried by the major carriers, something over 98 percent. Is that what you are talking about? You are saying that 98 percent of the communications traffic that we have, at least in this country, should not be interrupted, based on your assessment?

Mr. CASTELLANO. I think that is a pretty good assessment. It may be more than 98 percent, but I think there is less certainty about the rest at this point in time, based on the conversation we have had today.

Senator BINGAMAN. Does anybody on the panel want to dispute that?

Mr. BEACH. I will not dispute it, Senator, but I will comment that I support broad-based interoperability testing. I would only comment that the logistics of creating a broad-based test that replicate exactly what happened in our lives day in and day out in America is extraordinarily difficult, and just leave with the thought that we really have until this time next Year to control possible public panic about this issue. We asked those same people in the survey questions, and this time, in the summer of 1999, if it becomes apparent that this problem is not solved, there is a possibility for public concern, and "panic" is not too strong a word.

Senator BINGAMAN. Let me also just ask, Mr. Potarazu, your testimony says, "At this time, we do not believe that the INTELSAT satellites have any Year 2000 issues." So if we do not have any problem with the telecommunications infrastructure, at least 98

percent of it, and we do not have any problem with INTELSAT satellites, are there communication satellites that are not INTELSAT satellites that you believe will be affected by this, or are you speaking generally of communications-related satellites?

Mr. POTARAZU. My comments specifically addressed INTELSAT satellites. We have three manufacturers that build our satellites, Hughes Space and Communications Co., Space Systems/Loral, and Lockheed Martin. Other international satellite companies may have different vendors, but with the three vendors which manufacture INTELSAT's satellites, we have assurances that our satellites are compliant.

Senator BINGAMAN. But there is no reason to believe that they would be making Y2K-compliant satellites or satellites that are not affected by this problem for you and making satellites that are effective on this problem for others, is there? Just those three?

Mr. POTARAZU. With those three, that is correct. We do not believe so. The satellite manufacturer's have advised INTELSAT that they know of no Year 2000 problems with our satellites.

Senator BINGAMAN. And those are the three major U.S. manufacturers?

Mr. POTARAZU. In the United States, correct.

Senator BINGAMAN. Are we down to trying to figure out the extent to which the small telecos are going to create a problem for the rest of the system here, the less than 2 percent of traffic that goes over these 1,200 or so small companies? Is that where the effort ought to be concentrated, Mr. Castellano, and if so, what is being done to bring them up to speed?

Mr. CASTELLANO. At the present time, I agree with that, and I also think the international carriers should also be included in that statement. I think the next step is for those of us who have been in ATIS or part of the TELCO Forum. We are going to try to reach out to those companies and have them be involved in our activities. I think that would be the next step.

Frankly, we have not paid them a great deal of attention. We have been very involved with our own issues, trying to get to the point where we can say, yes, you were competent about our own efforts, but I think it is now time for us to try to help the others to get ready, as well.

Senator BINGAMAN. Is there a plan to do that in place? I mean, as you move into the fall and the rest of this summer, is there a plan to get information out to these folks and bring them in and share what you have learned with them?

Mr. CASTELLANO. Well, we are at the beginning of that. Last week, we had a meeting and we discussed the possibility of describing how we would work with others and writing a white paper on that issue as part of the next step in our activities, at the TELCO Forum meeting.

Senator BINGAMAN. That is very useful. Thank you very much, Mr. Chairman. I appreciate it.

Chairman BENNETT. Thank you.

Mr. Beach, you have raised an interesting question that, frankly, had not occurred to me before, but it is obvious once it is laid out. You call it the great paradox in your prepared statement. You say, let us say the telecom industry's Y2K remedial efforts are 100 per-

cent compliant, not a likely outcome, and the system works as advertised. The telecommunications infrastructure then becomes a powerful conduit for spreading Y2K problems.

Mr. BEACH. Yes.

Chairman BENNETT. That is an interesting paradox.

Let me go back to the statistic we had at the beginning of the hearing, which says, statistically, every time you fix 4.5 lines of code, you introduce an error into the system. Mr. Beach, as you look at that, do you have any sense of how big a problem that is going to be, to find those errors, or in the spirit of what you said here, a powerful conduit for spreading problems. Are those part of the errors that will be spread?

Mr. BEACH. Yes and yes. I mean, one of the problems, Mr. Chairman, is that information technology workers, once they have felt they have scrubbed a line of code, there is a perception that that has been done correctly and they have moved on to others. Some companies have 800 million lines of code to create.

What I would also like to comment on is I believe Judith List talked about this morning rather well, and it is the latency factor of the ability of a telecommunications network to spread these problems, whether they are billing problems or what have you. We are all preparing for January 1, 2000, which might even be before that, but there is a possibility that latent Year 2000 problems could be much like digital microbes that are invisible.

Deputy Secretary Hamre from the Department of Defense recently said, on the Year 2000, if the computers go down, it is not fine, but at least he knows where the problem is. A bigger problem for him, and, I argue, a bigger problem for users is if the system continues to work. I mean, if Ramu sends a satellite off and it is only one degree off, over time, that one degree becomes a huge gap.

Chairman BENNETT. You are going in the direction that I was going. I am beginning to realize that the life of this committee may extend far beyond January of 2000, not because I want to empire-build but because the problems are going to be there. We have seen that in testing, and I am going to end the hearing with this comment about testing and our experience and what we have seen in the committee and, hopefully, through this group, send a message to the telecommunications industry.

The military has done some testing. They found several things. The most disquieting one is that a majority of things that have been certified as Y2K-compliant on subsequent testing have been found not to be, and they have had to go back again.

The second is that the problems, as indicated in this last exchange, are cumulative. Something is compliant on January 1. It is functional on January 2. The degradation in its function begins to accumulate and it fails in February or March, and you find in the meantime that it may very well have been putting bad data into the database during the time it appeared to be functional.

We are not going to really know whether the telecommunications system has gotten by the millennium bug if all the phones have dial tones and everything is going through on the second of January. We may very well have problems that come along and bite us and bite us badly in the middle of January or February or later on, and finding the source of those is going to be much more difficult

than finding the original problems when you do the first remediation.

I am seeing some nods. Is that a fair characterization of the problem that we have?

Mr. ROTH. Absolutely.

Chairman BENNETT. Finally, we have the experience of last week's hearing. Last week, I had to do what Senator Dodd has had to do. I had to leave. I left him the gavel. At the end of the hearing, someone was called out of the audience who was not scheduled to be one of the witnesses but was connected with one of the witnesses who described the experience of standing there in a hospital holding in his hand the letter of certification from a manufacturer that a piece of equipment was Y2K-functional and watching it fail as the clock was set ahead to the Year 2000. If the hospital had depended upon the manufacturer's certification that everything was fine, someone would have died.

The witness, as I understand it, described several such circumstances, and one of the most frustrating ones, a piece of equipment where, when the clock was turned forward to the Year 2000, failed, would not recover when the clock was back off. By merely testing the piece of equipment, they ruined it, which raises another specter that I have heard about and we will hear about in subsequent hearings of the company that tried to set its clock forward to test and discovered that the failure that occurred in that instance was wiping out all the passwords. As a consequence, their database was rendered inoperable by virtue of the test because they could not get in it, and the passwords had all been deleted by the Year 2000 problem.

So my conclusion here, which I am leaving everyone who may be watching, either in the overflow room or on television or the journalists taking things down or those of you representing various industries, we cannot depend on the first test or the first certification or the first comfort letter that we get from a manufacturer or somebody looking at this. The testing has got to be extensive, it has got to be continuous, and it has got to extend beyond the Year 2000 because we absolutely cannot allow the telecommunications systems to fail, or everything else goes under.

I appreciate the reassurances that we have gotten, but I also appreciate the warnings that we have had that those reassurances need to be checked and rechecked and then checked again before we can take them at face value.

My thanks to all of the members of the committee. To all of the witnesses, thank you for your patience. The hearing is adjourned.

[Whereupon, at 12:30 p.m., the committee was adjourned.]

APPENDIX

ALPHABETICAL LISTING AND MATERIAL SUBMITTED

PREPARED STATEMENT OF GARY BEACH

My name is Gary Beach. I am publisher of CIO, a magazine written for chief information of officers—men and women who build and manage our nation's information technology infrastructure. These executives work in major corporations and in many government agencies nationwide. The subject of my testimony is "Industry Concerns about the Preparedness of the Telecommunications Industry As It Faces the Year 2000 Challenge." My perspective comes from 17 years in the information technology publishing business and from private discussions about the Year 2000 with CIO's and other technology and business executives.

No one today can dispute that we live in a globally interconnected, interdependent information society—an information society increasingly built on fragile supply chains. To give you a sense of the intricacy of this interconnectedness, consider these examples. Last year the United Parcel Service strike crippled many segments of the U.S. economy. This spring a single satellite malfunction caused millions of pagers to go down. A strike at a plant in Michigan disrupted the entire North American operations of General Motors.

Despite the calamity described in the above examples, our societal web of supply chains has shown the ability to take a hit in one place and maneuver resources from another locale to recover. But never has society in general or the telecommunications industry specifically faced the daunting, hard-stop challenge posed by the Year 2000 problem. In the past two months many witnesses have come before this committee professing their industry or their company will be Year 2000 compliant. My conversations with chief information officers and key executives of long distance and regional telephone companies have convinced me those claims of compliance may be based more on hope than on actual fact. This should not come as a surprise as we've never faced such a daunting challenge. True, the telecommunications industry has been working on Y2K compliance. Many have devoted efforts to the problem since the mid-1990's. At the same time, however, use of another technology, the World Wide Web, skyrocketed and millions of corporations have extended their internal information technology networks to external partners, suppliers, customers, yes, even competitors. Sears, for example, has 5,000 suppliers linked to its information infrastructure. Chief information officers are concerned that regardless of what they've done to make their own systems compliant, they may still fall victim to their connected partners' problems. And partner failures could have devastating economic results for a company no matter what it has done to become Y2K compliant.

This scenario presents the telecommunications industry with what I call the "The Great Paradox." Let's say the telecom industry's Y2K remedial efforts are 100 percent compliant—not a likely outcome—and the system works as advertised. The telecommunications infrastructure then becomes a powerful conduit for spreading Y2K problems. Technical problems will be passed down the information technology (IT) food chain as quickly as telephone connections occur. On the other hand, if the telecommunications system experiences significant Y2K problems, not only businesses but lives could be lost. Think about how much we depend on 9–1–1 for example. What if it doesn't work when we punch in those numbers?

Of particular concern is the Y2K readiness of the 23 million small businesses in America. And why should we all care? Because small businesses may not have the fiscal or human resources or the know-how to address Y2K. In a survey of 500 American businesses that employ 100 or fewer people, Wells Fargo Bank reported earlier this month that an incredible 50 percent of respondents plan to ignore Y2K issues entirely. The 23 million small businesses in America employ more Americans

than any other sector by far. If the Wells Fargo Bank survey is accurate, many of America's small businesses will not be Y2K compliant, many will suffer Y2K disruptions, and some may go out of business causing our nation's unemployment rate to rise.

Why my concern about small businesses and the food chain analogy? Because the United States telecommunications industry reflects in many ways the percentage composition of the general American economy. While most Americans are aware of names like AT&T, Bell Atlantic and GTE, the United States telecommunications industry is in reality an intricate web of over 1,100 small independent telephone companies and approximately 4,000 small Internet service providers. Day in and day out these companies rely on each other to complete the voice and data calls that make up the fabric of life in America today. What are those small telephone and Internet service providers doing to become Y2K compliant? Are they following the example of small businesses sampled in the Wells Fargo survey? And our concern should cover not only small businesses but also our global business partners. Many multinational corporations do business with countries around the world. In March 1998, the World Bank reported that of the 128 borrowing countries it monitors, only 37 even knew what the year 2000 problem was.

Earlier this week I visited the Web site for the United States Telephone Association, the group that represents these 1,100 independent telephone companies. I am disappointed to say that if what I found represents the USTA's interest in the Y2K issue for its members, many of those small telephone companies will not be Y2K compliant by the end of next year. I started my testimony talking about the intricate information chains that bind our society and economy. In Boston when I call the West Coast, my call has to proceed from a Bell Atlantic switch to the long distance carrier of my choice to the local telephone company servicing my end destination on the West Coast. The players large and small in the extremely competitive telecommunications industry need each other to complete those voice and data calls. What are they doing to join arms and fight the Y2K battle? While I applaud the efforts of the Telco Year 2000 Forum, it is largely an effort of the major local exchange carriers. I urge AT&T, MCI, and others to accept Telco Year 2000 Forum's invitation to join. As the days to 1/1/00 dwindle, the telecommunications industry must put aside its partisan nature for an all-hands-on-deck run at this problem. When American citizens are unable to make phone calls on January 1, 2000, they will not have the patience for finger pointing that may ensue among local, long distance and Internet services. The telecommunications industry is increasingly a global business as seen by this week's announcement of the AT&T/British Telecom joint venture. Chief information officers are increasingly concerned about data such as earlier reported from the World Bank: What kind of impact could a Y2K failure in a foreign PTT (Post, Telegraph, Telephone) have on their global information technology infrastructure. Alan Greenspan recently testified before the Senate Banking Committee that a small problem beginning somewhere in the international banking community could snowball into a Gargantuan problem. Could his point of view be transferred to our nation's telecommunications industry as it prepares for the Year 2000? Could a small Y2K problem beginning in some small European, Pacific Rim or Latin American country snowball into a large Y2K problem here in America? As the International Telecommunications Union recently reported, could Y2K unpreparedness cut off the developed countries that have worked on the Y2K problem from the developing countries, creating in essence a digitally disconnected Fourth World of nations? On July 23 Senator Dodd said in these hearings, "We are no longer talking about whether there will be any Y2K disruptions—only how serious those disruptions will be." On June 4 in Omaha, Nebraska, CIO magazine and the International Data Corporation released the industry's first predictive tool that helps companies gauge their Y2K vulnerability. We call it the Beach/Oleson Pain Index and it can be found at www.cio.com/y2k.html The index is based on the interconnectedness of corporations sharing applications with external partners. We quantify the problem into four states: catastrophic, meaning the problem experienced could cause socioeconomic harm; business critical, which refers to a Y2K problem that brings down an entire business for more than 24 hours; disruptive, including problems causing outages that are fixed within 24 hours; and annoyances, nonessential Y2K problems such as your e-mail password claiming it has expired. For example, a corporation or telecommunications company sharing 55 applications with external partners has a 57 percent probability that its Y2K problem will be an annoyance, a 34 percent probability the problem will be disruptive, a 11 percent probability the problem will be business critical and a 0.6 percent probability the problem will be catastrophic. While most companies will not experience catastrophic problems, the telecommunications industry certainly falls within the group that will

suffer deeply if partners' appropriate preparedness action steps are not taken. These are our recommendations to this committee moving forward:

1. Raise awareness of the Y2K challenge with small independent telephone companies and small Internet service providers while abating the potential for panic.
2. Encourage all sectors of the telecommunications industry to follow the example of the Telco Year 2000 Forum and expand their efforts to long distance carders, competitive LEC's, etc.
3. Encourage the FCC to put enforceable Y2K compliance policies in place immediately for all groups it monitors and hold the chief executive officers and board directors personally responsible for Y2K compliance statements shared with the FCC.
4. Recommend that the FCC impose an immediate moratorium on telecommunications mergers and acquisitions. The FCC needs to focus its finite resources on issues of national not corporate interest.
5. Consider the formation of Y2K Information Centers across America to inform consumers about not only likely impacts on communications but also the services they purchase from utilities, banks and the like. A recent survey by CIO magazine found nearly 4 in 10 Americans are totally unaware of Y2K. Of those that were aware, one in four plans to put his or her money under their mattress if it becomes apparent the Y2K challenge will not be solved by this time next year.
6. Mobilize millions of Americans to join a grass-roots volunteer effort to help solve the problem. The same CIO survey reported 45 percent of Americans said they would serve if asked. Earlier this month the president challenged retired federal workers to come back and help. This effort needs to be expanded to all. In the CIO survey the under 25 age group responded with most enthusiasm to volunteer. President Roosevelt mobilized this nation early in the century with his visionary civilian conservation corps. People can similarly join to attack the Y2K problem.
7. Create a telephonic version of the Federal Emergency Management Agency that small telephone companies and small Internet service providers could tap into for funds to hire workers to help meet the Y2K challenge.
8. Challenge the telecommunications industry to report back to this committee with an in-depth contingency plan on what will happen if the network goes down. Have the group particularly focus on the contingency plans for rural America, an area largely served by small telephone and Internet service providers. Moreover, task the industry with explaining how it plans to handle the extraordinary volume of calls from consumers demanding Y2K information from their banks, health care providers etc., anticipated in November and December 1999.
9. Work with Ambassador Kamal, head of the Informatics Committee at the United Nations, and encourage the ambassador to hold a major global summit at the United Nations on Y2K this fall.

American lives and the American economy live on the bandwidth provided by our nation's telecommunications infrastructure. Whatever threatens the delivery of that bandwidth threatens lives and the economy in America. The Y2K problem is threatening our nation's ability to deliver noninterrupted bandwidth. No one can come before this committee and say for certain how our national and global telecommunications infrastructure will fare during the digital tsunami known as Y2K. Several things are certain. We are all in this together. We should all prepare for the worst. And we should all pray for the best. Thank you for the opportunity to share this testimony with this distinguished committee.

RESPONSES OF GARY BEACH TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. You recommend the establishment of a special telephonic version of the Federal Emergency Management Agency (FEMA) to provide financial assistance to small telephone and Internet providers. How would you propose this be organized and funded?

Answer. Using the same FEMA infrastructure and processes, have Congress or the administration increase and/or create a special Y2K fund that could be used by companies with 50 or fewer employees.

Question 2. Could you please elaborate on assessment of United States Telephone Association members lack of Y2K preparedness?

Answer. What I have come to learn about publishing information on the World Wide Web is that if a topic is important to Web site editors and their audience, it is prominently displayed on the home page.

In preparation for testimony on July 31, 1998, CIO visited the USTA.org site. Then as now the USTA home page—or other areas on the site—lacks information that would lead CIO to believe the USTA is concerned about the Y2K situation.

Many USTA members are small, independent telephone companies. It is our belief that they employ old telephone switching technology and that many of those USTA members are in rural areas of the United States.

All USTA members are linked to our nation's long distance telephone networks. It follows that Y2K problems in these small telephone companies could be passed along to larger companies.

Question 3. What evidence can you cite to support your assertion that claims of Y2K compliance by the industry are based on hope rather than fact?

Answer. The best evidence of this is the actual testimony of industry representatives at the July 31, 1998, hearing. They conveyed the hope that the industry would be 98 percent Y2K compliant by January 1, 2000, or sooner but confessed that the networks have significant Y2K latency problems.

When a deadly infection enters a body, that body is 99 percent infection free. However, the body can succumb to infection as it spreads. Nothing I heard at the hearing convinced me that the telecommunications industry knows just how compliant it will be on Jan. 1, 2000.

Question 4. What do you predict the state of Y2K readiness will be in the telecom industry on January 1, 2000 based upon your contacts with CIO's nationwide?

Answer. Based on my conversations with CIO's, I predict there will be widespread telecommunication outages across America, particularly in rural parts of our country served largely by small, independent telephone companies without the resources to identify and fix the Y2K problem. Moreover, I predict latent Y2K bugs will continue to plague the nations telecommunications network well into the year 2000.

Question 5. You refer in your testimony to "the great paradox" whereby Y2K compliant telecommunications infrastructures will become "powerful conduits for spreading Y2K problems." Would you elaborate on this and cite specific examples?

Answer. The Great Paradox concept espouses this point of view: Even if the nation's telecommunications infrastructure is 100 percent Y2K-compliant, it may act as a superconductor that will pass Y2K erroneous data through companies connected via that infrastructure in large supply chains.

If the telecommunications infrastructure fails the nation, the consequences will be dire.

For example, many small companies in America—either because they do not have the IT manpower to correct Y2K code beforehand or because they didn't try to fix the code—will incubate errant information. They will pass this information to other companies they are linked to in information food chains.

That errant data could take the form of inaccurate invoices, payments or patient information. Or there could be significant disruptions in our nation's distribution of food, supplies and so on.

CIO recommends that the Senate pay particular attention to the northern areas of the United States from Alaska to Maine because Y2K hits these areas in the dead of winter and major disruptions in telephone, electricity, and heat could prove disastrous.

Question 6. We have heard this morning about the non-participation of the long distance carriers in the Telco 2000 Forum. In you testimony, you recommended that this situation be corrected. Why do you think broader participation is important? What might occur if this situation is not remedied?

Answer. As I stated in my testimony, the Telco 2000 Forum is a positive step. Its major limitation is that it does not include the long distance carriers, though I understand they have invited this group to participate.

This cuts to my major critique of this industry as it faces Y2K. If, for instance, I want to call San Francisco from my offices outside Boston, my voice and/or data call emanates from a local telco (Bell Atlantic), then moves to the long distance carrier of choice (AT&T) to another local telco (GTE) in San Francisco. Unless all of these entities are entirely Y2K functional on January 1, 2000, the probability that my voice/data call will go through decreases.

The nation's telecommunications infrastructure is only as strong as its weakest noncompliant Y2K company.

Question 7. You talk in your testimony about the growing reliance of large and small businesses on their information infrastructures, i.e., electronic data interchange with suppliers and customers. Would you describe examples of the impact of failed telecommunications infrastructure on these businesses?

Answer. Here's an example: Large companies are starting to perform Y2K IT triage with their partners connected in massive EDI or other telecommunication networks where they are abandoning entirely those companies not essential to their critical business processes that may not be Y2K-compliant. Sears Roebuck, Inc. has 5,000 vendors linked in its network. It has identified 900 of those companies—or 18 percent—as critical to making sure Sears does business on Jan. 1, 2000. The

"other" 82 percent of its current partners—or 4,100 companies, most small—did not make the cut. It is my opinion that as they perform Y2K triage larger firms will never go back to doing business with a portion of those smaller suppliers deemed noncritical.

The loss of a Sears type contract could devastate a small business.

PREPARED STATEMENT OF CHAIRMAN ROBERT F. BENNETT

Good morning, and welcome to the fourth hearing on the Year 2000 Technology Problem. To date, we have held hearings on energy utilities, financial services industries, and health care. Future hearings will include transportation, general government services, and general business issues.

Let me begin today's hearing by noting that the global telecommunications infrastructure is the central nervous system of modern society. Daily, 270 million Americans depend on this complex web of voice, data, and video services that enable their telephones, radios, fax machines, computer networks, televisions and other information appliances. Major national and international enterprises, such as emergency response, national security, finance, transportation, health care, government, energy distribution, and others, are critically dependent on reliable, 24 hours a day, 7 days a week telecommunications.

Without these services, our ability to receive, gather, and respond to information would be as limited as it was for our ancestors before Alexander Graham Bell invented the telephone. Some critical enterprises which depend upon telecommunications services include: The National Weather Service; the Department of Defense; the Federal Reserve Board & Wall Street; the National Airspace System; the American Red Cross's Blood Service and the United Network for Organ Sharing; the national electric power grid; and on and on.

However, I have great concerns that our global telecommunications infrastructure can ride out the millennium date change without significant disruptions for three reasons. First, it is a highly complex system of systems. Second is the fact that there is no identifiable U.S. public or private body taking the lead on the global aspects of the Y2K telecommunications problems. Lastly, is the fact that to have successful communications, both parties must be able to send and receive information. It is not enough to be ready just yourself.

With regard to the complexity of global telecommunications, the sheer number of players illustrates the problem. Today in the United States, there are five long distance carriers (not including the growing number of long distance resellers), five major national television broadcasters, six Regional Bell Operating Companies, more than 1,000 small phone companies, 16 communications satellite providers, more than 4,500 Internet Service Providers, hundreds of cellular phone companies, thousands of broadcast radio stations, and over 11,000 cable services companies. And this just captures the infrastructure of the United States and does not include the thousands of large and small communications equipment manufacturers.

Finally, it must be pointed out that this infrastructure relies on hundreds of millions of lines of computer code. It is too great a leap of faith to believe that all the elements of an endeavor this complex will be ready at the stroke of midnight just 17 months from today, especially in the light of the limited readiness the industry has shown to this committee.

As for coordination and oversight of telecommunications, let me note something from a 1995 National Research Council report.[1]

> In 1984 it was quite clear what the telecommunications/information infrastructure was and who defined it. It was, in essence, the telephone and broadcast networks. The defining players were AT&T, the Federal Communications Commission (FCC), and the broadcasters. You got only the connectivity and services that were offered; compared with what is available today, it was not much.
>
> All of this has changed radically. Instead of being defined by monopoly suppliers and regulators, the telecommunications infrastructure has become more closely defined by both market demand and the explosion of supporting technologies that have been brought to market by myriad suppliers. There has been much movement away from a supplier-defined infrastructure to a user-and market defined infrastructure.

---

[1] *The Changing Nature of Telecommunications/Information Infrastructure,* The National Academy Press, 1995.

In this new world of telecommunications which has given rise to a revolution in new services, no one party is charged with the task of assuring the reliability and interoperability of the entire network. This has made the millennium bug a much harder beast to squash as it only has to show up in one link in a communications chain to cause mayhem.

Finally, let me return to the two-way nature of telecommunications. Simply put, if the long distance carrier is up and running, but the regional carrier is down, the long distance call doesn't go through. If the Internet backbones are working, but the local Internet Service Provider is off-line, the World Wide Web is inaccessible to the user. And if a financial payment can be received in New York, but it cannot be sent from overseas, the transaction will not occur.

Like it or not, there is a link-to-link connectivity that starts locally, goes regionally, continues on nationally, and finally, ends internationally in this network upon which telecommunications and the enterprises supported by telecommunications critically depend. I am expecting today's panels to tell us how they are going to take charge and address this challenge. Getting telecommunications ready for the Year 2000 is a massive task that will require tremendous cooperation and coordination, but it is a task we must complete.

PREPARED STATEMENT OF SENATOR JEFF BINGAMAN

Mr. Chairman, today's hearing is very timely. We have only 518 days to make sure that our nation's telecommunications networks are prepared for the Year 2000 (Y2K).

> The telecommunications infrastructure has been revolutionized by advances in information technology in the past two decades to form an information and communications infrastructure. * * * Taking advantage of the speed, efficiency and effectiveness of computers and digital communications, all the critical infrastructures are increasingly connected to networks. * * * Networking enables the electronic transfer of funds, the distribution of electrical power, and the control of gas and oil pipeline systems. Networking is essential to a service economy as well as to competitive manufacturing and efficient delivery of raw materials and finished goods. The information and communications infrastructure is basic to responsive emergency services. It is the backbone of our military command and control system.[1]

We look forward to another century of exciting advances in communications. Yet, we face an unprecedented assault on the reliability and the resiliency of our telecommunications infrastructure because of Y2K problems. While there are many positive indications that the industry is working very hard to solve the Y2K problem, it is critical that we as the Congress, the Federal Government and the nation understand the awesome task facing the telecommunications industry. Telecommunications provide the flow of information on which we depend for national and economic security. Significant failures or unforseen Y2K telecommunications outages could have dramatic impacts on our ability to do maneuver military forces, respond to emergencies or simply do business.

We currently lack the assessments necessary to model potential Y2K failures. Experience, however, does tell us that hardware and software can fail unexpectedly. Private industry and government are both adept at surviving systems failures. But our ability to coordinate and continue operations in the event of a simultaneous wide spread failure is uncertain.

> The susceptibility of the current generation of switching equipment to software based disruption was demonstrated in the collapse of AT&T's long distance service in January 1990. A line of incorrect code caused a cascading failure of 114 electronic switching systems.* * * [Again] the potential for software-based disruption of common channel signaling was demonstrated in June 1991, when phone service in several cities, including 6.7 million lines in Washington, DC, was disrupted for several hours due to a problem with the network's Signaling System 7 protocol. The problem was ultimately traced to a single mix-typed character in the protocol code.[2]

---

[1] *Critical Foundations: Protecting America's Critical Infrastructures.* The President's Commission on Critical Infrastructure Protection; October 1997.

[2] *Critical Foundations: Protecting America's Critical Infrastructures.* The President's Commission on Critical Infrastructure Protection; October 1997.

In software engineering, it is common to find that very process of correcting code introduces new errors. The amount of telecommunications software that must be examined and then corrected is enormous, and it is inevitable that new errors will creep in. While a wide area outage is not necessarily going to result from errors caused through fixing the Y2K bugs, we must be ready for such, and contingency planning must be done.

I am increasingly concerned that the impact of Y2K on the telecommunications industry is not being fully addressed as a national security issue. Could a Y2K related failure cause such a problem in telecommunications? Could an error entered during the millions of lines of code correction cause a serious disruption? If so, would our current emergency response mechanisms be enough? What specific types of contingency planning do we need to consider?

Throughout today's hearing we will endeavor to understand the serious Y2K vulnerabilities facing the telecommunications industry. As we begin this hearing, I think that it's particularly important to remember that the United States has by far the most resilient and reliable telecommunications infrastructure of any nation in the world. In fact, despite the news of network outages and the Galaxy IV satellite failure, the telecommunications industry maintains a 99.9 percent success rate.[3]

As Americans, we look to the future in anticipation. We continually strive to improve the quality of life by improving communications and advancing technology. It is my hope that prompt action and technical communication about Y2K readiness will prevent significant problems. I am confident that the telecommunications industry is determined to meet the communications challenges of the next century. But, I also believe, to assume that the Y2K problem will not affect U.S. telecommunications "* * * is a dangerous complacency." [4]

PREPARED STATEMENT OF JOSEPH CASTELLANO

I. INTRODUCTION

Good morning Chairman Bennett and other members of the Senate Special Committee on the Year 2000 Technology Problem. I appreciate being given the opportunity to address the Committee on the Year 2000 issue.

My name is Joseph Castellano and I am the President—Network and Corporate Systems for the Bell Atlantic Corporation. I am also the officer responsible for leading the Company's Year 2000 program. In that capacity, I chair Bell Atlantic's Year 2000 Steering Committee.

Bell Atlantic is a communications and information company. With more than 41 million telephone access lines and 6.7 million wireless customers worldwide, Bell Atlantic companies are premier providers of advanced wireline voice and data services, market leaders in wireless services, and the world's largest publishers of directory information. Bell Atlantic companies are also among the world's largest investors in high-growth global communications markets, with operations and investments in more than 20 countries.

I have been asked to offer testimony today about the Year 2000 vulnerabilities facing telecommunications carriers and the legal complexities of information sharing.

II. THE YEAR 2000 PROBLEM

As you are aware, the Year 2000 challenge is to ensure that information technology accurately processes date/time data from, into and between the years 1999 and 2000. For the telecommunications industry, like other industries that are so technology dependent, this is a significant challenge, and one we must meet in order to ensure that our communications networks and services continue to perform as our customers expect.

A telecommunications carrier depends to a great extent on computers and their related software to deliver telecommunications services. Communications networks are comprised of a number of network elements, which together allow voice and data to be transported and switched. Many of these network elements contain computers and related software, and they interoperate with other network elements that are also controlled by computers and associated software. Bringing all of these

---

[3] *Network Reliability—The Path Forward*, The Network Reliability Council; February 1996.

[4] Steve Prentice, Director of Research for the Gartner Group in Europe Year 2000 Telecommunications Conference, sponsored by GSA, MITRE Corporation, McLean, VA, April 29, 1998.

network elements into Year 2000 compliance is the primary Year 2000 goal of the telecommunications industry.

The Year 2000 problem also affects other aspects of the telecommunications business in addition to the network itself. Like other businesses, our key business processes—ordering, provisioning, billing, payroll, etc.—are driven by information systems which rely on computers and related software that must be tested and confirmed as being Year 2000 compliant. Similarly, we face Year 2000 issues in connection with the continued operation of our general business infrastructure—elevator controls, air conditioning systems, security systems and even office equipment are all dependent to some degree on computers and related software.

So, like any other business, a telecommunications carrier must also deal with Year 2000 issues outside of its traditional "core business." However, today I will focus my comments on Year 2000 issues uniquely affecting the telecommunications industry, and in particular its network services.

III. HOW THE INDUSTRY IS ADDRESSING THE ISSUE

A. Industry group efforts

The telecommunications industry has at least three industry groups which are involved in the Year 2000 effort—the Telco Year 2000 Forum, the Alliance for Telecommunications Industry Solutions (ATIS), and the International Telecommunications Union (ITU). Although each group operates as an independent entity, they are all addressing Year 2000 compliance testing of network components, interoperability of the network components, and in some cases, testing between different networks. Other speakers will be addressing industry group efforts in greater detail in testimony today.

B. Individual carrier's year 2000 compliance efforts

In addition to the industry level activities, each telecommunications carrier must undertake an effort to identify Year 2000 concerns in its operations and to devise a plan to address each concern. The first step in this effort is to inventory all of the network elements, information systems and computers that could possibly be affected by the century change. As an example of the size of this effort, Bell Atlantic's inventory includes the following:

—Over 350 different types of network elements which Bell Atlantic has deployed tens of thousands of times in its network;
—More than 1,200 software applications, with over 250 million lines of computer code, which support Bell Atlantic's business processes;
—Approximately 88,000 personal computers, 800 mid-range computers, 40 mainframe processors and hundreds of supporting software products;
—Hundreds of unique security access, air conditioning, elevator control, and similar systems servicing thousands of buildings, garages, and other facilities.

Once inventoried, each type of network element and computer and each information system must be assessed to determine if it is Year 2000 compliant and, if not, when and how it will most likely fail. Knowing when a component may fail is important because this will influence the sequence and prioritization for correcting that component. Because telecommunications carriers purchase the vast majority of their network elements, information systems and computers from others, an extensive program of equipment vendor communication is necessary. Carriers must know what steps an equipment vendor is taking to make its products Year 2000 compliant.

Also, as part of this inventory and assessment activity, it is necessary to assign some level of priority for the remediation or replacement of network components. For example, network elements and related software that would have an immediate and severe impact on customer service in the event of failure should be assigned a higher priority than that given to a non-critical system.

Detailed planning follows assessment. In this phase, plans are developed for the remediation or replacement of each type of network element and computer and for each information system. Even components found to be compliant during assessment will require testing or verification to validate manufacturer-provided information. For those components evaluated as non-compliant, we must determine if they should be fixed or replaced. Detailed plans must include all activities required to insure that the particular components will operate correctly. Thousands of such plans must be developed by a carrier and its vendors. By the third quarter of this year, detailed planning should be completed or nearly complete.

As part of this planning phase, special attention must be paid to telecommunications systems and network components supporting emergency services, such as

911 services. Together with cities, towns and municipalities who operate such emergency service systems, and the manufacturers of the equipment used in these systems, telecommunications carriers share a common goal—to ensure that these and similar essential services remain unaffected by Year 2000 problems. Emergency services should remain a top priority in any telecommunications carrier's overall Year 2000 plan.

The next stage of a Year 2000 plan consists of testing compliant components; remediating and testing non-compliant components that will be retained; and replacing those components that will be retired. This is the stage most carriers are at currently and it is by far the most complex. Carriers on track to meet Year 2000 targets would have begun this phase in 1997; however, the majority of the work will be completed in 1998 with some to be completed in 1999. During this phase, new and remediated network elements, computers and information systems are comprehensively tested. These tests include testing for date handling, interface testing and regression testing. Regression testing assures that no other function of the component has been adversely affected by the remediation.

Once network elements, computers and information systems are fully tested, they can be deployed. For network elements, this requires the development of extensive deployment schedules, which must be coordinated with other network changes and supported by equipment vendors. Where a new information system is being installed to replace a non-compliant system, deployment will require that employees receive training in the new system. In addition, personal computers have to be replaced or upgraded, requiring extensive fieldwork by maintenance personnel. Deployment for most companies has begun and will continue through early 1999, with some additional deployment occurring after that.

Finally, it is important for a carrier to develop comprehensive contingency plans. These plans should address action required in the event that scheduled activities, such as replacement of a particular software application, do not occur on time, as well as planning for the possible failures of suppliers and internal operations. A contingency plan should also include the establishment of internal, industry and customer command structures to effectively manage critical situations. Initial contingency plans should be developed by the end of 1998, but these plans will necessarily evolve as circumstances require.

A comprehensive and effective Year 2000 program should also include a company-wide management structure and process—a senior officer responsible for overall leadership; an officer level steering committee (or similar group) representing all critical operations of the business with responsibility for establishing policy, resolving issues and monitoring the progress of the Year 2000 program; and a Program Office which provides a dedicated staff for central management and support of all Year 2000 activities.

C. Interrelated nature of telecommunications industry—a year 2000 concern

The performance and integrity of the worldwide communications network is primarily dependent upon: (i) The performance of the various network components and software manufactured by numerous equipment vendors; (ii) the integration of these network components by telecommunications carriers within their networks; and (iii) the interoperability of the separate networks owned and managed by numerous telecommunications carriers throughout the world.

Given this interdependency, it is critical that each equipment vendor and each carrier properly address its own Year 2000 issues, and that equipment vendors and carriers work cooperatively to ensure a seamless, uninterrupted operation of this global network. Information sharing among carriers and between carriers and their equipment vendors is essential. Likewise, information sharing between carriers and their customers is equally critical to enable customers to understand and address their Year 2000 requirements.

If an equipment vendor is not able to provide and support functional, Year 2000 compliant replacements or upgrades, that failure will likely have a material adverse impact on a carrier's Year 2000 efforts. Likewise, if a carrier fails to properly address its Year 2000 issues and a service disruption occurs, that carrier's customers will be affected, as will interconnecting carriers. The telecommunications industry is also dependent upon other suppliers of essential services, such as electric utilities, to successfully address their Year 2000 issues. For example, a serious disruption in electric power supply that results from a Year 2000-related failure will certainly interfere with a telecommunications carrier's ability to provide uninterrupted network services.

Although contingency planning will help mitigate the impact of supplier and carrier Year 2000 failures, contingency planning cannot be the solution. Each supplier

and carrier must address its Year 2000 issues, and must share with others the status of its Year 2000 efforts and other relevant Year 2000 information.

IV. LEGAL CONCERNS IMPEDING INFORMATION SHARING

In recent times, "Year 2000" has become a topic of considerable interest within the legal community. One has only to attend a few of the numerous seminars on the subject given by law firms, legal education organizations and others, with titles such as "[t]he Next Wave of Year 2000 Litigation" or "Year 2000 Liability" to understand why these issues are steadily driving businesses and their attorneys to distraction.

Year 2000-related liability is often mentioned in connection.with a variety of possible claims, including: actions under the federal securities laws; breach of contract or warranty; negligence (including negligent misrepresentation); product liability; antitrust; and defamation or product disparagement.

As discussed above, information sharing plays a critical role in the successful implementation of Year 2000 plans. Our experience has shown that liability concerns have an adverse impact on the free exchange of Year 2000-related information among businesses. These concerns affect not only the level or content of the disclosure but also the timing of the information exchange.

Given the compelling need to share Year 2000 information, we favor legislative action to reduce liability concerns in this area. In particular, we support legislation such as the proposed Year 2000 Information Disclosure Act to encourage the disclosure of Year 2000 information and urge your Committee to support its passage as well.

V. SPECIFIC GOVERNMENT ACTIONS TO SUPPORT REMEDIATION

Government can play a key role in supporting the telecommunications industry in our Year 2000 efforts.

First, passage of legislation such as the Year 2000 Information Disclosure Act to facilitate a more open and timely disclosure of information would be quite helpful.

Also, both federal and state agencies are properly attempting to gather as much information as possible from the entities within their jurisdiction in an effort to understand the issues confronting businesses and progress on Year 2000 matters. We believe that consideration should be given to the development of a more uniform approach to information gathering from the telecommunications industry. A uniform approach to information gathering would improve the usefulness of the information provided and minimize the impact on personnel working to address Year 2000 problems.

VI. CONCLUSION

I would like to thank the committee for allowing me to address the issues facing the telecommunications industry with respect to the Year 2000.

RESPONSES OF JOSEPH CASTELLANO TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. In your discussion on the steps to remediate systems with Y2K problems, you said regarding testing that "carriers on track to meet Year 2000 targets would have begun this work in 1997." What does this imply for companies that are just starting or haven't started testing yet?

Answer. This question, as stated, does not fully capture my testimony. In my statement, I testified that: "The next stage of a Year 2000 plan consists of testing compliant components; remediating and testing non-compliant components that will be retained; and replacing those components that will be retired. This is the stage most carriers are at currently and it is by far the most complex. Carriers on track to meet Year 2000 targets would have begun this phase in 1997; however, the majority of the work will be completed in 1998 with some to be completed in 1999." This phase of an overall Year 2000 plan includes much more than just testing. In addition, work in this phase of the plan will continue through 1999.

Thus, in our view, carriers who are "on track" would have at least started this phase in 1997. Viewed from a different perspective, if by the end of 1997 a major carrier has not at least started these activities—testing compliant equipment, remediating and/or testing of remediated components—meeting 2000 objectives would be more of a challenge. Of course, each company's situation is unique to the size and nature of its operations network. Therefore, no generalization should be made based

on my testimony without looking at the nature and magnitude of a particular company's network facilities.

Question 2. Would you please elaborate for the Members of the Committee on the anticipated effect of the legislation proposed by the White House if it passes Congress this year? Will it change the picture of the telecommunications information landscape?

Answer. The Year 2000 Information Disclosure Act provides some protection against liability to the maker of a statement regarding Year 2000 processing in actions based on an allegedly false, inaccurate or misleading Year 2000 statement, and defamation or product disparagement actions. By addressing these concerns, the Act will clear the way for timely, meaningful and necessary disclosures. Obviously, the more information that is exchanged efficiently between and among manufacturers, suppliers and customers, the more effective each company can become in addressing its Y2K issues.

Bell Atlantic's experience has been that companies are reluctant to make statements about Year 2000 readiness. If such statements are made, the maker most likely will require the recipient to sign either a non-disclosure or a limitation of liability agreement, or both. These non-disclosure agreements often impede the further dissemination of the relevant information, which reduces the effectiveness of a company and the industry in addressing the Y2K issues. In addition, negotiation of these agreements occupies precious time and can delay the remediation and testing process. Bell Atlantic believes that the proposed legislation will lower the concerns of companies making Y2K statements, expedite the exchange of information and allow companies to fully focus on evaluating and fixing any Y2K problems.

Question 3. What are the potential impacts of the proposed merger between Bell Atlantic and GTE on their individual and combined Y2K readiness? Won't the merger disrupt Y2K programs as the combined company strives to integrate systems and services?

Answer. We believe that our proposed merger with GTE will have no discernable impact onY2K readiness of Bell Atlantic or GTE. At least for the foreseeable future, each company will continue to manage its Year 2000 Programs independently through completion. Also, we believe that most merger integration activities are likely to occur shortly before or even after January 1, 2000, and will, therefore, have little impact on each company's individual Y2K readiness.

PREPARED STATEMENT OF SENATOR SUSAN M. COLLINS

Let me first thank you Mr. Chairman for holding today's hearing on this important topic. As you have mentioned before, a breakdown in the telecommunications sector could lead to a modern day version of the Tower of Babel. However, rather than not being able to speak to each other because of a language difference, this time it would be because our communication systems malfunctioned.

We have a couple of recent examples of the consequences of a failure in our communications systems. On April 13, AT&T's high-speed data network failed, leaving banks, retailers, and even the Red Cross scrambling to adjust to a telecommunications breakdown. And as I think most of us learned, on May 19, a communications satellite went into an uncontrolled spin, dizzying credit card authorization services and disrupting paging services for almost all of the pagers in the United States.

Obviously, a safe and viable telecommunications system is absolutely critical to our daily lives. I look forward to our witnesses' testimony.

PREPARED STATEMENT OF VICE CHAIRMAN CHRISTOPHER J. DODD

Thank you Mr. Chairman. I also want to express my appreciation to our colleague Senator Bingaman, who has taken on the difficult task of acting as the committee's point person on the telecommunications issue.

Before we turn to this very important topic, let me provide the members of the committee with a brief follow-up on our hearing last week.

As you may recall, both Chairman Bennett and I expressed our disappointment with those medical device manufacturers who had chosen not to comply with either the FDA's requests for information, nor with four separate requests for information from the Veterans Administration.

In particular, Dr. Kizer of the VA testified that 233 manufacturers had failed to respond, to their requests for information. However, I have been informed that after he returned to the VA from the hearing, his phone started ringing off the hook. As of today, that list of 233 has been reduced to a list of 99.

I also want to report that the chairman and I met with senior officials from the Health Industry Manufacturers Association earlier this week.

At that meeting, HIMA told us that they are going to reverse their policy of not cooperating with the FDA's requests for information, and will issue a letter early next week urging their 800 members to cooperate more fully with requests from both FDA and from the hospitals and clinics that use their medical devices.

We have, after much unnecessary obstruction from HHS, obtained from FDA the list of 2,200 manufactures of computerized medical devices that have not responded to their June 29 letter; we will watch closely over the next week or so to see how many of them begin to comply with FDA's information request.

We also have the list of the 99 manufacturers who still have not complied with VA's request for information and will also watch closely to see if that list continues to shrink.

We will also be watching to see that both HHS and FDA follow the injunction given to them by OMB way back on May 15 to become more aggressive in pursuing this information.

In order to mare sure that everyone has incentives to work cooperatively and voluntarily on this matter, Senator Bennett and I will be introducing legislation that mandates the cooperation of medical device manufacturers with FDA's request for information.

While I hope that it will not be necessary to pass such legislation, our forebearance will depend on FDA and the device manufacturers honoring their commitments to improve their performance to date.

I don't want to delay the hearing much longer with extended remarks, so let me just say that while I believe that the telecommunications industry has made good progress to date, I am somewhat disappointed that there has been no single entity designated to act as a clearinghouse for all the participants in the telecommunications industry.

While key individual companies have done assessing their Y2K problem, the real proof will come in the testing.

Unlike the securities and banking industries, it isn't possible for the telecommunications industry to take their system off-line to run a test. There are no weekends or holidays for phone service.

As a result, creating a sound testing environment, and in particular, trying to mare sure that the tests involve as many segments of the industry as possible, are critical hurdles that the telecom industry has yet to face.

I also hope that the panel of experts will focus on the readiness of foreign telecom companies and will assess for us the possibility of international disruptions impacting both U.S. domestic telecom service and, perhaps more importantly, whether there is a real possibility that we will not be able to communicate with people and businesses operating abroad.

As the committee has noted in each of its previous three hearings, contingency planning that starts today is a necessary part of any meaningful effort to confront the year 2000 problem.

Given the necessity of telecom service to continued economic growth and given the importance of simple phone service to every household in America, serious and significant plans must be in place soon to deal with any possible disruptions.

Thank you Mr. Chairman and Senator Bingaman for all of your work on this important topic and I look forward to the today's testimony.

PREPARED STATEMENT OF JOHN S. EDWARDS

I. INTRODUCTION

Thank you, Mr. Chairman, for the opportunity to testify here today on behalf of the President's National Security Telecommunications Advisory Committee (NSTAC). My name is Dr. John S. Edwards, and I am a member of the NSTAC's Industry Executive Subcommittee (IES) and Chair of its Network Group. For 16 years, the NSTAC has advised the President on issues pertaining to the reliability and security of telecommunications and the information infrastructure—issues critical to national security and commercial interests. The year 2000 (Y2K) issue is at the forefront of current NSTAC work and we, particularly the Network Group, have been aggressively addressing Y2K issues for some time. If approved by the NSTAC at its twenty-first meeting on September 10 of this year, the NSTAC will forward its Y2K recommendations to President Clinton.

Disclaimer

The NSTAC, a presidential advisory committee, provides industry-based telecommunications policy advice directly to the President, and its activities are governed by the Federal Advisory Committee Act (FACA). The NSTAC principals must approve any findings/recommendations of the subordinate working groups before they are officially declared NSTAC positions. Therefore, any information on the findings/recommendations of NSTAC's subgroups cannot be disseminated or discussed until approved by the NSTAC principals. All approved NSTAC reports and recommendations are posted on the NSTAC homepage at http://www.ncs.gov.

II. NSTAC

Established by President Ronald Reagan in 1982 in anticipation of the divestiture of AT&T, the NSTAC, a high-level industry advisory group, provides the President with a unique source of national security and emergency preparedness (NS/EP) telecommunications policy expertise and advice. Membership in NSTAC is limited to 30 presidentially appointed industry leaders who are senior executives (often chief executive officers) representing major telecommunications carriers, information system providers, manufacturers, electronics and aerospace firms, system integrators, and the financial services industry. (NSTAC's membership list is attached as Appendix A.) The IES, the principal NSTAC working body, consists of representatives appointed by each NSTAC principal. In accordance with FACA, the Manager, National Communications System (NCS), serves as the Designated Federal Official for the NSTAC. Through the NCS, the NSTAC coordinates its activities with the Federal Government. An interagency group created in 1963 initially to address communications failures during the Cuban Missile Crisis, the NCS was re-chartered in 1984 to plan and coordinate NS/EP telecommunications during times of crisis or disaster.

The NSTAC and NCS are long-standing and successful industry-Government and intergovernmental partnerships on NS/EP telecommunications, respectively. In December 1982, the NSTAC formed a task force to facilitate industry-Government response to the Government's growing NS/EP telecommunications service requirements in the post-divestiture environment. The task force was charged to identify and establish the most cost-effective mechanism to coordinate industry-wide response to NS/EP telecommunications requests. To that end, the task force report, submitted to the NSTAC in 1984, led to formation of the NCS's National Coordinating Center for Telecommunications (NCC). The NCC emergency response coordination center supports the Government's NS/EP telecommunications requirements and assists with the provision and restoration of telecommunications services during emergencies. Entities such as the NCC and the separate NSTAC and Government Network Security Information Exchanges are examples of existing coordinating partnerships developed by the NCS and NSTAC. They have established levels of industry-Government trust, cooperation, and information exchange critical to protecting the Nation's telecommunications infrastructure. To further enhance the trusted environment for information exchange, participation in NSTAC and in NSTAC-related activities is done on a non-attribution basis.

During its 16-year history, the NSTAC has evolved to mirror the dynamic changes in the telecommunications industry. As information systems have become more critical to the day-to-day operations of telecommunications and computing networks, the NSTAC has broadened its focus to consider potential NS/EP implications. In addition, and in keeping with the national security strategies articulated by Presidents Bush and Clinton, the NSTAC has considered the economic security dimensions of telecommunications and information system issues.

Today, the NSTAC is recognized as a model for industry-Government collaboration. Its substantive recommendations to the President have led to enhancements of the Nation's NS/EP telecommunications and information systems posture. Enhancements in the form of operational programs and policy solutions benefit both industry and Government as the Nation's security requirements and telecommunications infrastructure continue to evolve.

III. NSTAC Y2K ANALYSIS

In January 1998, the Manager, NCS, asked the NSTAC to update the President on the telecommunications industry's actions to ensure continuity of service through the millennium change. In response to this request, the NSTAC directed its Network Group to address the Y2K problem. The group's review of Y2K readiness covered the national telecommunications infrastructure and related NS/EP issues.

The Network Group broadly reviewed the telecommunications industry Y2K status by soliciting briefings from interexchange carriers, local exchange carriers, switching system vendors, large-scale system integrators, and Y2K risk assessment

and remediation solution providers. Several NSTAC member companies described their companies' Y2K initiatives and provided their perspectives on the Y2K problem. In addition, the Network Group heard briefings from the Telco Year 2000 Forum and the Alliance for Telecommunications Industry Solutions (ATIS) on their respective, cross-industry Y2K initiatives. By providing a unique forum for open discussion, the NSTAC's Network Group was able to generate valuable insight into the state of the industry. Based on the information gathered, the group's report to the IES included a consideration of the current Y2K readiness of the major telecommunications service providers and equipment vendors. I would like to share some of our observations.

In a briefing to the Network Group, the following information was offered to provide perspective on the magnitude of the Y2K problem for the telecommunications industry:

—A telecommunications company is generally a "large enterprise." For example, there may be 1,400 to 1,600 switches, 30 to 50 signal transfer points, 5 to 60 service control points, thousands of transport component systems, and many element management systems and operations systems, any one of which could have multiple date-sensitive functions.

—75 percent of voice networking devices are date-sensitive.
—25 percent of data networking devices are date-sensitive (25–35 percent for intelligent devices).
—100 percent of network management devices are Y2K impacted.

Clearly, the telecommunications industry needs to be aggressive in its Y2K approach—and it is. Efforts to make the telecommunications infrastructure Y2K-ready are well underway. In fact, the major service providers and their vendors have been working on these issues for several years. The Telco Year 2000 Forum and others (e.g., the General Services Administration and ATIS) are planning interoperability testing for critical products, networks, services, and systems. Those who briefed the Network Group on their Y2K initiatives expect the majority of critical products and networking to be Y2K-ready between late 1998 and early 1999.

According to the Telco Year 2000 Forum's briefing to the Network Group, the objective of the forum's network interoperability testing is to minimize the risk of network and service failures and ensure that functionality of date/time sensitive operations is not adversely affected. The forum also serves to provide a common view to telecommunications hardware/software suppliers regarding Y2K solutions, and encourages hardware/software providers to adhere to product and service implementation schedules. The forum's test of Y2K compliant products and services, scheduled for 3rd–4th quarter 1998, is designed to address the interoperability of components within discrete networks, rather than between networks. This intra-network interoperability testing will include the major North American suite of equipment and will cover emergency services (E911/911); basic, enhanced, and intelligent services; network management and operations, administration, maintenance, and provisioning operations support systems; data networks; and customer premises equipment. The interexchange carriers are not participating in the Telco Year 2000 Forum's intra-network interoperability test but are conducting their own intra-network tests of their products and services.

In a briefing by ATIS, the Network Group learned that ATIS is planning to conduct internetwork interoperability Y2K readiness testing to verify that there are no adverse effects on interconnected networks. The pretest and set-up work to support the testing is currently underway, with an anticipated completion date in 4th quarter 1998. This testing will be conducted during January and February 1999. The items identified for testing include mass calling events on December 31, 1999; potential congestion; cross-network services; rollover to Y2K in the local number portability (LNP) environment; impact of time zones; and key dates in an LNP environment (December 31, 1999, February 29, 2000, and December 31, 2000). Although ATIS plans to test the effects of mass calling events on the switching networks, it does not plan to test network management controls within network management operations support systems. ATIS's internetwork interoperability testing initiatives will include inter-exchange carrier participation.

Service providers and vendors know their companies' futures depend on how effectively they address their Y2K problems. Consequently, they are devoting substantial resources to achieving Y2K readiness. Their initiatives include taking comprehensive inventories of their systems, prioritizing them, assessing the extent to which they are date-sensitive, and then implementing and testing solutions. The telecommunications industry has been able to sustain its high level of reliability, in part, because it has traditionally conducted extensive regression testing. This should

minimize the adverse effects to the reliability of the public network (PN) caused by efforts to correct Y2K problems. However, as with any software implementation, it is not possible to foresee, and test for, every possible adverse interaction. Since Y2K readiness preparation is a massive, diverse, pervasive, and complex software augmentation, even the most thorough, exhaustive efforts may fail to achieve 100 percent success.

No organization, either private or Government, in their brief to the NSTAC's Network Group offered a guarantee on total eradication of the Y2K problem from their networks, services, or systems. In addition, these organizations could not offer guarantees of the adequacy of Y2K internetwork interoperability testing. Many felt the millennium change was not a January 1, 2000, problem, but a problem that would begin before, and extend well beyond, that date.

Though not yet approved by the NSTAC, the Network Group's report focuses on the current status of efforts to prepare the telecommunications infrastructure for Y2K, factors affecting these efforts, and problems possibly resulting if these efforts are not fully effective. Because the telecommunications infrastructure is essential to maintaining the national security posture and responding to man-made and natural disasters, the Y2K report gives particular attention to NS/EP telecommunications. The report recommends actions to the President to enhance the Y2K readiness of NS/EP telecommunications and to mitigate the impact of Y2K-induced service disruptions on the Nation's NS/EP posture. Further, the Network Group's report recommends actions for the NSTAC to help the Government respond to Y2K-induced service disruptions.

Because the the Network Group's Y2K report is pending final approval by the NSTAC, specific comments on the group's findings and recommendations are not available for public disclosure at this time. If the report is approved as anticipated at the September NSTAC meeting, the recommendations will be forwarded to the President and subsequently made available to interested parties. It would be our pleasure to forward copies to you, Mr. Chairman, and to other members of this committee at that time.

IV. NSTAC 1997 WIDESPREAD OUTAGE SUBGROUP REPORT

In addition to reporting on our important Y2K work, we also have been asked to comment this morning on the NSTAC's 1997 report to the President addressing the probability of a widespread telecommunications outage. (The report is attached as Appendix B.) While this report preceded and is not connected to NSTAC's current assessment of Y2K issues, it is highlighted today to convey our understanding of contingency planning for, and recovery from, a severe telecommunications outage, should one occur.

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, asked the NSTAC to provide its views on the possibility of a widespread service outage in the public telephone network. The NSTAC's Widespread Outage Subgroup (WOS) was established in July 1997 to address Dr. Gibbons' inquiry. The NSTAC approved and forwarded to the President on December 10, 1997, the group's final report.

The WOS began its task by developing a definition of a widespread telecommunications outage. It was defined as—

> A sustained interruption of telecommunications service that will have a strategic significance to Government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day.[1]

The WOS report recognized threats to, and vulnerabilities of, the public telecommunications network, such as equipment malfunctions, natural hazards, sabotage, and physical design. It also assessed potential concerns posed by the changing network environment (e.g., new technologies and regulatory mandates), as well as concerns that the growing threat from information intrusions could trigger systemic network failures.

---

[1] "Report on the Likelihood of a Widespread Telecommunications Outage," The President's National Security Telecommunications Advisory Committee, December 1997. (See Appendix B.)

Findings of the widespread outage report

The U.S. telecommunications service providers have historically offered unparalleled robustness, availability, and quality. Although the track record of the PN is superlative, natural and technological threats could adversely affect telecommunications services. These same threats could also disrupt other critical infrastructures, such as electric power, on which the PN is highly dependent for sustained operation. While the PN's supporting technologies provide an expanding array of services and features, and facilitate robustness, these same supporting technologies can introduce exploitable vulnerabilities with adverse effects on service availability and reliability.

The WOS report addressed several key issues. Perhaps most important, it examined the extent to which a widespread, sustained interruption of public telephone service—caused by common equipment or software failures, sabotage, or any other factor—was a realistic concern. The WOS determined the probability of such an outage to be low. Nevertheless, because of the potential impact of a widespread outage, industry's response to such an event must be given consideration.

To that end, the report looked at industry's plan for intercarrier coordination to facilitate recovery of the network from a widespread outage. The WOS found that existing carriers had disaster recovery plans in place for quickly recovering from outages. Many of these recovery plans include bilateral and multilateral mutual aid agreements, designed to address multicarrier network problems. These agreements focus on resource sharing, such as supplies, portable equipment, motor vehicles, personnel, and may also dictate arrangements for temporary routing of traffic and services over another carrier's spare facilities. In addition to formal agreements, informal arrangements were found to exist throughout the industry for intercarrier and carrier-vendor communication and cooperation during emergencies. The vast majority of telecommunications disruptions requiring a multicarrier/vendor response effort are addressed through industry cooperation. Instead of precisely defining the scope of network sharing or resource lending arrangements, the industry approaches each incident with a customer-focused "can do" approach with a long history of success. Informal arrangements offer additional flexibility in dealing with emergencies because each telecommunication outage situation is unique. These informal arrangements leverage relationships between network managers already established within the industry through day-to-day interaction and operations.

The industry has had limited experience with a systemic, widespread network outage. Therefore, the WOS found there was no industrywide plan to facilitate intercarrier coordination for recovering from a widespread outage of this nature. While an industrywide plan had not yet been developed, companies had prepared internal plans and processes for maintaining the integrity of their own networks. These plans and processes included specifics for diagnosing problems, identifying solutions, and ensuring service could be restored as rapidly and orderly as possible.

Looking further at contingency planning and recovery from a widespread outage, the NSTAC's subgroup also questioned whether existing communication and coordination mechanisms among service providers were adequate for the efficient diagnosis of the problem, identification of technical solutions, and restoration of service. Although some agreements, communications systems, and coordinating mechanisms were found to exist between and among carriers, it was questionable whether they would be sufficient response to a severe widespread service outage. To assist in service restoration, most of the larger telecommunications companies have alternate communications capabilities between critical centers in their networks. Reconnection with other networks would be initiated only after individual carriers were confident of the health of their own network and those to which they were connecting. During this phase, a means of communication and coordination between and among critical centers would be indispensable. Several communication capabilities exist outside the PN for intercarrier coordination of service, including, for example, the NCC's network, the National Telecommunications Coordinating Network (NTCN).

The WOS report also identified legal and regulatory obstacles to a rapid recovery from a widespread outage. The NSTAC's Legislative and Regulatory Group (LRG) further analyzed these legal and regulatory obstacles and found the most significant barrier to be uncertainty regarding which authority could expeditiously address carriers' concerns regarding their compliance with relevant laws or regulations during emergency situations. The LRG is investigating the seriousness of that concern and will present its findings and recommendations at the September 10 NSTAC meeting.

Finally, the WOS report found the NCC to be the appropriate interface between the telecommunications service providers and the Government. This interface will assure the President that restoration priorities meet the national interest. For many years, the telecommunications industry has voluntarily provided the NCC with relevant information pertaining to major outages. In addition to having notable experi-

ence, the Office of the Manager, NCS, has a direct communications capability with the Executive Office of the President to keep the President apprised of the progress of restoration efforts in the event of an outage affecting multiple companies.

Recommendations of the widespread outage report

Contingency planning is key. Recognizing that there can be no ironclad guarantee against a widespread outage, the report offered several cost-effective recommendations for the President and the NSTAC to further decrease the overall probability of a widespread outage and to improve recovery plans and procedures. The following recommendations are quoted from the report:

—*Improve Intercarrier Coordination for Widespread Outage Recovery.* Because industry plans and coordination procedures for responding to a widespread telecommunications outage were found to be company-oriented, the Network Group recommended that the President direct the appropriate Federal departments and/or agencies to work with industry to improve intercarrier coordination plans and procedures.

—*Remove Legal and Regulatory Obstacles to Widespread Outage Recovery.* The WOS recommended that the President encourage the Federal Communications Commission (FCC) to maintain a Defense Commissioner at all times to help industry and Government overcome legal and regulatory impediments to widespread outage recovery. In addition, it was recommended that the President encourage the FCC to guard against premature implementation of "unseasoned" technologies that might contribute to the possibility of a widespread outage.

—*Advance the State-of-the-Art for Software Integrity and Interoperability to Reduce the Probability of a Widespread Outage.* All U.S. infrastructures, including the PN, continue to be increasingly reliant on software-controlled information systems. Security analysis of software products is not universally practiced by major equipment manufacturers. It is possible, because of the complexity of the large systems involved, that hidden, malicious code, or unintentional code interactions could allow unauthorized access to network systems or lead to protracted denial of service. The WOS recommended that the President task the appropriate Federal departments and agencies to work with industry to advance the state-of-the-art for software integrity. In addition, the WOS recommended that the NSTAC work to increase awareness within the telecommunications industry of the importance of software security and the use of best business practices for managing complex automated systems.

—*Expand Research and Development (R&D) Efforts to Address Telecommunications Technology Vulnerabilities.* The WOS advised the President to direct the expansion of government R&D efforts to address the most significant vulnerabilities of new and evolving telecommunications technologies and services. As a specific case, the WOS recommended that the President encourage the FCC to examine and assist with the implementation of the Network Reliability and Interoperability Council (NRIC) recommendations related to potential widespread outage vulnerabilities attributed to physical network design and new supporting technologies.

—*Foster Education and Awareness.* The WOS recommended that NSTAC, as part of its outreach efforts, offer the NSIE model to the Network Interconnection/ Interoperability Forum (NIIF) for consideration and potential use by network operations managers. The NSTAC was also encouraged the use the NSIE model to help foster effective plans, procedures, and intercarrier relationships in the increasingly competitive telecommunications environment.

The NSTAC is continuing to monitor issues related to the reliability and security of the PN and will provide future recommendations in that area should they be necessary.

V. CLOSING

In light of the potential threat posed by Y2K, we are experiencing a heightened emphasis on protecting our Nation's critical infrastructures. Simultaneously, "worse case scenario" contingency planning has gained broader public interest in the face of what is a widely publicized technology and management problem. Our national infrastructures—including telecommunications, financial services, electric power, and transportation—represent the cornerstone of our Nation's economic, political, and military strength. These interdependent infrastructures rely on a growing and vital web of communications, computer, and associated information technologies. Similarly, natural and technological threats—including those posed by Y2K—could disrupt other critical infrastructures, specifically electric power, on which the information infrastructure is highly dependent for sustained operation. Understanding

and addressing the interdependent nature of critical infrastructures is immensely important to protecting the Nation from an unmanageable Y2K crisis and must not be overlooked.

The NSTAC believes the telecommunications infrastructure is robust and reliable, but even the most exhaustive efforts can not guarantee total Y2K eradication from networks, services, or systems. Further, we must understand that the millennium change is not a January 1, 2000 problem; it is a long-term problem beginning before, and extending well beyond the ringing in of the new century. The NSTAC will continue to focus on NS/EP communications and overall continuity of service in light of the Y2K problem. Of course, information sharing is crucial to our efforts, and for that, we will rely on our long-standing success as a unique and trusted environment for high-level industry exchange of critical NS/EP telecommunications information.

We appreciate the opportunity to testify today. The NSTAC looks forward to sharing the results of its Y2K analysis with you pending final consideration and approval of the report.

APPENDIX A.—NSTAC MEMBERS

THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE (NSTAC)

MEMBERSHIP (AS OF JULY 21, 1998)

Mr. Lester M. Alberthal, Jr., Chairman and CEO, Electronic Data Systems (EDS)
*Mr. John H. Mattingly, President, COMSAT Satellite Services, COMSAT Corporation
*Mr. C. Michael Armstrong, Chairman and CEO, AT&T
*Mr. Michael T. Smith, Chairman and CEO, Hughes Electronics Corporation
*Mr. James W. Evatt, President, Information Services and Communications Systems, The Boeing Company
Dr. J. Robert Beyster, Chairman and CEO, Science Applications International Corporation (SAIC)
Ms. Margo H. Briggs, President and CEO, Executive Security and Engineering, Technologies, Inc. (ESET)
Dr. Vance D. Coffman, CEO and Vice Chairman, Lockheed Martin Corporation
*Mr. J. D. Cosgrove, President, Avionics and Communications Rockwell Collins, Inc. Rockwell International Corporation
Mr. D. Travis Engen, Chairman, President and CEO, ITT Industries, Inc.
Mr. William T. Esrey, Chairman and CEO, Sprint Corporation
Mr. Joseph T. Gorman, Chairman and CEO, TRW, Inc.
Mr. William J. Hilsman, Chairman, Advanced Digital Technologies Company (ADTC)
Mr. Van B. Honeycutt (NSTAC Vice Chair), President and CEO, Computer Sciences Corporation (CSC)
Mr. Charles R. Lee (NSTAC Chair), Chairman and CEO, GTE Corporation
Mr. Craig O. McCaw, Chairman, Teledesic Corporation
Mr. Solomon D. Trujillo, President and CEO, US WEST, Inc.
Mr. Robert W. Orent, First Vice Chairman, U.S. Telephone Association (USTA)
*Mr. Dennis J. Picard, Chairman and CEO, Raytheon Company
Mr. Bert C. Roberts, Jr., Chairman and CEO, MCI Communications Corporation
Mr. Charles E. Robinson, Chairman, President and CEO, Pacific Telecom, Inc. (PTI)
Mr. Donald J. Schuenke, Chairman, Northern Telecom, Inc. (Nortel)
Mr. Larry Schumann, President and CEO, National Telecommunications Alliance, Inc.
*Mr. John W. Sidgmore, Vice Chairman and CEO, WorldCom, Inc.
Mr. Martin A. Stein, Vice Chairman, Automation and Support Services, BankAmerica Corporation
*Mr. Gary L. Tooker, Chairman, Motorola, Inc.
*Mr. Lawrence A. Weinbach, Chairman and CEO, Unisys Corporation

*Approval pending at The White House.

APPENDIX B.—NETWORK GROUP 1997 WIDESPREAD OUTAGE SUBGROUP REPORT

EXECUTIVE SUMMARY

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, requested that Mr. Charles Lee, Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), provide NSTAC's forward-looking views on the possibility of a widespread service outage in the public telephone network. The Widespread Outage Subgroup was established in July 1997 to address Dr. Gibbons' letter.

A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would impact the availability and integrity of telecommunications service for at least a significant portion of a business day.

U.S. telecommunications service providers have historically offered robustness, availability and quality unparalleled by other public services. Although the public network (PN) track record is superlative, natural and technological threats could adversely affect telecommunications service. These threats could also disrupt other critical infrastructures, such as electric power, on which the PN is highly dependent for sustained operation. While the PN's supporting technologies provide an expanding array of services and features, and facilitate robustness, these same supporting technologies can introduce exploitable vulnerabilities with adverse effects on service availability and reliability. Considering these threats and vulnerabilities, the potential concern for a widespread network outage is reasonable. Given the limited precedent for telecommunications outages of this magnitude, NSTAC members' prior experiences with smaller-scale outages lead them to believe there is a low probability of a widespread, sustained outage of public telephone service. The potential societal impacts of such an outage are high enough to warrant consideration.

The Widespread Outage Subgroup offers the following cost-effective recommendations for the NSTAC and the President to decrease the overall probability of a widespread outage. These measures will further facilitate the readiness of the PN for a more open, interconnected, and uncertain global information infrastructure.

—*Improve Inter-Carrier Coordination for Widespread Outage Recovery.*—Current industry plans and coordination procedures for responding to a widespread telecommunications outage are company oriented. The President should direct the appropriate Federal departments and/or agencies to work with industry to improve inter-carrier coordination plans and procedures. To support this mechanism, communications capabilities are required between Government and the telecommunications industry to respond to and recover from a possible widespread outage affecting National Security Emergency Preparedness (NSEP) services.

—*Remove Legal and Regulatory Obstacles to Widespread Outage Recovery.*—It is not clear who has the authority to resolve legal and regulatory impediments to the rapid and orderly restoration of service during a widespread outage. The President should encourage the Federal Communications Commission (FCC) to maintain a Defense Commissioner at all times to help industry and Government overcome these impediments and to clarify the Defense Commissioner's authority to address NSEP telecommunications regulatory concerns. The President should also encourage the FCC to ensure Local Number Portability (LNP) national standards and requirements, including NSEP, are agreed on and adhered to before implementing LNP on a widespread basis. Sufficient time to complete reliability, interoperability, and security testing of new services and products should be allowed prior to implementing regulatory mandates.

—*Advance the State-of-the-Art for Software Integrity and Interoperability to Reduce the Probability of a Widespread Outage.*—All U.S. infrastructures, including the PN, continue to be increasingly reliant on software-controlled information systems. Security analysis of software products is not universally practiced by major equipment manufacturers. It is possible, because of the complexity of the large systems involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to protracted denial of service. The President should task the appropriate Federal departments and agencies to work with industry to advance the state-of-the-art for software integrity. The NSTAC should work to increase awareness within

the telecommunications industry of the importance of software security and the use of best business practices for managing complex automated systems.

—*Expand Research and Development (R&D) Efforts to Address Telecommunications Technology Vulnerabilities.*—The President should direct the expansion of government R&D efforts to address the most significant vulnerabilities of new and evolving telecommunications technologies and services. As a first step, existing R&D efforts should be examined and coordinated to determine any necessary increases. Industry should be urged to participate in these efforts. As a specific case, the President should encourage the FCC to examine and assist with the implementation of the Network Reliability and Interoperability Council (NRIC) recommendations as they relate to potential widespread outage vulnerabilities attributed to physical network design and new supporting technologies.

—*Foster Education and Awareness.*—The NSTAC, as part of its outreach efforts, should offer the NSIE model to the Network Interconnection/Interoperability Forum (NIIF) for consideration and potential use by network operations managers. The NSTAC should encourage the use of this model to help foster effective plans, procedures, and inter-carrier relationships in the increasingly competitive telecommunications environment.

1.0 INTRODUCTION

1.1 Background

In April 1997, Dr. John Gibbons, Assistant to the President for Science and Technology, wrote to Mr. Charles Lee, Chairman of the President's National Security Telecommunications Advisory Committee (NSTAC), seeking the NSTAC's forward-looking views on the possibility of a widespread, sustained interruption of the public telephone network. In response, the NSTAC's Network Group and Operations Support Group established the Widespread Outage Subgroup (WOS) to answer Dr. Gibbons' inquiry. This report provides NSTAC's views on the validity of this concern, considering the rapid changes foreseen in the industry structure, regulation, and technologies of the public telecommunications network and other critical infrastructures.

1.2 Scope

This report focuses on the current public telecommunications network and recognizes traditional threats and vulnerabilities, such as equipment malfunctions, natural hazards, sabotage, and physical design. It also addresses potential concerns as the network evolves through new technologies and regulatory mandates, as well as the growing threat from information system intrusions which could trigger systemic network failures.

The specific issues addressed are drawn directly from Dr. Gibbons' letter, including: (1) the likelihood of a widespread outage; (2) possible causes of outages; (3) coordination mechanisms required for recovery of network operations; and (4) the ability of service providers to keep the President apprised of recovery activities and status.

1.3 Widespread Outage Definition

A widespread outage is defined as a sustained interruption of telecommunications service that will have strategic significance to government, industry, and the general public. Such an outage would likely affect the telecommunications service in at least one region of the country including at least one major metropolitan area. It would involve multiple carriers, affecting both long distance and local service, and significantly degrade the ability of other essential infrastructures to function. Such an outage would have an impact on the availability and integrity of telecommunications service for at least a significant portion of a business day.

2.0 OBJECTIVE

This report answers the following questions:

—To what extent is a widespread, sustained interruption of public telephone service—because of common equipment, software, single point of failure, sabotage, or any other factor—a realistic concern?

—What plan does the industry have for inter-carrier coordination to facilitate recovery of the network from a widespread outage?

—Are existing communication and coordination mechanisms among service providers sufficient for the efficient diagnosis of the problem, identification of technical solutions, and restoration of service from an outage of this type?

—Are there legal or regulatory obstacles that would hinder recovery from such an outage?
—What interface between the telecommunications service providers and the Government would allow the President to be sure that restoration priorities meet the national interest? How would the service providers keep the President apprised of the progress of restoration efforts in the event of an outage affecting multiple companies?

In responding to Dr. Gibbons' questions, this report acknowledges both the current and future states of the public network (PN).[2] It further discusses the potential impact of new technologies and regulatory mandates on robustness and reliability.

3.0 FINDINGS

United States (U.S.) telecommunications service providers have historically offered unparalleled service robustness, availability, and quality. The June 1997 Network Reliability Steering Committee report acknowledged that the PN has maintained a 99.9 percent operational availability while the network has experienced significant growth and technological change. Although the PN's track record is superlative, known threats do adversely affect telecommunications service. Natural disasters such as earthquakes and hurricanes have disrupted elements of the PN, but overall the industry has been successful in mitigating the service impact. Outages in other critical infrastructures, such as electric power,[3] also stress the PN's reliability. While the PN's evolving technologies provide an expanding array of services and features and facilitate robustness, these same technologies can introduce vulnerabilities which, if exploited, could adversely affect service availability and reliability. The rapid implementation of changes to the network fostered by the Telecommunications Act of 1996 (e.g., Local Number Portability, interconnection, unbundling, infrastructure sharing, and collocation) have the potential to introduce further vulnerabilities into the PN. Considering these factors, it is prudent to consider the possibility of an unprecedented and widespread telecommunications outage.

3.1 To what extent is a widespread, sustained interruption of public telephone service—because of common equipment, software, single point of failure, sabotage, or any other factor—a realistic concern?

Given the limited precedent for telecommunications outages of this magnitude, NSTAC members' prior experiences with smaller-scale outages lead them to believe that there is a low probability of a widespread, sustained outage of service. However, the potential impact on society of such an outage is high enough to warrant consideration. As an example, the Common Channel Signaling (CCS) disruptions experienced in 1991[4] by some of the NSTAC member companies provided a strong impetus for subsequent improvements to network standards, software, and hardware.

Several additional examples of contributing factors are described in the following subsections.

3.1.1 Software

Within the modern PN, all of the nodes within each network, as well as those within interconnecting networks, are controlled by software furnished by the node equipment manufacturers or their vendors. This software, as with all computer software, is vulnerable to design flaws, implementation errors, and other problems that could cause it to fail or not function as desired, despite its designers' best efforts. Software patches are frequently released to add minor feature enhancements, as well as to correct previous errors. While testing is performed to ensure the software operates as designed and intended, it is not feasible to test for and against every conceivable network condition. Finding and mitigating software mistakes is often a

---

[2] "The PN includes any switching system or voice, data or video transmission system used to provide communications services to the public (e.g., public switched networks, public data networks, private line services, wireless systems, and signaling networks)" ANSIE Risk Assessment, December 1995.

[3] On July 2, 1996, a massive power blackout swept across the western United States. One telecommunications carrier reported that 87 of its 1,475 switches used backup generators or batteries to remain in service. Technicians were sent to switches where batteries were being used and in some cases secondary generators were sent to central offices where heat-caused battery exhaustion threatened to shut down the system. Switches on backup power served about 70,000 customers, yet the network remained "fully operational" throughout the power interruption.

[4] In June and July 1991, network outages occurred in several parts of the United States that were attributed to software errors in the control elements of the SS7 network. Network switching outages and call processing delays were experienced in Los Angeles, CA, San Francisco, CA, Pittsburgh, PA, and parts of Maryland, Virginia, West Virginia and the District of Columbia.

difficult and imperfect process. Detecting subtle but intentional and destructive software alterations could be much more problematic. Destructive code, if propagated through large portions of the PN (for example, in a commonly-used equipment node, database, or protocol), could cause widespread turmoil when activated.

Security analysis of software products, including patches, minor version updates, and full new releases, is not universally practiced by many manufacturers. Adequate tools to verify the anti-tampering integrity of the product are not widely used or, in some cases, may not be available. Most software testing is performed to ensure the program features interact and operate as intended. It is possible, because of the complexity of the large systems often involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to a protracted denial of service. For example, the urgent need to update software-dependent systems, nodes, and databases to accommodate Year 2000 or Local Number Portability (LNP) functionality could create an environment where software introduced into the network fabric may result in unintentionally anomalous network behavior.

3.1.2 SONET operations control

The incorporation of Synchronous Optical Network (SONET) as the transport medium of choice for trunks, data communications lines, asynchronous transfer mode (ATM) and common channel signaling (CCS) links (also known as Signaling System 7) makes it among the most crucial of PN components. Despite its importance to the health of SONETbased networks, SONET's address resolution functions support almost no security measures that could prevent an intruder from subverting it. An attack on the control protocols within portions of a SONET network could degrade operations, with a resulting loss of control of the SONET network elements and transport capabilities.

3.1.3 CCS (SS7) gateway screening

Public networks are dependent on CCS, a packet-switched data network employing Signaling System 7 (SS7) protocols, to set up and terminate calls as well as transmit advanced feature data such as Caller ID. A second application of SS7 is its use as a rapid transport network for fraud protection and billing authorization within wireless and wireline networks. Because of publicly-available detailed information about SS7 protocols, an adversary could potentially exploit the CCS packet data network by independently generating SS7 messages and injecting them into the PN signaling links.

SS7 is one of many network capabilities subject to unbundling and widespread interconnection as part of the regulatory scheme implementing the Telecommunications Act of 1996. In addition, a number of commercially-available devices and tools have SS7 message generation capabilities. The pro-competitive impetus to open SS7 networks up to traffic other than that generated by the service provider operating those networks, coupled with the proliferation of third parties who desire to access it, reflects the SS7 network's importance. Loss of, or damage to, the SS7 network almost inevitably precipitates a corresponding degradation or interruption of service to the PN. SS7 network and software security is therefore a requirement of substantial significance to reliability.

Gateway screening is one of a very limited set of SS7 security tools currently available to all network service providers and is implemented at the interface between service providers' networks. Presently, there is no industry-wide understanding of how gateway screening should be extended into the new competitive network environment. Without "standardized" screening, large quantities of malicious or erroneous messages could lead to a widespread degradation.

Many network subsystems, such as operations support systems (OSS), which are used by incumbent carriers for operations, maintenance and billing, were not designed for third-party access. This may be particularly problematic considering the number of potential new service providers that will need access to incumbent networks and subsystems, including the CCS network and OSSs. Many of these new providers are not familiar with security considerations and practices and could present risks to overall network reliability. There is currently no overall unified scrutiny of the interconnected CCS networks for real-time management and control to guard against intrusions and unauthorized users.

3.1.4 Physical design

The U.S. public networks have been designed to preclude single points of failure above the local switching level. This has been accomplished through substantial investments in both physical and logical diversity. As examples, signal transfer points (STP) of SS7 systems are commonly deployed in mated pairs that are physically and electronically redundant as well as geographically diverse. Long-haul transmission

links between switches are increasingly designed to be resilient and self-healing (e.g., SONET rings). Networks are utilizing dynamically-controlled routing, with non-hierarchical network architectures capable of routing traffic around damaged or congested portions of the network in real time. These factors, coupled with the diversity of carriers that exist in the United States, contribute to a high level of PN reliability and robustness. It is therefore highly unlikely that a single point network failure would result in a widespread outage of service. This conclusion is supported by the continuing success of carriers providing reliable service even while experiencing the impact of traditional threats such as natural disasters, cable cuts, and power failures.

Economic tradeoffs, enabled by technological advances, continue to cause some carriers to consolidate and collocate both facilities and network operations functions. While somewhat decreasing the physical diversity of the PN, it has enabled the rapid introduction of advanced network management technologies into consolidated control centers. It will be important for carriers, service providers and vendors to continue to employ "best practices" for reliability and security as new technologies are deployed, networks continue to expand, and new providers connect to the network.

3.1.5 Sabotage

The act of sabotage can take many different forms. Two primary forms of sabotage are damage (physical or electronic) or interference with normal operation. Both of these acts result in disruption of service. To cause a widespread outage, these disruptions would have to occur at a number of facilities, affect multiple carriers, and be successfully coordinated to have a significant and measurable impact. Sabotage can be instigated by either insiders (e.g., employees, contractors), outsiders (e.g., hackers, criminals, nation-states), or—more likely—both. Multiple acts of sabotage may use different attack methods and have different goals, which would increase the confusion and diminish service providers' ability to effectively restore network services. The massive coordination and long-range planning required to execute such an attack, while eluding law enforcement and intelligence agencies, coupled with the physical and logical diversity of the PN, implies a low probability of success.

In summary, the likelihood of a widespread, sustained outage of service resulting from sabotage is remote.

3.1.6 Introduction of new technologies or services

New technologies, by their nature, are often more complex and sometimes create unintended consequences and unexpected interactions among subsystems. Because new technologies cannot be tested for and against every conceivable set of events or network conditions, unforeseen vulnerabilities may be introduced into the network.

Rapid introduction of changes mandated by the Telecommunications Act of 1996 (e.g., Local Number Portability, seamless interconnection, unbundling, infrastructure sharing, and collocation) could potentially introduce unforeseen vulnerabilities into the PN. The Telecommunications Act requires existing carriers to allow new carriers to interconnect with existing networks "at any technically feasible point."[5] The lack of standards and interfaces to support multiple carrier use of OSS's increases the likelihood of potential conflicts and mistakes. Additionally, security and privacy concerns must be addressed as these standards and interfaces are developed. Conflicts and mistakes, or overt malicious actions, increase the probability of a significant outage. The Network Reliability and Interoperability Council's (NRIC) report to the FCC, published in July 1997, provides additional guidance and recommendations to be considered in developing such standards.

Increasing connectivity of OSS and PN control mechanisms to the Internet remains an item of NSTAC concern. As described in "An Assessment of the Risk to the Security of Public Networks" in December 1995:

> Connections to the Internet are increasing, and while many service providers have exercised due care in isolating critical network systems and components from more open-enterprise data networks and the Internet, there may still be potentially exploitable connectivity, such as through a restrictive router or firewall. An error in the design, configuration, or implementation of such a protective barrier could lead to compromise of critical systems from anywhere in the world."[6]

---

[5] Telecommunications Act of 1996 (47 U.S.C. Section 251c(2)(B)).

[6] "An Assessment of the Risk to the Security of Public Networks," Network Security Information Exchange (NSIE), December 1995.

Conversely, the Internet is highly dependent on PN-based switching and transport networks for long-haul transmission of traffic. A disruption or outage in the PN will likewise interfere with Internet traffic.

3.2 What plan does the industry have for inter-carrier coordination to facilitate recovery of the network from a widespread outage?

There are two categories of widespread outages. The first type is caused by the impact of traditional hazards, threats, and vulnerabilities. The other is characterized by a systemic and widespread network failure.

3.2.1 Traditional hazards, threats, and vulnerabilities

Existing carriers have disaster recovery plans and a proven track record of quickly recovering from traditional outages. Included in many of these recovery plans are bilateral and multilateral mutual aid agreements, designed to address multicarrier network problems. These agreements focus on resource sharing, such as supplies, portable equipment, motor vehicles, personnel, and may also dictate arrangements for temporary routing of traffic and services over another carrier's spare facilities. In addition to formal agreements, informal arrangements exist throughout the industry for inter-carrier and carrier-vendor communication and cooperation during emergencies. The vast majority of telecommunications disruptions that require a multi-carrier/vendor response effort are addressed through industry cooperation. Instead of precisely defining the scope of network sharing or resource lending arrangements, the industry approaches each incident with a customer-focused "can do" approach that has a long history of success. Informal arrangements offer additional flexibility in dealing with emergencies because each telecommunication outage situation is unique. These informal arrangements leverage relationships between network managers already established within the industry through day-to-day interaction and operations.

3.2.2 Systemic and widespread network failure

The industry has had limited experience with a systemic, widespread network outage. Currently, there is no industry-wide plan to facilitate inter-carrier coordination for recovering from a widespread outage of this nature. While an industry-wide plan has not yet been developed, companies have prepared internal plans and processes for maintaining the integrity of their own networks. These plans and processes include specifics for diagnosing problems, identifying solutions, and ensuring service can be restored as rapidly and orderly as possible.

3.3 Are existing communication and coordination mechanisms among service providers sufficient for the efficient diagnosis of the problem, identification of technical solutions, and restoration of service from an outage of this type?

Although some agreements, communication systems, and coordinating mechanisms do exist between and among carriers, it is questionable whether they would be a sufficient response to a severe widespread service outage. In the event of an outage affecting multiple carriers, individual carriers will first concentrate on restoring service in their own systems before reestablishing connections with other carriers. To assist in service restoration, most of the larger telecommunications companies have alternate communications capabilities between critical centers in their networks. These alternatives include private line networks, high frequency (HF) radio, and satellite telephone systems.

Reconnection with other networks would only be initiated after individual carriers are confident of the health of their own network and those to which they are connecting. It is during this phase that a means of communication and coordination between and among critical centers is indispensable. Several communications capabilities exist outside the PN for inter-carrier coordination of service restoration. The Backup Emergency Alerting Management System (BEAMS) is a switched private line network operated by the National Telecommunications Alliance (NTA) connecting selected telecommunications carriers, equipment and switch vendors, and the National Communications System (NCS). The National Telecommunications Coordinating Network (NTCN), a multimedia network administered by the NCS's National Coordinating Center for Telecommunications (NCC), provides emergency communications among critical Federal Government and industry operations centers. Although some of the major U.S. carriers are connected via BEAMS and/or NTCN, both networks would require expansion to meet an emerging need for inter-carrier coordination of restoration from a widespread telecommunications outage.

Several industry fora have taken strides to alleviate potential coordination problems in the event of a catastrophic outage. For example, the Network Interconnection/Interoperability Forum (NIIF) of the Alliance for Telecommunications Industry Solutions (ATIS) developed emergency traffic management guidelines for network

management personnel at local and interexchange carriers. The guidelines provide alternatives for dealing with network emergencies, including network congestion, switch or network failures, and SS7 failures. In addition, the NIIF maintains contact directories for use in emergencies. These directories are targeted toward incident type and include contact and reporting numbers for network management centers, for use in the event of catastrophic SS7 failures, media simulated mass calling events, and other service troubles. The NIIF and other committees within ATIS address industry-wide issues concerning telecommunications interconnection and interoperability, network reliability analyses, and implementation and deployment of new technologies, including Synchronous Optical Network (SONET) and Advanced Intelligent Network (AIN) services.

A successful coordinating mechanism requires a high level of mutual trust and information sharing. An example of such a mechanism is the Network Security Information Exchange (NSIE),[7] whose goal is to share information and experiences among telecommunications network security managers. The NSIE has established trusted relationships among and between the government and industry members. Trust among industry and government participants facilitates responses to routine and emergency security incidents.

Much of the telecommunications industry's success in recovering from outages is attributed to long-standing inter-carrier relationships existing among incumbent network managers that arise from day-to-day interaction and operations. In the increasingly competitive telecommunications market, this level of cooperation and trust may be difficult to sustain. Although not a perfect model, the NSIE example could be offered to industry network operations managers. Through the auspices of the NIIF, industry might benefit from an NSIE-like body to share their inter-carrier operations concerns in the increasingly diverse and competitive environment.

3.4 Are there legal or regulatory obstacles that would hinder recovery from such an outage?

NSTAC members have identified several legal and regulatory barriers to the rapid and orderly restoration of service during a widespread outage. For example, the ability of a local exchange carrier to provide emergency inter-Local Access Transport Area (LATA) communications to state or Federal agencies may prove to be critical to their ability to protect the interests of public safety and national security.[8] In addition, it may also be necessary for a carrier to utilize the resources of its affiliates to make necessary physical repairs to the network that could be perceived to involve manufacturing of telecommunications hardware.[9] Finally, domestic carriers may often need to call on the assistance of international carriers to recover from a significant outage. While many companies are not prohibited from providing in-region inter-LATA and manufacturing services, Sections 271 and 273 of the Telecommunications Act require that Regional Bell Operating Companies (RBOC) satisfy a number of requirements and receive Federal Communications Commission (FCC) approval to offer these services. No RBOC currently has approval to perform these services, and until such approval is requested and obtained, this obstacle remains and could potentially hinder recovery from a future widespread outage. Additionally,

---

[7] The Network Security Information Exchange (NSIE) is a forum for industry and Government members to share and coordinate information security knowledge that will assist in preventing, detecting, and/or investigating public network penetrations. The NSIE identifies issues involving penetration or manipulation of software and databases affecting NSEP telecommunications, and exchanges views on threats, incidents, and vulnerabilities affecting the PN. The current NSIE membership includes 9 Government organizations from the law enforcement, national defense, and intelligence communities, and 19 NSTAC member companies representing the telecommunications, information systems, and financial industries.

[8] In 1991, BellSouth experienced a 1-year delay in receiving a Modification of Final Judgment (MFJ) exception. Hurricane Hugo caused disruption to the State of South Carolinas private line network. As a result, the BellSouth Corporation asked the Department of Justice (DOJ) to support a petition seeking an exemption from part of the MFJ in order to provide emergency inter-LATA communications for the State of South Carolina. After a year delay, and following an extensive public comment and review period, the DOJ endorsed the petition.

For reference, a copy of the request, dated 18 March, 1991, from Mr. Ted Lightle, Director, Division of Information Resource Management, State of South Carolina, to Ms. Constance K. Robinson, Esq., Acting Chief, Communications and Finance Section, Antitrust Division, U.S. DOJ, is attached in Appendix C.

[9] In 1991, Bell Atlantic Corporation requested Bellcore's assistance to restore part of the PSN serving the mid-Atlantic region, including Washington D.C. and the Federal Aviation Administration's air traffic control system at Newark International Airport. As a Regional Bell Operating Company (RBOC) affiliate, however, Bellcore was concerned that physical repairs made to the network might be viewed as "manufacturing" and thus violate the then existing MFJ provisions prohibiting the manufacturing of telecommunications equipment by the RBOC's or their affiliates.

other regulatory safeguards imposed on other companies and RBOCs alike could likewise affect the ability of carriers to fully use their corporate resources to respond effectively to a widespread outage (e.g., restrictions imposed on the financial, marketing, and operational interactions of dominant and non-dominant carriers, and FCC requirements for carriers to keep their regulated and unregulated businesses completely separated).

The Telecommunications Act of 1996 transfers many telecommunications policy enforcement responsibilities from a single Federal judicial official to the FCC and, to a lesser extent, the Department of Justice (DOJ). This transfer of authority raises questions about the appropriate official(s) or organization(s) telecommunications companies should approach for swift and consistent guidance in an emergency. It also is unclear whether the FCC has the authority to grant temporary waivers of applicable sections of the Telecommunications Act during a widespread outage recovery effort, even when the waiver is in the public interest. Currently, existing regulations regarding the National Security and Emergency Preparedness (NS/EP) responsibilities of various Federal officials and organizations, as described below, do not place a single Federal official in charge of deciding whether to enforce or waive compliance with applicable laws or regulations.

3.4.1 Federal Communications Commission

Executive Order (E.O.) 12472 requires the FCC to perform functions during national non-wartime emergencies, including the investigation of violations of pertinent law and regulations and the initiation of appropriate enforcement actions.[10] The FCC's rules accordingly assign the FCC Defense Commissioner the specific duties of assuring continuity of the Commission's NS/EP functions and of approving NS/EP plans and programs (including the provision of service by common carriers and the investigation and enforcement of violations of Federal law).[11] These regulations task the Defense Commissioner to uphold carriers' compliance with applicable law. The rules are unclear, however, as to whether they extend to the Defense Commissioner or the entire Commission (with or without consultation with the DOJ) the power to forbear from enforcing relevant provisions of the Telecommunications Act during a crisis. Even if the rules did place one official in charge, that one Commissioner may not have the authority to override the Telecommunications Act (i.e., permit something that is specifically prohibited or precluded by the Act) in an emergency such as a widespread outage.

3.4.2 The President

Section 706(e) of the Communications Act of 1934, as amended, empowers the President to suspend or amend, during a national emergency, FCC rules applicable to any wire communications facilities. Section 706(g), however, prohibits the President from making any amendment to the FCC's rules that the agency would not itself be authorized by law to make.[12] Because it is questionable whether the FCC Defense Commissioner or the entire Commission by itself could grant to service providers waivers from complying with relevant portions of the Telecommunications Act, it follows that the President's power to do so is also questionable.

3.4.3 The National Security Council (NSC) and Office of Science and Technology Policy (OSTP)

Section 2(c)(1)(a) of E.O. 12472 instructs the NSC to coordinate the development of policy, plans, programs, and standards within the Federal Government for the use of the Nation's telecommunications resources during non-wartime conditions. Section 2(b)(2) charges the Director, OSTP, to provide appropriate guidance and assistance to the President and other Federal organizations responsible for the provision, management, or allocation of telecommunications resources during such conditions. Section 2(b)(3) further assigns the Director, OSTP, with establishing and chairing a Joint Telecommunications Resources Board (JTRB) to assist the Director in exercising non-wartime telecommunications functions.[13] Although the NSC and

---

[10] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984.

[11] Federal Communications Commission rules, "Defense and Emergency Preparedness Functions," 47 C.F.R. 0.181–0.186.

[12] Section 706 of the Communications Act of 1934 (47 U.S.C. 606), "War Emergency—Powers of President."

[13] Executive Order 12472, "Assignment of National Security and Emergency Preparedness Telecommunications Functions," April 3, 1984. The JTRB's membership consists of the Assistant Secretary of Defense, Command, Control, Communications, and Intelligence; the Assistant Secretary, Communications and Information, of the Department of Commerce; the Commissioner, Federal Telecommunications Service, of the General Services Administration; the Associate Di-

the JTRB might help craft future policy initiatives to address the industry's legal concerns prior to the occurrence of a widespread outage, it is unclear whether either group would play a significant role during an actual recovery effort.

3.5 What interface between the telecommunications service providers and the Government would allow the President to be sure that restoration priorities meet the national interest? How would the service providers keep the President apprised of the progress of restoration efforts in the event of an outage affecting multiple companies?

For many years, the telecommunications industry has provided the NCC with relevant information pertaining to major outages. More recently it has also provided the FCC with reports of outages that conform to the FCC's specific requirements. Because the NCC's mission is to monitor NSEP telecommunications, and experience has shown that industry willingly provides relevant outage information to the NCC, then the NCC is positioned to collect widespread outage information for the President. To support this function, the Office of the Manager, National Communications System (OMNCS), has a video teleconferencing system that is used to communicate directly with the Executive Office of the President. The NCC Vision Subgroup is addressing the issue of sharing intrusion and network outage information among industry and government.

4.0 CONCLUSIONS/RECOMMENDATIONS

While the PN is robust and highly reliable, it is also built on a complex, interconnected set of heterogeneous technology platforms. The PN can be disrupted by natural calamities, electric power outages, or assaulted by hostile forces. In addition, rapid legislative, regulatory and market changes could potentially introduce unforeseen vulnerability into the PN. Although the probability of a widespread sustained outage is low, the high potential societal cost of such an outage requires that the concern be addressed. Industry and government can take cost-effective measures to reduce the overall risk of a widespread outage and enable an orderly restoration of service if such an outage occurs.

Other Industry Executive Subcommittee groups, including the Intrusion Detection Subgroup, Information Infrastructure Group, Legislative and Regulatory Group, and the NCC Vision Subgroup, are examining several of the issues addressed in this report that would improve the overall ability of the United States to respond to a widespread telecommunications outage. We recommend that their conclusions be examined in light of our findings.

Pursuant to the concerns expressed in Dr. Gibbons' letter, the Widespread Outage Subgroup offers the following recommendations:

4.1 Recommendations

4.1.1 Improve inter-carrier coordination for widespread outage recovery

Current industry plans and coordination procedures for responding to a widespread telecommunications outage are company-oriented. Inter-carrier coordination plans and procedures for responding to a widespread telecommunications outage require upgrading to meet new and emerging threats.

The President should direct the appropriate Federal departments and/or agencies to:

—Cooperate with industry to build a mechanism to upgrade current industry:
  —Recovery plans
  —Coordinating mechanisms, and
  —Emergency communications capabilities.

—Ensure adequate communications capabilities are available between Government and the telecommunications industry, as well as with other critical infrastructures, to respond to and recover from a possible widespread outage affecting NS/EP services.

4.1.2 Remove legal and regulatory obstacles to widespread outage recovery

There are potential legal and regulatory impediments to the rapid and orderly restoration of service during a widespread outage. It is not clear who has the authority to resolve these impediments. The relative specificity of the rules governing the FCC Defense Commissioner's responsibilities suggests that this individual could help industry and Government overcome these impediments.

The President should encourage the FCC to:

---

rector, Operations Support, of the Federal Emergency Management Agency; the Defense Commissioner of the FCC; and the Manager, NCS.

—Appoint and maintain a Defense Commissioner
—Clarify the Defense Commissioner's authority to:
—Address NSEP telecommunications regulatory concerns in Commission activities, rulemaking, and particularly during emergency situations.
—Establish a process for the expeditious resolution of NSEP issues and other impediments affecting industry recovery from a widespread telecommunications service outage.

Competitive market and legislative mandates often create a rush to introduce new products and services before they are fully evaluated in the laboratory and under live network conditions (e.g., Local Number Portability [LNP]). Before schedules are mandated through FCC regulations, reliability, interoperability, and security concerns need to be carefully considered to guard against premature implementation of "unseasoned" technologies that may contribute to the possibility of a widespread outage. An additional concern is the impact of industry restructuring on NSEP communications, especially considering the entry of new carriers under the Telecommunications Act.

The President should also encourage the FCC to:
—Minimize the possibility of a widespread outage by ensuring LNP national standards and requirements, including NSEP, are agreed on and adhered to before implementing LNP on a widespread basis
—Allow sufficient time to complete reliability, interoperability, and security testing of new services and products prior to implementing regulatory mandates.

4.1.3 Advance the state-of-the-art for software integrity and interoperability to reduce the probability of a widespread outage

All U.S. infrastructures, including the PN, continue to be increasingly reliant on software-controlled information systems. Security analysis of software products is not universally practiced by major equipment manufacturers. It is possible, because of the complexity of the large systems involved, that hidden, malicious code or unintentional code interactions could allow unauthorized access to network systems or lead to protracted denial of service.

The President should:
—Task the appropriate Federal departments and agencies to work with industry to lead the advance of the state-of-the-art for software integrity through intense research, development, and operational investigations.

The NSTAC should:
—Increase awareness within the telecommunications industry of the importance of software security and the use of best business practices for managing complex automated systems.

4.1.4 Expand research and development (R&D) efforts to address telecommunications technology vulnerabilities

New technologies, by their nature, often are more complex, sometimes resulting in unintended consequences and unexpected interactions among subsystems. Because new technologies cannot be tested for and against every conceivable set of events or network conditions, unforeseen vulnerabilities may be introduced into the network.

The President should:
—Direct the expansion of government R&D efforts to address the resolution of the most significant vulnerabilities of new and evolving telecommunications technologies and services. As a first step, identify or coordinate more closely existing R&D efforts in order to determine any necessary increases.
—Encourage industry to assist in these efforts.
—Encourage the FCC to examine and assist with the implementation of the Network Reliability and Interoperability Council (NRIC) recommendations as they relate to potential widespread outage vulnerabilities attributed to physical network design, and new supporting technologies.

4.1.5 Foster education and awareness

Trust among telecommunications network managers facilitates the effective response to routine and emergency network incidents. Much of the telecommunications industry's success in recovering from outages is attributed to long-standing inter-carrier relationships among network managers arising from day-to-day interaction and operations. Achieving and maintaining this level of trust becomes more difficult in an increasingly competitive environment.

The NSTAC should, as part of its outreach efforts:
—Offer the NSIE model to the Network Interconnection/Interoperability Forum (NIIF) for consideration and potential use by network operations managers.

—Encourage the use of this model to help foster effective plans, procedures and inter-carrier relationships in the increasingly competitive telecommunications environment.

ANNEX A.—REFERENCES

—"Potential Legal and Regulatory Obstacles to Widespread Outage Recovery," Draft Report of the Legislative and Regulatory Group (LRG) of The President's National Security Telecommunications Advisory Committee (NSTAC), September 30, 1997.
—"Network Interoperability: The Key to Competition," Network Reliability and Interoperability Council (NRIC) of the Federal Communications Commission (FCC), July 1997.
—"Electric Power Information Assurance Risk Assessment Report," Information Assurance Task Force (IATF) of The President's NSTAC, March 1997.
—"Analysis of Power Related Network Outages," Alliance for Telecommunications Industry Solutions, Network Reliability Steering Committee, August 29, 1996.
—"An Assessment of the Risk to the Security of Public Networks," Network Security Information Exchange (NSIE), December 1995.
—"Final Report of the Common Channel Signaling Task Force," The President's NSTAC, January 1994.
—"Network Reliability: A Report to the Nation," Network Reliability Council of the FCC, June 1993.
—FCC Common Carrier Bureau Report on Network Outages, July 1991.
—"Growing Vulnerability of the Public Switched Networks," National Research Council, 1989.

ANNEX B.—ACRONYMS

AIN	= Advanced Intelligent Network
ATIS	= Alliance for Telecommunications Industry Solutions
BEAMS	= Backup Emergency Alerting Management System
CCS	= Common Channel Signaling
DOJ	= Department of Justice
EO	= Executive Order
HF	= High Frequency
JTRB	= Joint Telecommunications Resources Board
LATA	= Local Access Transport Area
LNP	= Local Number Portability
NCC	= National Coordinating Center for Telecommunications
NCS	= National Communications System
NIIF	= National Interconnection/Interoperability Forum
NRIC	= Network Reliability and Interoperability Council
NSEP	= National Security Emergency Preparedness
NSIE	= Network Security Information Exchange
NSTAC	= President's National Security Telecommunications Advisory Committee
NTA	= National Telecommunications Alliance
NTCN	= National Telecommunications Coordinating Network
OMNCS	= Office of the Manager, National Communications System
OSS	= Operations Support System
OSTP	= Office of Science and Technology Policy
PN	= Public Network
R&D	= Research and Development
SONET	= Synchronous Optical Network
SS7	= Signaling System 7
STP	= Signal Transfer Point
U.S.	= United States
WOS	= Widespread Outage Subgroup

ANNEX C.—WIDESPREAD OUTAGE SUBGROUP MEMBERS

NTA—Mr. Bob burns, Chair
AT&T— Mr. Dave Bush
Bellcore—Mr. Carl Ripa
GTE—Ms. Ernie Gormsen
MCI—Mr. Mike McPadden

OMNCS—Mr. Bernie Farrell
SAIC—Mr. Hank Kluepfel
USTA—Dr. Vern Junkmann
US West—Mr. Jon Lofstedt

ANNEX D.—LETTERS

(1) April 24, 1997, letter from Dr. John H. Gibbons, Assistant to the President for Science and Technology, to Mr. Charles R. Lee, Chairman, National Security Telecommunications Advisory Committee (NSTAC), Chairman and Chief Executive Officer, GTE Corporation.
(2) March 18, 1991, letter from Mr. Ted L. Lightle, Director, Division of Information Resource Management, State of South Carolina, to Ms. Constance K. Robinson, Esq., Chief, Communications and Finance Section, Antitrust Division, U.S. Department of Justice.
(3) August 24, 1992, letter from Mr. Richard L. Rosen, Esq., Acting Chief, Communications and Finance Section, Antitrust Division, U.S. Department of Justice, to Mr. Michael J. Schwartz, Esq., General Attorney, BellSouth Corporation.

RESPONSES OF JACK EDWARDS TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. One of the recommendations of the NSTAC report was that the legal and regulatory obstacles to widespread outage recovery be removed. For example, in an emergency could a regional Bell Operating Company be permitted to provide temporary long distance service? Has the NSTAC seen any actions taken on these recommendations?

Answer. Since the President's National Security Telecommunications Advisory Committee (NSTAC) issued its Widespread Outage Subgroup (WOS) Report in December 1997 at NSTAC XX, two of its recommendations have been acted upon. The recommendations are as follows:

IMPROVE INTER-CARRIER COORDINATION FOR WIDESPREAD RECOVERY

—The National Coordinating Center for Telecommunications (NCC) has initiated an effort to expand the National Telecommunications Coordinating Network (NTCN) to improve communications capabilities with critical entities, for both Government and industry, during network outage conditions.

REMOVE LEGAL AND REGULATORY OBSTACLES TO WIDESPREAD OUTAGE RECOVERY

—The Federal Communications Commission (FCC) appointed a FCC Defense Commissioner.
—The NSTAC Legislative and Regulatory Group (LRG) and the FCC have worked together to establish a procedure to resolve regulatory issues with the FCC, on an expedited basis, which will minimize delays in the provision and restoration of emergency telecommunications services during major service disruptions. This procedure is intended for use during and outside of normal business hours. NSTAC and the FCC approved the new procedure in August 1998.

Question 2. Will NSTAC continue to examine the national security implications of Y2K on telecommunications?

Answer. The Network Group will continue to monitor the Year 2000 (Y2K) readiness of the telecommunications infrastructure as test results become available and provide its insight on the matter, through the NSTAC, to the President.

Question 3. Could you please describe the role of the National Telecommunications Alliance in emergency preparedness?

Answer. The National Telecommunications Alliance (NTA), incorporated by the Regional Bell Operating Companies (RBOCs) in December 1995, serves as an industry consortium supporting the reliability and security of its clients' networks, and the interoperability and interconnectivity of their networks with other networks. In support of this critical mission, NTA's CEO serves on the President's NSTAC.

In 1997, NTA became the NS/EP single point of contact between the federal government and its clients. NTA operates the National Emergency Control Center (NECC) from its Washington, D.C. headquarters, as well as a National Emergency Relocation Center (NERC) outside of Washington, D.C., which has the same capabilities as the NECC.

During any crisis affecting an NTA client, all information is channeled through the NECC, which keep the Government, NTA clients' operation centers and staffs, and other affected parties informed. In addition, NTA operates the Alerting and Coordination Network (ACN), a dedicated telecommunications system separate from the public switched telephone system that is operated from the NECC and NERC. All NTA clients have links from their own Emergency Control Centers and Emer-

gency Relocation Centers directly into the ACN. Also, the ACN provides direct connectivity to Government agencies, other telephone companies, and telecommunications equipment manufacturers.

The source for the information on NTA can be found at http://www.nta-inc.org.

PREPARED STATEMENT OF DIANE FOUNTAINE

Good morning, Mr. Chairman, and distinguished members of the Special Committee on the Year 2000 Technology Problem. I appreciate the opportunity to address you on behalf of the National Communications System's Executive Agent, Defense Secretary William S. Cohen, and its Manager, Lieutenant General David J. Kelley, on the crucial role and initiatives that the National Communications System is taking toward tackling the Year 2000 as it applies to national security and emergency preparedness telecommunications.

The National Communications System is a confederation of 23 agencies across the Federal Government (listed in attachment 1) tasked with ensuring the availability of a viable national security and emergency preparedness telecommunications infrastructure. The President designates member organizations that own or lease telecommunications facilities and services of significant value to national security and emergency response or that have important telecommunications policy, regulatory, or enforcement responsibilities. The assets of these 23 organizations comprise the bulk of the Federal Government's telecommunications resources. National security/emergency preparedness telecommunications, in general, are considered to be the necessary communications for the Federal Government under all conditions, ranging from peacetime to national emergencies to international crises or war.

The Manager, National Communications System, is also the designated Federal Official for the National Security Telecommunications Advisory Committee. Established in 1982 by President Ronald Reagan in anticipation of the divestiture of AT&T, the National Security Telecommunications Advisory Committee is a high-level industry advisory group that provides the President with a unique source of national security and emergency preparedness telecommunications policy expertise and advice. Membership in the National Security Telecommunications Advisory Committee is limited to 30 Presidentially appointed industry leaders who are senior executives (often chief executive officers) representing major telecommunications carriers, information system providers, manufacturers, electronics and aerospace firms, system integrators, and the financial services industry. (The National Security Telecommunications Advisory Committee's membership is listed in attachment 2.)

I will specifically address implications of the Year 2000 problem on national security/emergency preparedness telecommunications issues and the role of the National Communications System in ensuring these telecommunications remain fully operational. I will also address the Office of the Manager, National Communications System views of the nation's telecommunications industry preparedness for Year 2000 as it relates to national security/emergency preparedness.

Mr. Chairman, the Office of the Manager, National Communications System, shares in the concerns expressed by this committee relating to Year 2000 compliance. in addressing the Year 2000 issue, we are focusing on three primary areas: First, on the national security/emergency preparedness capabilities that we contract with the interexchange and local exchange carriers to develop and maintain in the commercial public networks (e.g., priority call recognition and handling); second, on the overall voice services in the public network which are the primary foundation for our national security/emergency preparedness communications; last, on the contingency plans that we follow during a national security or emergency event. We have taken the following actions in each of these areas.

UNIQUE NATIONAL SECURITY/EMERGENCY PREPAREDNESS NETWORK FEATURES & CAPABILITIES

In conjunction with our primary contracting offices within the Defense Information Systems Agency and the Defense Information Technical Contracting Organization, my office is requesting from its contractors verification that services or systems being provided to the National Communications System are year 2000 compliant.

National security/emergency preparedness telecommunications services provided by the Government Emergency Telecommunications Service, the Telecommunications Service Priority Program, and the Emergency Response Link are required to be Year 2000 compliant as a result of modifications to the associated contracts. (more detailed descriptions of these programs are contained in attachment 3.)

Additionally, all new or replacement contracts for National Communications System-provided national security and emergency preparedness telecommunications services contain Year 2000 compliance requirements consistent with Department of Defense policy.

Where possible, we will test the national security/emergency preparedness features for Year 2000 compliance, to include practical demonstrations, in addition to written certification by our telecommunications service providers. We plan to complete these tests before January 1, 1999.

Testing for the Telecommunications Service Priority has been completed with minor problems discovered which are being corrected. Testing for the Emergency Response Link is slated for completion in September.

In order to achieve Government Emergency Telecommunications Service internetwork interoperability testing, we are collaborating with the Alliance for Telecommunications Industry Solutions. The Alliance for Telecommunications Industry Solutions is establishing a test network that will emulate major portions of the public switched network. The Government Emergency Telecommunications Service testing requirements were outlined at the last meeting of the Alliance for Telecommunications Industry Solutions Network Testing Committee held from June 29 and 30, 1998. The network testing committee accepted the potential scenario for Government Emergency Telecommunications Service testing and requested further details, to include a draft test script and an implementation summary, that will be presented at the next meeting from August 24–25, 1998. Bellcore is assisting the Office of the Manager, National Communications System in this effort, and this testing will be completed in March 1999.

Specific testing will include the ability to recognize the Government Emergency Telecommunications Service 710 area code and successfully complete Government Emergency Telecommunications Service calls end-to-end over local and interexchange carrier networks. While the scope of this Government Emergency Telecommunications Service testing is limited, the benefits of the Alliance for Telecommunications Industry Solutions internetwork testing among several major carriers in the U.S. Telecommunications Network are substantial.

ASSESSMENT OF BASIC NETWORK SERVICE

The Manager, National Communications System, requested that the National Security Telecommunications Advisory Committee focus on the Year 2000 issue as it relates specifically to national security/emergency preparedness and the national telecommunications infrastructure. The National Security Telecommunications Advisory Committee's network group has completed its initial assessment of this subject, and you will hear from Dr. Jack Edwards of Nortel, the network group's chair. This report will be reviewed by the National Security Telecommunications Advisory Committee principals at their upcoming meeting on September 10.

In implementing special national security/emergency preparedness capabilities in the public network we chose the major interexchange service providers, i.e., AT&T, MCI, Sprint, and the primary local exchange companies (e.g., Bell Atlantic, Cincinnati Bell, etc).

Based on information gathered by the National Security Telecommunications Advisory Committee working group and discussions with individual companies, we believe that there will be little or no interruption of service from these major service providers due to Year 2000. While they will have conducted extensive network element testing and intranetwork interoperability testing, the biggest challenge for all of these companies will be the testing of their network's external interfaces, both domestic and international. Ensuring the interoperability of these various solutions is critical, particularly in a system as complex as the U.S. telecommunications infrastructure, and this is why the Alliance for Telecommunications Industry Solutions internetwork testing is so important.

The Office of the Manager, National Communications System is also coordinating on the Year 2000 Telecommunications Compliance Program of the General Services Administration. This program was established to provide a focal point for Year 2000 telecommunications compliance information across the Federal Government and to facilitate government/industry partnership in addressing Year 2000 compliance challenges. We are participating in periodic forums being held by the Program Management Office and facilitate their interaction with the National Security Telecommunications Advisory Committee.

While I have only focused on those large telecommunications providers on which we depend, I believe that Commissioner Powell will address the state of preparedness of the industry in the broader context of all companies and services.

CONTINGENCY PLANS

Even though we do not expect a major telecommunications service interruption resulting from Year 2000, we are putting a great deal of emphasis on proper planning for a contingency in this area. The National Coordinating Center for Telecommunications is reviewing current operational response procedures and the existing national telecommunications coordinating network, looking for additions to current process or backup connectivity peculiar to Year 2000 (for example, connections to software experts from the telecommunications switch manufacturers.)

In addition to its current HF radio capabilities, the National Telecommunications Coordinating Network is being augmented with non-public network and satellite communications connectivity among critical national security/emergency preparedness operational sites, major service providers, and equipment manufacturers. This additional connectivity will allow the national coordinating center for telecommunications to coordinate with the telecommunications industry and key Federal operations centers in the event of service disruption resulting from Year 2000 complications.

HF radio connectivity is currently available to AT&T, Sprint, The National Telecommunications Alliance, The Federal Communications Commission, Bell Atlantic, The National Aeronautics and Space Administration, GTE, Bell South, AmeriTech, Southwestern Bell, The Federal Emergency Management Agency, AT&T Wireless, and Pacific Bell. Through the shared resources high frequency radio program these sites have HF message relaying support from over 1,000 government and telecommunications company HF locations worldwide.

Currently, the National Coordinating Center for Telecommunications has private line national telecommunications coordinating network connectivity to the FCC; all of the regional Bell operating companies; GTE; Sprint; and switch manufacturers, DSC, Ericsson, Lucent, Nortel, and Siemens. The National Coordinating Center for Telecommunications is exploring extending connectivity to the general service administration's FTS–2000 Consolidated Operations Center, The Office of Science and Technology Policy, The National Infrastructure protection center, and The Bellcore Year 2000 Test Bed Site. The National Coordinating Center for Telecommunications Industry members are also compiling point of contact lists that will be utilized for Year 2000 problem referral and escalation within their companies.

An additional, state of the art capability to cross-connect various communications media will be available in the National Coordinating Center for Telecommunications by the end of December 1998. This capability will extend to our continuity of operations site in the event relocation out of the immediate area becomes necessary.

In conclusion, Mr. Chairman, we are working with The National Communications System departments and agencies, and The National Security Telecommunications Advisory Committee member companies, to provide continuous national security/emergency preparedness telecommunications services prior to, through, and beyond the millennium change. While much has been accomplished, there is still much to be done, particularly regarding internetwork Year 2000 testing and contingency planning. As the National Security Telecommunications Advisory Committee Year 2000 report points out, efforts to make the public network Year 2000 ready will go a long way toward making national security/emergency preparedness telecommunications services year 2000 ready. I would urge the committee to support the efforts underway in the telecommunications industry and continue to stress the importance of internetwork interoperability testing as this work progresses.

Mr. Chairman, this concludes my statement on our efforts toward solving the Year 2000 problem, and I am prepared to take your questions on this issue.

ATTACHMENT 1.—NATIONAL COMMUNICATIONS SYSTEM MEMBER AGENCIES AND DEPARTMENTS

Department of State
Department of Treasury
Department of Defense
Department of Justice
Department of Interior
U.S. Department of Agriculture
Department of Commerce
Health and Human Services
Department of Transportation
Department of Energy
Veterans Affairs
Central Intelligence Agency
Federal Emergency Management Agency
U.S. Information Agency
Joint Staff
General Services Administration
National Aeronautics and Space Administration
Nuclear Regulatory Commission
National Telecommunications and Information Agency

National Security Agency
U.S. Postal Service
Federal Reserve Board
Federal Communications Commission

ATTACHMENT 2.—NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE MEMBERS

Advanced Digital Technologies Company (ADTC)
AT&T
BankAmerica
Boeing
Comsat
Computer Sciences Corporation
Electronic Data Systems
Executive Security & Engineering Technologies
GTE
Hughes
ITT
Lockheed Martin
MCI
Motorola
Nortel
National Telecommunications Alliance
Pacific Telecom, Inc.
Raytheon
Rockwell
Science Applications International Corporation
Sprint
Teledesic
TRW
Unisys
United States Telephone Association
U.S. West
Worldcom

ATTACHMENT 3.—PROGRAM DESCRIPTIONS

Government Emergency Telecommunications Service supports national security/emergency preparedness telecommunications users with priority switched voice and voice band data service in the public switched network. it provides authenticated access, enhanced routing, and priority treatment in local and long-distance telephone networks. users acquire access through a simple dialing plan featuring a dedicated area code (710) and personal identification number.

Telecommunications Service Priority System enables priority provisioning and restoration of national security/emergency preparedness telecommunications services obtained from the telecommunications industry companies.

Telecommunications Electric Service Priority Program promotes modification of the existing electric utility emergency priority restoration systems to include telecommunications facilities considered critical to national security/emergency preparedness. it utilizes the existing processes in place for restoring electric service to specific customers in the event of threatened or actual electric power supply emergencies.

Emergency Response Link provides a controlled access web site designed to assist the emergency response community in sharing disaster response planning and operations information. the response community includes the signatory agencies to the federal response plan and state and local agencies and organizations.

Shared Resources High Frequency Radio Program provides emergency communications in support of special operations and all-hazards situations, incorporating the resources of 1098 HF radio stations, contributed by 63 Federal, State, and industry organizations, into a nationwide emergency message handling network.

RESPONSES OF MS. DIANE FOUNTAINE TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Bellcore suggested that because of the size and complexity Y2K problems in the telecommunications industry, it is absolutely critical that contingency planning and disaster recovery planning and training be implemented. They also stated that multiple carrier failures should be entertained. How is the NCS working with industry on these issues?

Answer. In collaboration with its industry representatives the National Coordinating Center (NCC) for Telecommunications is working to insure that national security and emergency preparedness telecommunications contingency planning fully addresses year 2000 problems, to include:

—Formulation of a joint government/industry Y2K-specific Contingency Plan to be completed by April 1999.
—Verification of non-public switched network (PSN) connectivity to major operations centers from the NCC.
—Identification of those operation centers (industry & government) which have connectivity via non-PSN voice and/or data connectivity to vendors, suppliers,

subject matter experts, etc. that might play a key restoral role in any Y2K-related telecommunications outage.

—Identification of key Y2K-related facilities, elements, vendors, suppliers, subject matter experts with which the NCC does not currently have non-PSN connectivity that should be provided connectivity to the NCC.

The NCC is also currently fielding an upgraded National Telecommunications Coordinating Network (NTCN) which will allow the NCC to bridge any type of communications terminating on the NTCN to any other subscriber regardless of communications vehicle. This includes connecting any combination of HF, UHF, and VHF radios, private lines, ring downs, satellite, and wireless to any of the other media. The bridge is Y2K compliant, and will have a backup with redundant capabilities located at the NCS Continuity of Operations site.

Question 2. Could you please describe how the National Coordinating Center for Telecommunications works in a time of crisis?

Answer. The National Coordinating Center for Telecommunications (NCC) has three Emergency Operations Teams (EOT) manned with experts in various emergency response disciplines from the Office of the Manager, NCS staff, and industry representatives of the NCC. The Manager, NCC activates the on-call team to support a declaration of the Federal Response Plan or if required by other emergency. The three teams allow for ramping up to 7 days a week, 24-hour a day operation, if the situation warrants that level of support. A team will be activated prior to each critical year 2000 switch over date.

Question 3. How would the NCS and the FCC interact in the event a Y2K telecommunications crisis?

Answer. The FCC has a representative assigned as a member of the NCC. Operational issues would be coordinated with that representative. The NCC or the FCC representative can also contact the FCC Duty Officer at the FCC's Communications and Crises Management Center, which operates on a 24-hour, 7 days a week basis. The Duty Officer is responsible for locating senior FCC staff to apprise them of status of ongoing events, or to get an action officer to assist the NCC in addressing FCC-related issues. The FCC Center is connected to the NCC through the National Telecommunications Coordinating Network (NTCN) and the NTCN has connectivity to the FCC regional representatives through connections to each of the Federal Emergency Management Agency regional offices.

Question 4. When does a network outage advance from an economic concern to a national security concern?

Answer. Determination that a telecommunications public network failure impacting the economy has reached a national security concern would ultimately be made with Cabinet and/or National Security Council level deliberations.

Question 5. Besides, helping the industry to exchange the information it needs to solve its Y2K problems, do you think the proposed safe harbor legislation would also make it easier for the NCS to obtain the information needs to ensure national security and emergency preparedness telecommunications?

Answer. Although NCS has not experienced any reluctance on the part of the telecommunications industry to provide information on Year 2000 readiness, the legislation should help the NCS to continue to obtain the information it needs to ensure national security and emergency preparedness telecommunications.

Question 6. I noticed that the NCS is not represented on the telecommunications working group or the emergency services of the President's Y2K Conversion Council, Chaired by John Koskinen. Is there any particular reason why the NCS was not asked to participate in these groups?

Answer. The NCS has been an active participant in the Telecommunications Working Group since its first meeting and will attend the next meeting of the Emergency Services Working Group. NCS membership and attendance on these working groups has been considered part of the Department of Defense representation.

Question 7. Has the NCS done any studies looking into how failures in foreign networks could impact U.S. Communications? If not are you aware of any such studies?

Answer. The NCS has not done any independent studies regarding failures in foreign networks impacting U.S. communications. We are, however, aware of the special Year 2000 Task Force established (Mar 1998) by the International Telecommunication Union to "provide information on and promote Year 2000 compliance standards amongst ITU members to create greater global consistency and a common understanding." One of their first actions was to issue a Year 2000 questionnaire regarding "Millennium Compliance" and promoting ISO Standard 8601 "Data elements and interchange formats—Information interchange—Representation of dates and times." A Generic Year 2000 Testing Checklist was adopted to define the mini-

mal set of tests which will be required to demonstrate that a network system or component is Year 2000 compliant. Additionally promoted is a British Standards Institute publication from January 1997, Definition of Year 2000 Conformity Requirements.

Question 8. Is the NCS relying upon vendor certification or is it also conducting independent tests as Bellcore recommends to ensure equipment is Y2K functional?

Answer. The NCS is relying on vendor certification as well as the performance of independent tests. We are working with Bellcore in this area to help ensure that independent testing being performed by the Alliance for Telecommunications Industry Solutions (ATIS), Network Testing Committee, includes scenarios developed by the NCS. These scenarios focus on maintaining reliable communications in the public networks for national security and emergency preparedness purposes. This independent testing is planned to be completed in the spring of 1999.

PREPARED STATEMENT OF SENATOR JON KYL

Mr. Chairman, I would like to thank you and Senator Bingaman for your efforts in putting this hearing together.

Y2K will cross the globe in a 24 hour period. It has the potential to wreak havoc with our communications networks and consequently with all of our critical infrastructures. Our first concern must be with the readiness of the nation's telecommunications system to smoothly transition into the next century. But we must also recognize the potential for disruptions that may pose serious public safety as well as national security concerns, and to plan accordingly. We have a distinguished panel of witness today who will help us to understand the Y2K problems facing the telecommunications industry. We will also hear testimony from the National Communications System, a little known but very important entity.

The NCS was created by President Kennedy, in response to communications problems that arose during the Cuban Missile Crisis. It has the responsibility to ensure enduring communications in times of crisis, ranging from national disasters to acts of war. And it has enjoyed a unique and close working relationship with the telecommunications industry, in designing and implementing preparedness plans programs. I look forward to learning the status of contingency planning for national security and emergency preparedness in anticipation of potential Y2K disruptions. The Defense Authorization Act of 1996 directed the President to report to Congress on the future of the NCS. We recognized that the telecommunications infrastructure was facing new threats, especially from information warfare tools and techniques; and that the NCS has unique experience and resources to contribute to an overall strategy to protect the nation against such threats. While Y2K is not an information warfare threat per se, its overall effects could be very similar to a deliberate attack on the nation's information systems. I am sorry to report that, 3 years later, the President still has not filed this report. My most recent letter from Sandy Berger on this subject, dated February of this year, promised that the report would be forthcoming promptly. We are still waiting.

In March, I wrote to FCC Chairman Kennard, to recommend that the Network Reliability and Interoperability Council (NRIC) be directed to examine Y2K concerns. I was pleased to receive his response in May, informing me that the NRIC would be tasked to undertake this effort. I am concerned, however, that this work is not yet underway, and that the hour is late. I look forward to learning about the NRIC's plans for addressing Y2K in the limited time they have.

A key element in solving the Y2K equation is information. We have heard reports that corporate concerns over liability are restricting the flow of technical information and statements of Y2K readiness which telecommunications carriers need for remediation and preparedness efforts. It is vital that industry, as well as consumers, have access to the information needed to fix Y2K problems, and for contingency planning. To the extent liability concerns are chilling this necessary exchange of information, we will need to find ways to alleviate those concerns.

Time is very short. The Y2K Committee and the Judiciary Committee will be working with industry associations, consumer groups, and other interested parties during the August recess to evaluate legislative options to help meet those needs. I would like to invite our witnesses to offer their thoughts and recommendations on such legislative relief.

PREPARED STATEMENT OF JUDITH LIST

INTRODUCTION

Thank you Chairman Bennett, Vice Chairman Dodd, and members of the Special Committee for inviting me to testify on how telecommunications networks could be affected by the Year 2000 technology problem. I am Judy List, Vice President and General Manager of Integrated Technology Solutions for Bellcore.

Bellcore, an SAIC company headquartered in Morristown, New Jersey, is a leading provider of communications software, engineering, consulting, and training services based on world-class research. Our customers include major telecommunications carriers as well as telecom companies of all sizes both in the United States and abroad. The business I head for Bellcore provides Y2K services—primarily to telecommunications carriers and suppliers, financial institutions, and power utilities.

In response to your request, I will focus today on what Bellcore is doing for the industry concerning Y2K, on elements of telecommunications networks that could be impacted by the Y2K problem, on the challenges of testing, on the outlook for the problem as I see it, and on what positive steps can be taken to help with the situation.

BACKGROUND/BELLCORE'S ROLE IN Y2K READINESS

To set the stage, let me say that Bellcore has been working on Y2K solutions for our own software products since 1993, with a concerted effort begun in 1995. Bellcore currently supports approximately 150 software system products that are installed and deployed in the networks or operations of its licensed customer users. Those users include the top tier local exchange carriers, among others. The software system products include operations support systems and network systems that support provisioning, maintenance and other management functions for local telephone services. All Bellcore-supported software system products either are now or will be, by year-end 1998, Year 2000 Functional.[1]

In addition, Bellcore has taken a proactive role in providing our licensees and other customers with Year 2000 information. We have been sharing information about Year 2000 functionality in the following ways, to name just a few:

—by issuing information kits that include Bellcore's Y2K Test Strategies, methodologies and results of our Year 2000 functionality testing;

—by placing information on Bellcore's website, which includes Y2K Frequently Asked Questions and Bellcore software product information; and

—by hosting and participating in customer meetings and forums.

All of this information will continue to be provided and updated regularly by our Year 2000 Program Office.

TELECOMMUNICATIONS NETWORKS

Like many companies, Bellcore assists clients by providing comprehensive services that cover the entire lifecycle for fixing the Year 2000 problem for information technology, or IT, systems. However, in addition to the considerable industry attention on IT systems, Bellcore has supported increased attention on networks. Networks are large, distributed computing environments. While the major telecommunications carriers have recognized the Year 2000 challenges that confront their core business, many commercial companies have been relatively late in recognizing that the Year 2000 problem affects not only their IT systems, but their private networks as well.

In both private and public telecommunications networks, as in software and hardware computing systems, Y2K impacts are possible at every layer of the infrastructure. That is, Y2K problems can be found in applications, operating systems, file systems, databases, protocols, middleware, and hardware platforms, as well as in the interfaces between interconnected systems.

To aid in the remediation and testing process for network equipment, Bellcore worked with telecommunications carriers and equipment suppliers to develop a set of generic requirements for Y2K functionality (Bellcore's GR–2945, "Year 2000 Generic Requirements: Systems and Interfaces"). In general, this document contains requirements for both telecommunications network elements and operations systems and covers a variety of date-sensitive functions. Let me give you just one example. There is a "common platform" section that specifies the minimum date range for all systems as 1/1/1980 through 12/31/2036. The former limit was chosen because it is

[1] As used here, the term "Year 2000 Functional" is the ability of software to record, store, process, recognize, display and calculate calendar dates falling on or after January 1, 2000, in the same manner, and with the same functionality as such software records, stores, proceesses, recognizes, displays and calculates calendar dates falling on or before December 31, 1999.

the date when PC-based management systems began counting time. The latter limit was chosen because this is the date just before many UNIX® -based system clocks will fail. GR–2945 simply sets this range as the minimum requirement every system should meet. However, some vendors may choose to design their systems to operate well outside of this range, which is completely acceptable. Bellcore's GR–2945 was available to the industry on January 31, 1997.

In addition to using GR–2945, we recommend that companies follow a structured approach in addressing Y2K issues. This approach starts with establishing a corporate program office that manages the scope of the program, including schedules, resource allocation and budgets, awareness of Y2K issues throughout the company, and quality assurance. The subsequent activities are: assessment, remediation, testing, and deployment. It has been our experience in working with major US telecommunications carriers and several Fortune 50 clients that a structured approach is being taken with respect to Y2K.

NETWORK ASSESSMENT

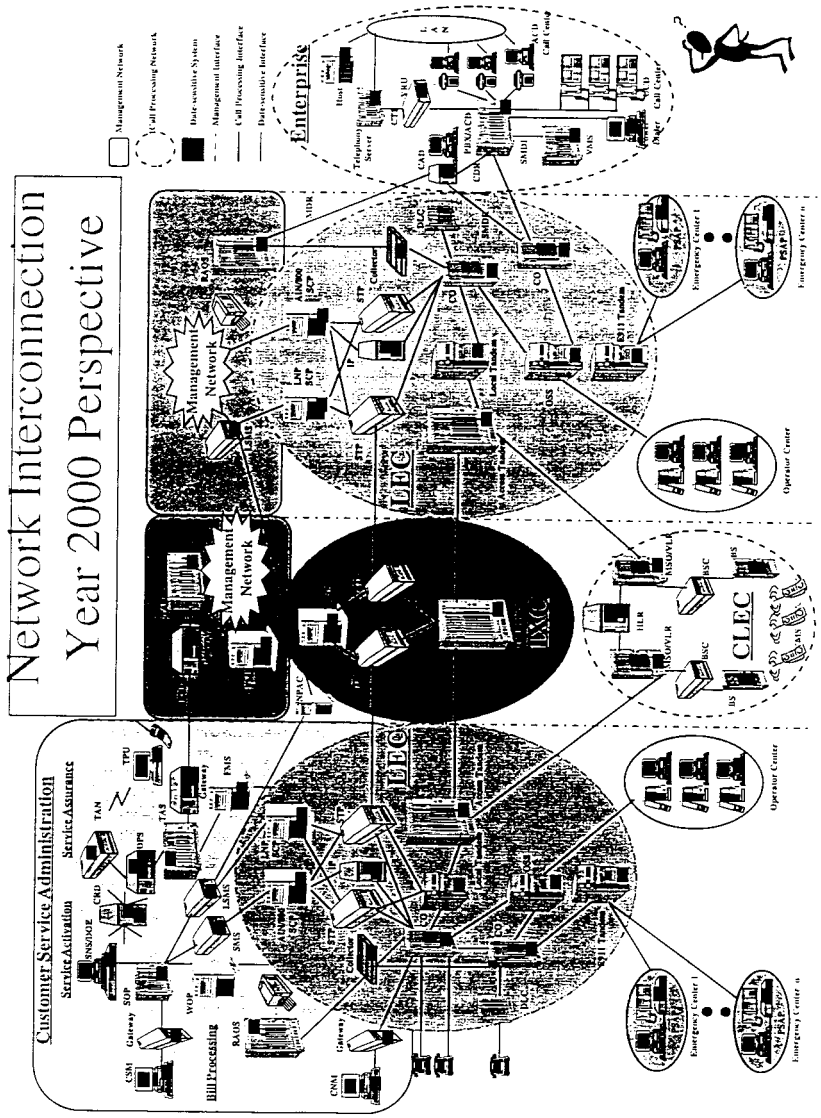
Bellcore has conducted risk assessments of major domestic and international carrier networks as well as risk assessments of the networks of a number of Fortune 50 companies. Risk assessments begin with a comprehensive inventory of all network equipment in the carrier or private network. Then, detailed questionnaires are sent to the suppliers of this network equipment inquiring about the Y2K readiness of the equipment. This information, along with information from the carrier or company about the extent of equipment deployment in their network, network architecture and topology, services, and other information, is used to assess the risk of Y2K vulnerabilities in providing services.

In our work, we have found that approximately 75 percent of voice networking equipment has date sensitive processing in it, 25–35 percent of data networking devices have date-sensitive processing, and almost 100 percent of network management devices have date-sensitive processing in them. The kinds of functions that are date sensitive include: service routing and scheduling, message reporting, network administration and management, system clock maintenance and restoration, event/alarm time-stamping, history sorting and reporting, security (e.g., logins and passwords), user interface displays and user input, trend analyses, logging of information, reports, and data processing functions.

The data we have gathered and the analyses we have performed through these risk assessments, as well as high-level, preliminary experiments we have conducted in our labs, support the conclusion that there is little date sensitive information in the fundamental call processing or data routing capabilities of networks. Where we do see date sensitive information is in the operations, administration, and maintenance functions of networks. Examples of the latter type of functions include: billing, provisioning of services, network surveillance and maintenance, and other network management and administration functions. Let me refer to the chart in the front of the room for a quick look at the complexity of communications networks and to explain where Y2K vulnerabilities are in these networks. (See attached diagram.)

These functions are provided by network equipment that carriers and large corporations license from equipment suppliers as well as in systems that many companies develop themselves. Thus, fixing the software code sometimes means that the company's own organizations are responsible for the fixes, and sometimes means that the equipment manufacturer or software provider is responsible for the fixes. In some instances, a carrier or commercial enterprise may decide not to solve a Y2K issue by having the code fixed. Instead, they may replace the system with a new one or retire the system altogether because the functionality can be provided somewhere else in the network. It is equally important to manage and track progress for the replacement or retirement of systems, because if they are not replaced or retired on schedule, there could be Y2K impacts.

® UNIX is a registered trademark of NOVELL, Inc.



Acronyms:

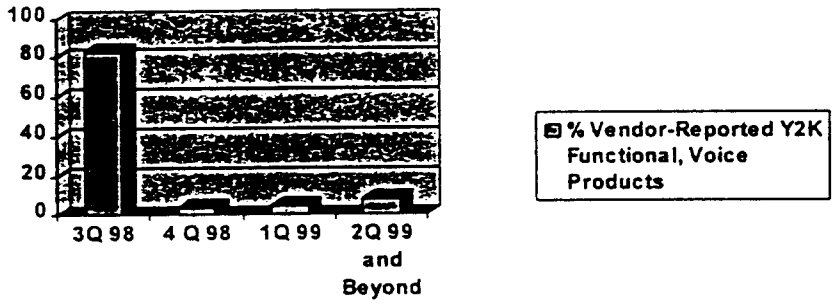
ACD	= Automatic Call Distributor
BS	= Base Station
BSC	= Base Station Controller
CAD	= Call Access Device
CDR	= Call Detail Recording
CLEC	= Competitive Local Exchange Carrier
CMS	= Call Management System
Collector	= Billing Collector
CO	= Central Office, End Office Switch
CRD	= Corporate Record Database
CSM	= Customer Service Management

Acronyms:

CTI	= Computer Telephony Integration
DLC	= Digital Loop Carrier
DPS	= Dispatch System
EBI	= Electronic Bonding Interface
FMS	= Fault Management System
HLR	= Home Location Register
IP	= Intelligent Peripheral
LAN	= Local Area Network
LEC	= Local Exchange Carrier
LSMS	= LNP Local SMS
MDR	= Message Detail Recording
MSO/VLR	= Mobile Switching Office/Visitor Location Register
NPAC	= Number Portability Administration Center System
OSS	= Operator Services System
PBX	= Private Branch Exchange
PSTN	= Public Switch Telephone Network
PSAP	= Public Safety Answering Point
RAOS	= Revenue Accounting Office System
SMDI	= Simplified Message Desk Interface
SMDR	= Station Message Detail Recording
SMS	= Service Management System
SCP	= Service Control Point
SNS/DOE	= Service Negotiation System/Data Order Entry
SOP	= Service Order Processor
SSP	= Service Switching Point
STP	= Signal Transfer Point
TAN	= Technician Access Network
TAS	= Trouble Administration System
TPU	= Technician Portable Unit
UCD	= Uniform Call Distributor
VLR	= Visitor Location Register
VMS	= Voice Messaging System
VRU	= Voice Response Unit
WOP	= Work Order Processor

The analyses we have conducted on the Y2K issues in network equipment have covered thousands of voice and data products, manufactured by hundreds of US and international companies. We have analyzed the data gathered from a variety of sources, including manufacturer's responses to questionnaires, information available on manufacturer websites, and other publicly available sources. We have gathered and analyzed this information in support of our customers; we have not embarked on a comprehensive survey of all carriers, large enterprises, or equipment manufacturers. The charts at the front of the room summarize our analyses of these data, based on our experience, but they have not been independently validated.

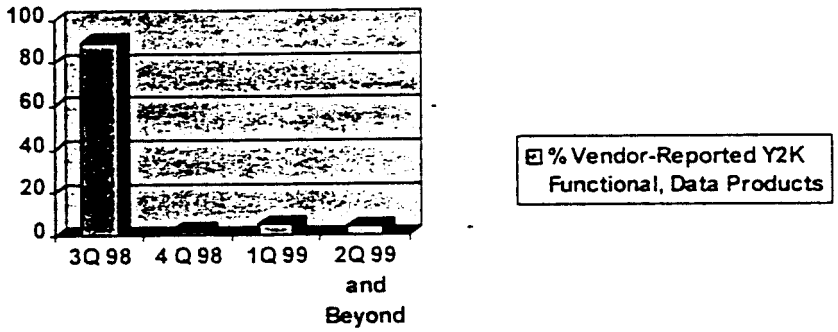
Figure 1. Percentage of Voice Network Products Reported by Manufacturers to be Y2K Functional by Quarter.



Note: 3Q 98 date includes products that have no date sensitivity and products that will be Y2K functional by the end of 3Q 98, according to vendor-supplied information. 2Q 99 and beyond

includes products that will not be Y2K functional by 2Q 99 and those products that the vendor will not make Y2K functional (e.g., manufacturer discontinued products), according to vendor-supplied information.

Figure 2. Percentage of Data Network Products Reported by Manufacturers to be Y2K Functional by Quarter.



Note: 3Q 98 date includes products that have no date sensitivity and products that will be Y2K functional by the end of 3Q 98, according to vendor-supplied information. 2Q 99 and beyond includes products that will not be Y2K functional by 2Q 99 and those products that the vendor will not make Y2K functional (e.g., manufacturer discontinued products), according to vendor-supplied information.

The first chart presents data on voice network products. According to various sources, for the products on which we have collected data, 83 percent of the products are planned to be Y2K functional by the third quarter of 1998, while another 4 percent are planned to be Y2K functional by the end of 1998. An additional 5 percent are planned to be Y2K functional by the end of the first quarter of 1999, and the remaining 8 percent will either not be made Y2K functional (because, for example, they are discontinued products) or are planned to be Y2K functional sometime during or after the second quarter of 1999.

The second chart presents information on data network products. Again, of the products for which we have collected data, 89 percent of the products are planned to be Y2K functional by the third quarter of 1998, while another 2 percent of the products are planned to be Y2K functional by the end of 1998. An additional 5 percent are planned to be Y2K functional by the end of the first quarter of 1999, and the remaining 4 percent will either not be made Y2K functional or are planned to be Y2K functional sometime during or after the second quarter of 1999.

These results indicate that over 85 percent of the telecommunications network products we have surveyed for our major carrier and large commercial enterprise customers are planned to be Y2K functional by the end of 1998, according to their manufacturers. Further analysis of the detailed information we have gathered indicates that the majority of critical network components in carrier networks will be Y2K functional by year-end 1998. It is largely the peripheral devices that will not be Y2K functional until first quarter 1999 and beyond. For example, according to manufacturers, most of the major central office switches used in the US are planned to be Y2K functional by year-end 1998.

Within a commercial enterprise, there are a small number of Private Branch Exchanges (PBXs), voice mail systems, and automatic call distribution systems (ACDs) that will not be Y2K functional by year-end 1998. This market is very diverse and the consequence of non-compliance of any one vendor's device is significantly less. In addition, the non-compliant devices tend to be older and smaller, which again lessens the impact because fewer users are affected. While many of the devices that will not be Y2K functional by the end of this year are peripheral, many of them interact with more critical devices. It is important to test how non-compliant devices (e.g., a network management system) might interact with a Y2K functional device (e.g., a PBX).

Finally, the upgrades to this equipment may still need to be tested by the carrier or commercial enterprise in whose network it is used and then installed in the net-

work. It is important to schedule and track delivery of equipment upgrades and the subsequent testing and installation.

TESTING

Once the software is fixed (either by a supplier, the carrier, or the carrier's agent), the software should be tested. For a software application, this includes unit testing of the code changes, as well as integration testing of various modules of the application together. In addition, system tests are conducted to incorporate the operating system environment, the hardware platform the application runs on, as well as any third party software that may work with the application software. Finally, the interfaces between systems should be tested, particularly for high risk systems, to assess the impact of Y2K remediation on interoperability between systems.

Year 2000 poses significant testing challenges. First, there are a variety of dates that need to be tested; this increases the number of tests that need to be conducted. Second, tests should be repeated—for example, as problems are found and fixed or as additional changes or enhancements are made to the system between the time the code is Y2K functional and the rollover of the millennium. Third, there are difficult test environment issues due to the general need to test applications in a "clock rollover" environment. It is not feasible for carriers to roll the clocks forward in a live network; therefore, doing system clock rollovers requires either extensive laboratory environments or significant investment in parallel systems to test for year 2000 functionality. Testing requires specialized expertise and tools. Finally, industry analysts have estimated that testing is at least 50 percent of the effort in Year 2000. The most significant challenge is that there is too much to test in too little time.

Not only must testing of individual network elements be completed, but interoperability testing is needed as well. We recommend that interoperability testing be conducted for several reasons. There are some interfaces in networks over which date information is passed, and processing on the date information occurs on one side or the other of the interface or on both sides of the interface. In these instances, interoperability testing is needed to assess the extent to which dates are passed and processed correctly on both sides of the interface. However, there are many more instances in networks where date information is not passed or processed across an interface between two systems. While the need for Y2K interoperability testing is less obvious in these instances, it may be possible that while fixing code to address Y2K in one of the systems, some non-date related functionality may be inadvertently "broken" in the interface between the systems.

Finally, because both private and public networks in the US are quite heterogeneous in the types of equipment and the number of equipment vendors who supply equipment, it is often the case that the equipment on either side of the interface is manufactured by different vendors, who may use different date standards. Interoperability testing helps to address these issues.

OUTLOOK

Mr. Chairman, you asked for my personal outlook on the situation in the ttelecommunications industry, and so I will make four points in that regard.

First, as is the case in most other industries, it has been my experience that larger corporations have been more attentive to and more active in resolving the Y2K issue than have smaller companies. All of the major carriers have corporate-level Y2K programs, they understand and are actively working the problem, and they have the ability to work with their major equipment vendors to address the issue. In addition, the US is ahead of most of the rest of the world. Europe lags behind the US in their attention to this issue, and generally, with some exceptions, so does the rest of the world. South America, much of Asia/Pacific (with the exception of Australia), and Africa are quite far behind. I do have a concern that the general lack of attention to Y2K in some parts of the world could adversely impact our ability to communicate with them, largely because of failures in critical infrastructures like power that may impact their telecommunications providers.

Second, as I've mentioned, the Y2K vulnerabilities in the telecommunications network do not appear to be in the fundamental call set-up and processing or data routing capabilities of the network. Rather, they appear to be in the operations, administration, and maintenance functions that support these fundamental capabilities. While this suggests that getting basic dialtone at midnight on January 1, 2000 is less likely to be a problem, it is possible, in my opinion, that there may be disruptions in billing, processing service orders, and so on. In addition, continued difficulties with operations, administration, and maintenance functions could eventually impact service.

Third, telecommunications manufacturers indicate that the majority of them will be Year 2000 functional by the third quarter of this year. Furthermore, our analysis of vendor responses indicates that the majority of critical network components will be Y2K functional by the end of 1998. However, testing and deployment/installation are still required, as is ongoing attention to timely delivery of upgrades.

Finally, there will be problems, and there is a level of uncertainty in this area that makes it difficult to predict where the problems will be. In the software industry today, the best in class companies find 95 percent of code anomalies before the software ever gets to the field. That means that 5 percent of software anomalies are found after the code is operational Furthermore, according to the Software Engineering Institute, a new defect is introduced with every approximately 4½ fixes of software code. Both of these statistics suggest that, given the pevasiveness and extent of Year 2000 elements, there will be problems. It is critical that contingency and disaster recovery planning and training be implemented. Furthermore, Y2K contingency planning and disaster recovery needs to address plans differently than traditional business continuity plans because backup systems are likely to have the same Year 2000 problems, issues may be more widespread across a number of industries, and problems may last for a longer period of time.

RECOMMENDATIONS

In closing, let me make the following brief recommendations on positive steps that could be taken to help with the Y2K issue in telecommunications. First, the entire industry should be doing whatever it can to promote interoperability testing.

Second, the industry should work on a plan for cooperation in the event that emergency business recovery should become necessary. This should include scenarios where only one company is affected as well as scenarios where multiple carriers are affected.

Third, the government could help by continuing to promote awareness of the Y2K problem, as this Committee and others are doing. Raising awareness is particularly important among small and medium-sized businesses.

Finally, there might—at some point—be a need for safe harbor legislation. Such legislation would be designed to protect responsible companies from some of the torrent of litigation we know is headed our way—much of which could be frivolous and could distract attention and divert resources from the most critical work: fixing the problem. This should remain the industry's primary concern, and anything you can do to allow us to focus our efforts on that would be most appreciated.

Again, thank you for the opportunity to testify before you today. I will be happy to take your questions.

RESPONSES OF JUDITH LIST TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. It strikes me that there is no comprehensive industry wide test planned. SIA just began end-to-end (street-wide) testing of all partners in the securities industry. When will the telecommunications industry begin such testing, and who should coordinate such a test?

Answer. In my written testimony before the Committee, I emphasized the challenge of Y2K testing for telecommunications networks and wish to restate that point here. Year 2000 testing for networks is critical but complex because of the variety of dates that need to be tested, and tested repeatedly, the difficult test environment issues, and the need for specialized expertise and tools to conduct tests of networks. However, I do believe that Y2K testing of telecommunications networks is an integral phase in a Year 2000 program. Specifically, it is essential that testing encompass both the interfaces between systems to assess Y2K impacts and interoperability across networks, in addition to stand-alone product testing. As others testified before the Committee, both types of testing are in process through several industry efforts, namely through the Y2K Telco Forum for testing of network interfaces and through the Alliance for Telecommunications Industry Solutions (ATIS) for interoperability testing.

Question 2. You mentioned that according to the Software Engineering Institute that an error is introduced for every 4.5 lines of software fixed. Can you estimate the amount of errors which have been introduced into the system? Could such software errors result in an expected systems failure?

First, a point of clarification. The statistic, as it was presented to me, was that for every approximately 4½ (it actually was 4.4) fixes of software, a new error is introduced. There can be multiple fixes per line of code; conversely, some programs have many lines of code that require no Y2K fixes. Thus, without knowing about a particular application, it is impossible to estimate how many fixes are required

to make the program Y2K functional and therefore, to estimate how many new errors might have been introduced. In this context, I would again emphasize the importance of testing, including testing of the remediated portions of code, product test, as well as interface and interoperability testing. Regression testing is the process by which modified software code is tested against a baselined version of the code to assess the extent to which planned, and only planned, changes to the code have been correctly implemented. Regression testing should be conducted and repeated so that, as additional fixes are made to the code, or new features are added, these can be tested to assess the extent to which new errors may have been inadvertently inserted into the code. With respect to systems failures attributable to newly introduced errors, the potential impact could be different than existing Y2K errors. Our work thus far has indicated there is little date sensitive information in the fundamental call processing or data routing capabilities of networks and that there are relatively few interfaces between network equipment that involve date processing.. However, it is possible that while fixing Y2K problems in some parts of software, errors could be inserted inadvertently that affect non-date related functionality. This possibility, again, emphasizes the need for extensive and repeated testing of the types described above.

Question 3. I understand that much of the code correction for U.S. carriers has been done in foreign countries. What kind of a security risk does this present?

Answer. The issue of security for both the public switched telephone network (PSTN) and private networks as it relates to year 2000 remediation is of paramount importance. As a critical infrastructure supporting the provision of local emergency response, national security preparedness, and commerce and economic transactions throughout the nation and the world, telecommunications networks must be protected from threats, both domestic and international, to their functioning and reliability. Such assurances are fundamental to a robust and reliable telecommunication infrastructure.

There is the possibility that security risks can be introduced into any code that is being remediated, not just code that is corrected in foreign countries. Programmers can, for example, introduce trap doors or back doors for non-malicious reasons, for example, to make it easier for them to maintain the code. These trap doors or back doors can then be used for other purposes to obtain unauthorized access to the software program. In other instances, security problems can be introduced for directly malicious purposes during the code remediation process. To date, I know of no easy way to assess code to ascertain the existence of these types of security risks. It requires labor intensive examination of the code, line by line. Companies can work to protect themselves from such risks by conducting adequate due diligence of employees, contractors, and service providers that they may hire to remediate Y2K problems. In addition, implementing various policies (such as code inspections) to monitor the code remediation process also can help reduce risk.

Question 4. Your recommend that the industry should be preparing contingency plans for scenarios with multiple carrier failures. In what forum should this occur? In your opinion should this be coordinated through the FCC, National Telecommunications Alliance or though the National Communications System? Or would you suggest another entity?

Answer. The telecommunications industry has been successful in the past in providing quick response to problems impacting service both at the individual company level and in working collaboratively to respond to common service-related issues. With the advance knowledge that service could be impacted due to the year 2000 problem, the industry has a unique opportunity to undertake advance contingency planning for potential service degradation or loss. My recommendation on emergency business recovery is for an industry-based effort to be undertaken in advance that would address scenarios in which one company as well as multiple carriers might be affected by Y2K problems.

Such a coordinated effort could be managed by one of a number of entities including those identified above. Rather than recommend a preferred forum for business recovery planning, I would suggest that such a forum be as inclusive as possible with representation from all segments of the telecommunications industry—local and long distance carriers, wireless companies, and equipment manufacturers, for example.

Question 5. Do you suggest interoperability testing between foreign carriers and domestic carriers?

Answer. The challenges of interoperability testing discussed above and in my written testimony apply as well to testing between domestic and foreign carriers. However, such challenges may be heightened by virtue of the geographic and political divisions of the world's countries, the sophistication of their telecommunications infrastructure and their level of awareness and remediation of Y2K-related problems.

U.S. companies, I believe, can serve as leaders in the international arena through their international operations and through partnerships with foreign carriers to increase awareness, to exchange information and knowledge, and to engage in testing where feasible. International organizations, such as the International Telecommunications Union (ITU), can also play an instrumental role in supporting these activities for telecommunications carriers around the globe. Clearly, the importance of interoperability testing both domestically and internationally cannot be overstated and to the extent that it can be facilitated with the support and encouragement from Congress, international organizations, and the carriers, the more likely testing will be conducted.

Question 6. Are the Year 2000 telecommunications test beds available for application testing (such as business applications)? When could such testing begin and who would coordinate them?

Answer. Bellcore has some central-office laboratories that have been used extensively by telecommunications carriers and suppliers for both stand-alone product testing as well as interoperability testing. For example, we recently conducted extensive interoperability tests for local number portability under the oversight of the Alliance for Telecommunications Industry Solutions (ATIS). These laboratory facilities include several of the major switching systems in use in the United States, as well as a hub capability that allows for interconnection with remote laboratories located at carrier or supplier sites. Bellcore also has a separate testing platform in its Quality Assurance testing labs to enable product and interoperability testing of Bellcore's licensed software products in a clock-reset environment. This is a key component of our Y2K testing strategy.

Question 7. You mention that in your assessment of fortune 50 companies you discovered that 25–35 percent of data networking devices have date problems. Isn't that number as high as 50 to 65 percent with (Automated) Intelligent Networks (AIN)? What is the implications of these failure rates?

Answer. The risk assessments we have conducted for carriers have included network equipment that provides Advanced Intelligent Network (AIN) services. The Y2K vulnerabilities of this equipment are similar to the vulnerabilities identified in voice networks. That is, approximately 75 percent of these devices have date-sensitive processing in them, and this date processing is largely in the administrative, maintenance, and operations functions. AIN services can, at times, involve some additional capabilities in call processing (e.g., time-of-day, day-of-week flexible scheduling or routing logic) that may increase exposure to Y2K risks. In addition, AIN is a distributed network environment, so interoperability testing between distributed network elements is critical.

With regard to data networking devices in large commercial enterprises, we've found that 25–35 percent of those devices have date-sensitive processing in them. The higher number (i.e., 35 percent) reflect intelligent data networking devices. That is, data devices that have network management capabilities included as part of the network device itself (as opposed to a separate system) are somewhat more likely to have date processing than data devices that do not include network management intelligence. This is consistent with our overall conclusion that it is the operations, administration, and management capabilities that are most at risk.

PREPARED STATEMENT OF RAMU POTARAZU

Good morning Mr. Chairman, members of the Special Committee. My name is Ramu Potarazu, and I am the Vice President and Chief Information Officer of INTELSAT, the International Telecommunications Satellite Organization. I appreciate the opportunity to testify before you today on the important issues raised by Year 2000.

This morning, my testimony will concentrate on what INTELSAT is doing to address the Year 2000 issues. In fact, we calculate that we have 370 business days left before Year 2000 is upon us.

Let me begin with a very brief history of INTELSAT. INTELSAT was established in 1964 as a global commercial cooperative on the initiative of the United States. At that time, President Kennedy said "I invite all nations to participate in a communications satellite system, in the interest of world peace and closer brotherhood among peoples of the world." President Kennedy's bold and prescient statement led to passage by the United States Congress of the Communications Satellite Act of 1962, which, in turn, resulted in the formation of INTELSAT in 1964, the initiation of commercial satellite service in 1965, and the establishment of full global coverage by INTELSAT in 1969.

INTELSAT's main mission is to provide the space segment for public satellite communications services throughout the world on a non-discriminatory basis. "Non discriminatory" means that INTELSAT provides services to all countries of the world at the same prices. Today, INTELSAT has 143 member countries and interconnects virtually every country and territory in the world. INTELSAT provides international, domestic and regional satellite communications services such as telephone, television, Internet and data.

INTELSAT began its official Year 2000 program several years ago. We recognize that INTELSAT potentially could be affected by the Year 2000 in several areas—from our desktop computing, to our regular daily business transactions, to our ground systems which control our satellites, ground stations operated by our Signatories and direct access users and even the power, air conditioning and security of our headquarters building here in Washington.

INTELSAT adopted a standard, five-step approach to resolving our Year 2000 issues. In the first phase, the Preliminary Assessment Phase, INTELSAT produced an inventory of all equipment that included computer software or hardware (or embedded systems) that could be affected by dates. INTELSAT's second phase is the Analysis and Plan Phase. After we created an inventory in the first phase, we analyzed the inventory and developed plans to remediate any Year 2000 issues. In the Analysis and Plan Phase, we first sub-divided INTELSAT's inventory into three categories: critical, essential and non-essential. INTELSAT's plans, at this time, are to remediate the Year 2000 issues in the critical and essential systems by the end of the first quarter of 1999. INTELSAT's focus would then shift to the remediation of the less urgent, non-essential systems.

The third phase, which we are currently in, is called the Remediation Phase. In this phase, INTELSAT is remediating the critical and essential systems for Year 2000 compliance. INTELSAT is making progress and is on schedule for completion in the first quarter of 1999, as planned at this time.

After remediation of its Year 2000 issues, INTELSAT will engage in the fourth phase: the Testing Phase. The Testing Phase is very complex because, at INTELSAT, we cannot simply shut down our daily operations and easily test software and hardware. Therefore, new facilities have to be set up in temporary locations. We are currently preparing to conduct such tests as soon as the software remediation is complete.

INTELSAT's fifth and final phase is the Deployment Phase. In this phase, INTELSAT will put the systems into production and operation. When this phase is complete, INTELSAT will be ready to operate into the new millennium.

Out of the five phases, the two phases that are the most complicated and manpower-intensive are the Remediation and Testing Phases. As I stated earlier, testing is very difficult but we have very thorough test plans to implement and complete this phase.

In the invitation letter from Chairman Bennett to testify today, I was asked to address four questions. The first question asked was, "How does the Year 2000 problem affect satellite communications?"

INTELSAT has received information from our satellite manufacturers that indicates that the INTELSAT satellites do not have Year 2000 problems. INTELSAT has three satellite vendors, all from the United States, that comprise our current and planned fleet. These vendors are Space Systems/Loral, Lockheed Martin and Hughes Spacecraft. All of our vendors have advised us that there are no known problems on the spacecraft. Typically, a communications satellite does not reference a time and a date; rather, a satellite references what we commonly refer to as "satellite local time," that is a reference to the sun. When there is a technological reference to the sun, there usually is no reference to a specific year. INTELSAT's own analysis and testing will seek to confirm this information. Thus, at this time, we do not believe that our INTELSAT satellites have any Year 2000 issues.

As a result, INTELSAT's Year 2000 emphasis primarily has focused on our ground systems that fly, command and control, and monitor our satellites.

The second question asked was what are "INTELSAT's concerns about international communications?" This, quite frankly, is INTELSAT's biggest concern and is one that is mostly out of our control.

To respond to this question, I will describe the Year 2000 issue as it affects three major groups of INTELSAT users, each of whom operates its own incountry ground network to access the INTELSAT satellite network. The first group is the high tech user group that has a familiarity with computers, is aware of the Year 2000 issue, knows what to do, and is remediating any Year 2000 issues.

The second group is composed of users who have computer systems that may not have been replaced over the last 10 or 15 years. These users have a more limited knowledge of computers because they only repair the computer system when it

breaks. They may or may not be fully aware of the Year 2000 issue, and they may or may not be remediating any Year 2000 issues.

The third group is composed of users throughout the world who have "antiquated" technological systems. They generally do not use computer systems at all to run their systems, and use a lot of manual-intensive labor to perform operations.

Categories 1 and 3 present the smallest problems from INTELSAT's perspective. Our focus is on the users in the middle category—the users that have outdated systems, do not have money to remediate any Year 2000 issues, and sometimes, don't even have the money to recognize that they have a Year 2000 problem.

Many of the earth stations throughout the world have several hundred pieces of computer equipment from various manufactures that control their ability to receive telecommunications information. For example, if antenna control units fail, this failure could cause complete loss of pointing to the satellite by the antenna and no information could be sent or received.

Perhaps I can use an illustration to demonstrate INTELSAT's concerns about Year 2000 issues affecting international communications in satellite communications. A significant part of INTELSAT's international communications is a two-way communication that uses an INTELSAT satellite between country A and country B. If country A's ground network is Year 2000 compliant; and INTELSAT, being the supply chain in the middle, is also compliant; and country B's ground network is *not* Year 2000 compliant, then you will have a failure of the complete chain. To summarize, INTELSAT has some concerns about the Year 2000 compliance of all international communications.

The third question asked was, what is "The general preparedness of the satellite industry?" I cannot answer on behalf of any other satellite competitors or satellite industry leaders. However, INTELSAT has a thorough remediation plan and we are working very diligently to make ourselves Year 2000 compliant. The most appropriate way for me to answer at this time is to say that, yes, we at INTELSAT have a plan in place to be prepared for our global satellite system.

In addition, INTELSAT has been proactive in working with our customers, our Signatories and other international organizations in regard to the Year 2000 issues to exchange and gather information. Here is a brief overview:

With the *World Bank*: INTELSAT's CEO, Irving Goldstein, recently met with the World Bank President, James Wolfenson to discuss cooperation on Year 2000 technical awareness issues. INTELSAT has offered free usage of the INTELSAT space segment to the World Bank for promulgation of Year 2000 issues on a more global basis. INTELSAT understands that the World Bank and other intergovernmental financial institutions have made funding available to governments and the private sector for the Year 2000 program. Last month, INTELSAT participated in the World Bank's Multilateral Development Bank Conference in Washington, D.C. INTELSAT also will be providing technical awareness assistance at the World Bank-sponsored Year 2000 seminars for developing nations. Over 10 seminars in different countries are scheduled between July–October 1998, and the first seminar was held earlier this month, in Brazil.

With the *International Telecommunication Union*: INTELSAT provided Year 2000 speakers at the ITU Africa Telecom conference in South Africa earlier this year and INTELSAT has been assisting the ITU with other Year 2000 initiatives.

With the *Caribbean Telecommunications Union*: INTELSAT spoke about the Year 2000 issue at the CTU Annual Policy Seminar earlier this month.

With the *INTELSAT Advantage Program*: INTELSAT has developed a Year 2000 seminar for its customers and users, and will be offering this information throughout the world over the next 12 months.

With the *INTELSAT Corporate Intranet/Seminars*: INTELSAT has developed an extensive corporate Intranet on Year 2000 issues as a technical resource for our staff and our customers. Because this Intranet includes proprietary business information, its use is restricted. However, INTELSAT would be pleased to meet separately in a seminar format with those interested in learning more about INTELSAT's Year 2000 Program.

The fourth question asked was, what "Specific actions that you believe the Congress or others should take to facilitate the Year 2000 remediation efforts?" From a conceptual point of view, INTELSAT's policy is to encourage the implementation, in every country throughout the world, of some type of legislation which allows INTELSAT and others to share information more readily. Right now, many entities are reluctant to share information because of legal ramifications. As a result, testing and remediation is often duplicated at great expense. In a perfect world, any effective legislation to limit legal liability should have been implemented a year or two ago. Nevertheless, INTELSAT encourages implementation of any legislation that can help alleviate some of the potential legal liabilities that have created a "chilling

effect" on the remediation of Year 2000 issues among organizations and businesses around the world.

INTELSAT also encourages continued congressional support for efforts throughout the world, and particularly in the developing countries, to educate and promote awareness about the Year 2000 issues in order to facilitate technical remediation efforts.

In conclusion, we at INTELSAT have made the Year 2000 issue a top priority and hope that the rest of the industry takes this issue as seriously as we do. And, we believe today's hearing is a very useful way to promote awareness of this very important issue. Once again, I am honored to be here today and will be happy to answer any questions regarding the Year 2000 issues in regard to INTELSAT.

RESPONSES OF RAMU POTARAZU TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. Could you tell the committee how long your satellites would be recoverable without control from the ground. What is the longest time in the recent past that you have lost contact with a satellite due to failure in ground station software and still have managed to regain satellite control and operations?

Answer 1. Answering the second half of the question first, the longest time in the recent past that INTELSAT has lost contact with a satellite due to a ground station failure is approximately two minutes. This is due to the fact that the INTELSAT system has backup redundancy whereby a failure at one ground station is immediately backed up by a second ground station. The second ground station is fully capable of providing the necessary requirements to operate the satellite, including: telemetry processing, tracking, commanding and ranging.

The basic operation of a satellite, however, is autonomous from its ground control station. Therefore, should INTELSAT lose both the primary and backup ground stations for a satellite, then under normal atmospheric conditions, INTELSAT would expect to be able to recover the satellite up to one week after the commencement of the double outage at the ground stations. The only known exception to INTELSAT's estimated "one week" window of recovery is during the two eclipse periods that occur every year. The eclipse periods are two 45-day windows that begin 22 days before and end 22 days after the 15th of March and the 15th of September. During these periods, INTELSAT conducts critical commands and monitoring controls on an hourly basis, 7 days a week, 24 hour a day. If INTELSAT loses its ability to communicate with a satellite during either of these annual eclipse periods, then INTELSAT's failure recovery window of one week could potentially be reduced to half a day.

The time frame of most concern for the Year 2000 issue is a period of 2 days, 31 December 1999 through 1 January 2000. Therefore, even under the extreme and unlikely circumstances of a double outage at the ground stations, as described above, the critical 2-day Year 2000 time period is well within INTELSAT's anticipated "one week" window of recoverable failure time. Moreover, the transition to the new millennium is not during an eclipse period.

Question 2. Can you say how many developing nations are significantly threatened by major communications disruptions due to Y2K problems impacting their ground station or wireline telecommunications?

Answer 2. Although INTELSAT has not conducted its own study with regard to the Year 2000 "readiness" of developing nations, INTELSAT is a member of the ITU Year 2000 Task Force. This ITU group has issued a questionnaire and is conducting a study on this issue. The ITU has indicated that, as of 13 August 1998 over 200 operators from around the globe have responded to its questionnaire. The ITU's questionnaire asked several Year 2000 management questions, and asked the respondents to provide a number rating (1 = high level of confidence, to 4 = low level of confidence) for such areas as:

(a) Systems and Applications,
(b) Networks (domestic, interconnect, international and telex),
(c) Products and Services,
(d) Communications to Customers,
(e) Communications to Suppliers,
(f) Supplier Relationships,
(g) Integration and Testing, and
(h) Business Continuity Planning.

The ITU's questionnaire also asked for the respondents to indicate an expected system compliance date and a final testing-completion date. The summarized results can be found on the ITU's web site at http://www.itu.int/y2k/.

Additionally, as stated in the 31 July 1998 U.S. Senate testimony of Mr. Ramu Potarazu, INTELSAT's Vice President and Chief Information Officer, INTELSAT is participating as a technical telecommunications representative in the World Bank's InfoDev Program, which focus is on Year 2000 issues in developing nations. To date, INTELSAT has participated in the World Bank's regional seminar in Jamaica and the national seminar in Brazil. INTELSAT is scheduled to participate in several additional World Bank seminars by the middle of October 1998.

Question 3. Are you aware of and satisfied with the changes being made to the voice networks you will have to connect to?

Answer 3. By way of background, INTELSAT only provides the space segment portion of a global commercial telecommunications satellite system. Therefore, all connectivity to INTELSAT's network must be made through antennas owned by other entities. These antennas primarily exist at earth stations. Most earth stations have multiple antennas. INTELSAT has no ownership interest in any of the earth stations (or antennas) connecting to its satellite communications network. There are two types of earth stations that connect to INTELSAT. First, Telemetry, Tracking and Commanding (TT&C) earth stations connect to INTELSAT's network. Second, a large number of traffic earth stations that carry commercial services are connected to INTELSAT's network. Each of these types of earth stations are discussed in greater detail below.

TT&C Earth Stations.—All of the TT&C earth stations that connect to INTELSAT's network are independently owned. The TT&C earth stations provide the services necessary for INTELSAT to fly its satellites, and these stations provide for the safety of INTELSAT's satellite fleet as required. INTELSAT has a contractual relationship with specific TT&C earth station sites to provide services. In addition, as part of INTELSAT's Year 2000 Program, INTELSAT has agreements with these TT&C earth station sites to conduct end-to-end testing of the telemetry, tracking and commanding services that they provide to INTELSAT. INTELSAT expects to conduct this end-to-end testing during the fourth quarter of 1998.

Traffic Earth Stations.—The traffic earth stations that connect to the INTELSAT system for commercial voice networks, video, data, Internet, etc. consist of hundreds of earth stations and thousands of antennas. These earth stations and antennas are owned and operated by INTELSAT's customers. INTELSAT recognizes that it is impossible to conduct end-to-end testing with all of these earth stations and antennas prior to the year 2000. Therefore, INTELSAT has embarked on an awareness campaign to inform these traffic earth station operators about INTELSAT's Year 2000 remediation program, and the critical need for these operators to develop their own Year 2000 program. As part of INTELSAT's Year 2000 Program, it has: written letters to all of the Operation Representatives (technical operators of earth stations connected to the INTELSAT network) and written letters directly to each traffic earth station terminal about INTELSAT's Year 2000 efforts. In addition, INTELSAT has made several Year 2000 presentations at various INTELSAT fora including: the INELSAT Global Operation Representatives Conference (GORC), the INTELSAT Global Traffic Meeting (GTM), the INTELSAT Meeting of Signatories, and the INTELSAT Board of Governors meetings and its many committee meetings. As a result of INTELSAT's dissemination of Year 2000 information, INTELSAT has an acceptable level of confidence that the traffic earth station operators are aware of their individual Year 2000 responsibilities.

Finally, the thousands of domestic terrestrial telecommunications operators throughout the world connect to the traffic earth stations described above. Therefore, these terrestrial operators are at least one step beyond the earth stations in the distribution chain of INTELSAT telecommunications services, and INTELSAT does not see the need to directly participate in further end-to-end testing with these operators at this time.

Question 4.—Can you say anything about the readiness or preparations for Year 2000 in these (Far East) countries at this time? Should we be extra concerned given the other problems some of these economies and political systems are already having at this time?

Answer 4. INTELSAT has participated in a number of forums in which it has discussed its Year 2000 Program, including: INTELSAT's involvement in the ITU and World Bank programs (discussed in the answer to Question 2, above), INTELSAT's Advantage Program (which provides technical seminars and training for developing countries who are members of INTELSAT) and INTELSAT's meetings with its Signatories who represent INTELSAT's 143 nation membership. Both the World Bank's InfoDev Program and INTELSAT's Advantage Program have scheduled regional seminars in the Far East during September and October of 1998. Countries on the World Bank's InfoDev current schedule include: India, Pakistan, China, Vietnam, Indonesia, and tentatively Thailand.

While INTELSAT is concerned with the Year 2000 readiness of the Far East, especially in light of the recent economic and political situation, we are somewhat encouraged by the published results of the ITU Year 2000 Task Force questionnaire, previously cited above. The ITU has indicated that, of the 50 questionnaires returned by operators in Asia and "Australasia," only seven operators have given any indication that Year 2000 work has not yet been initiated. According to the ITU's study, the remaining 43 operators have Year 2000 programs in place and the vast majority of these were willing to offer a completion date.

PREPARED STATEMENT OF MICHAEL K. POWELL

INTRODUCTION

Good morning, Mr. Chairman, Senator Dodd and distinguished members of the Committee. I commend the Senate Special Committee on the Year 2000 Technology Problem for its active participation on this issue. I welcome this opportunity to share with you what the Federal Communications Commission (FCC) has learned about industry efforts to address the Year 2000 Problem, as well as to discuss the fundamental importance of the national telecommunications infrastructure and the potential impact of the Year 2000 Problem on embedded telecommunications networks and systems.

My comments today will focus primarily on wireline telecommunications services. However, it is important to note that the FCC is engaged in outreach and assessment initiatives in each of the different subsectors of the communications industry, including terrestrial wireless, radio and television broadcast, cable television, international telecommunications and satellites. Appended to my testimony, as Appendix A, is a summary of how each of these different industries may be affected by the Year 2000 Problem and what industry and the FCC are doing to address these problems.

BACKGROUND

As you are aware, there are many automated and intelligent systems that were not designed to account for the millennial date change of January 1, 2000, and if not addressed, the Year 2000 Problem or so-called "Millennium Bug" could consequently affect every telecommunications subsector. At the FCC, we have developed and continue to develop outreach and advocacy strategies to raise industry awareness of the issue, as well as methods for assessing and monitoring the industries' efforts to address the problem. Finally, we have been looking into ways to facilitate the development of effective contingency plans in the event that a major disruption to the network should occur.

As an initial matter, it is important to remember that no single entity owns or controls the public switched telephone network. There are the major telecommunications carriers, like the Bell Operating Companies, GTE, AT&T, MCI and Sprint, that provide service to the majority of the country. But there are also 1,400 small to mid-size independent telephone companies that serve many rural and insular parts of the country as well as the U.S. territories and possessions. And these companies are only one in a long chain of interdependent companies required for the network to operate domestically.

For example, in order to fix the Year 2000 Problem, the carriers rely on manufacturers of central office switches and other network equipment. And then there are the end users which must make sure their equipment such as their telephones, voice mail systems, Private Branch Exchanges (PBX's), and local area computer networks are all Year 2000-ready otherwise they will not be able to send or receive voice and data traffic. These groups are, in turn, dependent upon other manufacturers for their equipment, who are, in turn, dependent yet again on other providers for parts and services like power. And on it goes.

Without a doubt, the telecommunications network is a tremendously complex and interdependent thing, and consists of millions of interconnected parts. The public switched telephone network processes millions of calls per minute. To transit each and every call, automated and intelligent machines and systems (in the possession of the thousands of telecommunications carriers and users described above) make calculations for the most efficient multi-path, real-time interaction of all points along the established circuit between the call's origination and destination.

For example, in milli-seconds, a phone call from Washington, D.C. to New York travels from your telephone, to the Private Branch Exchange (i.e., switchboard) in your building, to the local exchange carrier's central office switch, through the carrier's network components and systems that route your call to an inter-exchange

carrier (or carriers), through long-distance trunk lines (or other telecommunications facilities like microwave, satellite, fiber optic), to another local exchange carrier's central switch, and ultimately to the telephone on the other end. Make the same call two minutes later and the call may be routed in a completely different manner as calculated by the network.

The foregoing description points to the mathematical impossibility (i.e., the infinite number of permutations and combinations of routing possibilities and service events to transit a voice or data call) of testing the entire public telephone network for Year 2000-readiness or of expressing a high degree of confidence about the readiness of the network. If any one of those components/systems (e.g., central office switch), network elements (e.g., advance intelligent network, Signaling System 7), or network interconnectors (e.g., local exchange carrier, interexchange carrier, Internet Service Provider, private telecommunications network user) is affected by the Year 2000 Problem, a call might be disrupted.

However, I believe that with time and greater knowledge of the scope of the problem, and by maximizing the amount of information available to all companies faced with this problem, we will be able to better predict where and how problems in the network are likely to occur. In my role as Defense Commissioner, I plan to work closely with the industry and the Network Reliability and Interoperability Council to help them address these problems.

FCC EFFORTS

In mid-March, the Commission created its Year 2000 Task Force. In mid-April, at the request of FCC Chairman William Kennard, I agreed to oversee the FCC's Year 2000 efforts and represent the agency on the President's Council on Year 2000 Conversion, which was established on February 4, 1998. I also co-chair with Dennis Fischer of the General Services Administration (GSA) the Council's Telecommunications Sector Group.

At the FCC, we are working to promote an effective public-private, "mission-oriented" partnership to ensure that users of telecommunications services enjoy as close to the same level of quality and reliability on and after January 1, 2000, as they do today. We believe that the FCC can play an important role by encouraging companies to share information with each other and with their customers. This will increase the sharing of solutions, avoid duplicative testing, help companies spot undetected problems, and reduce customer uncertainty and anxiety.

In Appendix A, attached to my testimony, you will find summaries of actions that the FCC has taken to promote its outreach and assessment efforts. As a result, I will only highlight those efforts here.

In an attempt to encourage private sector compliance efforts and to foster information sharing we have set up a special Internet site (www.fcc.gov/year2000/) which has received over 24,000 hits to date. Chairman Kennard, myself, the other commissioners, and FCC staff are all highlighting this problem in speeches and in meetings with leaders in the telecommunications industry.

We have sent over 200 letters to major companies and organizations in all sectors of the telecommunications industry asking them about their efforts to become Year 2000-ready. In June and July alone, we organized eight informational forums with representatives of different sectors of the telecommunications industry to facilitate information sharing and see how the FCC can assist industry efforts to tackle the Year 2000 Problem. In addition, I have asked representatives of each of the communications subsectors to participate on the Telecommunications Sector Group of the President's Council. We had our first meeting with the industry participants on July 17, 1998. I believe that their participation in the sector group will better facilitate communication and information sharing between government and private industry.

We have elected this engagement approach, rather than an adversarial, regulatory one for a number of reasons. First and foremost among them is that there is very little time to get this job done. Only private firms can fix these problems and we must have their full cooperation and must obtain timely and candid disclosure of information. We are of the opinion that a heavy regulatory approach will lead to guarded communications, the involvement of lawyers rather than technologists and managers, and a huge loss of time while we haggle over requests and regulatory demands. Furthermore, most formal regulatory actions require compliance with standard procedures which often take months, time we do not have. Moreover, significant time would be lost to developing, issuing, evaluating and compiling lengthy data requests. Such efforts would divert both the FCC's limited resources and those of the companies from actually working the problem, which after all is what matters most.

Only the industry can fix this problem. It is important to remember that telecommunications carriers and users rely upon a complex, technical network that is engineered for near unfailing reliability. The Bellcore standard is 99.9999 percent up time. (For example, the Bellcore standard for switch reliability requires that any given switch not be inoperable for more than 3 minutes per year. That is 3 minutes of 525,650 minutes in a year.) Thus, these companies have a strong stable of trained experts in network reliability issues. They have experience with identifying threats to network reliability, planning corrections and executing those corrections. They also have experience doing similarly Herculean tasks, having pulled the public switched telephone network apart during the AT&T divestiture and the re-engineering that took place when the country instituted the three-digit area code convention.

ASSESSMENT

Our general assessment of the telecommunications industry remains positive. Our inquiry letters dispatched in late April, for example, asked 20 telecommunications carriers, accounting for roughly 98.1 percent of the country's access lines, to report on their critical systems. We learned that generally, the carriers have completed their review of the inventory for these systems, have completed assessing the impact of the Year 2000 Problem on these systems, and they have set completion dates for remediation, testing and integration by the second-quarter of 1999.

We are led to believe that most major U.S. equipment manufacturers will be able to meet projected demands for equipment. The major manufacturers have had extensive Year 2000 programs in place for some time, and have been working closely with both local and long distance carriers to develop strategies for Year 2000-readiness. Manufacturers report that most of their software and hardware products are already Year 2000-ready and have been made available to customers. They have targeted end-of-year 1998 or first-quarter 1999 for general availability for all Year 2000-ready products. Our continuing dialogue with the industry should allow us to assess any change due to unexpected increases in the demand for products.

The carriers are also cooperating on interoperability and end-to-end testing. Testing is (and will continue to be) the hardest, yet most important, part. Most telecommunications companies estimate that testing comprises 50–70 percent or more of their Year 2000 efforts. And we have learned that testing often uncovers more problems that need to be fixed.

The Telco Year 2000 Forum, which is comprised of eight large regional local exchange carriers, has contracted with Bellcore and is already performing integration testing on Year 2000-ready equipment. ATIS, which is an industry-funded organization whose mission is to advance new telecommunications technologies, will conduct inter-network interoperability testing in January and February 1999, and is also working with Bellcore. According to ATIS, the interoperability tests should encompass network configurations that serve over 90 percent of the country. This type of cooperative industry testing is very important because it is nearly impossible to conduct interoperability and end-to-end tests on the actual public switched telephone network. Unlike the Securities Industry Association's interoperability tests where the securities exchange network can be shut down from daily traffic, the nation's phone network has to be up and running 24 hours a day, 7 days a week and it involves millions of different elements. The telephone companies cannot disconnect their network and turn the clock ahead to the year 2000 to do a test.

I would also like to announce that C. Michael Armstrong, Chairman and Chief Executive Officer of AT&T, has agreed to chair the Network Reliability and Interoperability Council (NRIC) which will play a central role in our Year 2000 efforts. The new Council will have a staff group dedicated to the Year 2000 effort, headed up by A. John Pasqua, Vice President-Corporate Year 2000 Program, also from AT&T, and we hope a representative from a major equipment manufacturer. We believe that NRIC will be invaluable in coordinating overall testing, advising the FCC on the status of the industries' readiness, and assisting the Commission in facilitating the development of contingency plans. A representative of NRIC will also sit on the Telecommunications Sector Group of the President's Council, which will facilitate constructive dialogue between the industry and those government entities that rely most heavily upon the telecommunications infrastructure.

While we have programs in place to address this problem, all that we have observed is not comforting. At this juncture, with respect to the telecommunications industry, the FCC continues to be concerned about the effect of Year 2000 problems on small to mid-size independent carriers as well as on international telecommunications carriers. These two areas of concern arise from the numerous informational meetings the FCC's Bureaus have conducted and the reports received that many of the companies: (1) may not realize (or may be slow to realize) the seriousness of the

problem; and (2) will not have the financial resources, available personnel, or management structure to begin implementing appropriate Year 2000 compliance measures.

With regard to the independent telephone companies, as I stated, there are some 1,400 small to mid-size companies that serve many rural and insular parts of the country. The Commission is working continuously with various trade associations, to which many small and mid-size carriers belong, in an effort to alert their members that they need to begin Year 2000 remediation efforts now. Moreover, the FCC has commenced a dialogue with the National Association of Regulatory Utility Commissioners (NARUC), and specifically the association's Communications Committee for the purpose of promoting State-level awareness of the Year 2000 Problem because of the close regulatory relationship between telecommunications carriers and their State regulators. In fact, just two days ago I attended NARUC's annual Summer meeting where they convened a Communications Committee panel on State-level Year 2000 initiatives. Finally, the FCC intends to transmit letters to each and every one of the 1,400 small and independent carriers in the coming weeks.

We are even more concerned about international telecommunications carriers. The United States, Canada and the U.K. are forging ahead, but we have many concerns about carriers in other nations, especially those in developing countries, that have not yet taken the necessary steps to prevent system failures. We are further concerned that international economic challenges may prevent foreign carriers and users from addressing the Year 2000 problem. For example, in Europe, we have concerns as to whether carriers and users will be ready for the onset of the Euro and still be able to implement Year 2000 compliance efforts. Moreover, in Asia, we are concerned that the current recession and economic difficulties could prevent carriers and users from satisfactorily meeting the Year 2000 challenge.

In concert with the other Bureaus and offices of the Commission, the FCC's International Bureau hosted a series of roundtable discussions with the U.S. communications sector to raise awareness, seek solutions, and informally survey progress of industry efforts. In tandem with these roundtables, we have raised the issue with foreign delegates in the context of the FCC Visitor's Program and Foreign Regulator Workshops. The Year 2000 problem has also been addressed in speeches presented in bilateral discussions and international forums. We have also circulated letters to the U.S. international telecommunications companies informing them of our efforts and encouraging them to take prompt and effective action, including with their foreign correspondents.

In addition, the International Telecommunications Union (ITU) has been addressing this issue. The ITU has established a Year 2000 Task Force with five subgroups (including a contingency planning subgroup) spearheaded by British Telecom's Ronald Balls to increase international awareness and provide direction on the global Year 2000 Problem. The ITU also has circulated "The Year 2000 Millennium Compliance Questionnaire" to its 5,000 members governments, telecommunications carriers, and operators however, the response has been poor. The ITU is redoubling its efforts to mobilize governments to put pressure on operators to respond to the questionnaire. The questionnaire will serve to uncover where efforts are needed and what resources should be directed to those countries.

Other activities of the ITU include hosting workshops, making presentations, and participating in discussions and roundtables. It has established a "Y2K Ambassadors" program to serve as regional coordinators for assistance on Year 2000 Problems and activities around the world. The FCC has agreed to be such an Ambassador for the region of the Americas. The ITU is supporting and involved with Year 2000 testing in Europe and Africa, and dispersing information on various Year 2000 standards such as those of the British Standards Institute (BSI) to telecom and satellite operators, which are its members.

IMPACT OF YEAR 2000

As I stated earlier, the telephone network is a very complicated and interdependent thing and consequently it is difficult to predict with any level of certainty all the ways that the failure of one piece of the network could trigger failures elsewhere in the system. For example, if calls to a particular country fail to be completed, there will likely be many redial attempts, which will place increased burden on one central office switch. Securities trading may target a specific country at a particular time of day. Calls that do not go through will result in increased and unexpected traffic at that switch. In addition, a carrier may be unable to bill correctly for calls. As a result, the carrier receives no revenue or delayed revenue from its customers. As a consequence, the carrier is unable to pay its suppliers in a timely manner.

There are also secondary effects to consider. For example, although no date-sensitive information crosses the interface between two carriers, the Year 2000 issue poses problems when carriers try to conduct maintenance on systems. Performance data is collected on either side of the interface. Some reports are generated on a date/time basis. The problem arises when a failure occurs. If one carrier sees a problem and the other does not, it is difficult to determine which carrier is right, and therefore difficult to identify the root of the problem. There could also be testing and coordination delays. Most carriers are planning to conduct Year 2000 tests with each other.

These are only examples of the types of problems the industry must confront in addressing the impact of the Year 2000 Problem. I believe our role is to facilitate the sharing of information that both raises concerns like these and facilitates the search for solutions.

THE ROLE OF THE FCC DEFENSE COMMISSIONER

In addition to my role as FCC Commissioner and member of the President's Council, I have additional responsibilities in connection with my role as the designated Defense Commissioner. Section 0.181, Title 47 of the Code of Federal Regulations sets out the duties of the Defense Commissioner at the FCC. In Appendix B, appended to this statement, you will find a copy of this section of the code.

In my role as Defense Commissioner, I have endeavored to make sure that the FCC is ready to continue operations in the event of a national emergency. In this regard, our Compliance and Information Bureau (CIB) has been revising the agency's continuity of operation plan to ensure that the agency will continue its work in the event of an emergency that affects FCC headquarters. The revised plan was developed with the help of an expert from National Communications System (NCS) who was detailed to the Commission to help with this project.

In addition, CIB has recently reviewed and evaluated its plan to handle emergency authorizations and other industry-related needs if an emergency were to occur after business hours. In general, this procedure grants CIB the authority to authorize special temporary authority for services requested that it believes are necessary to ensure safety and the continued operation of the network.

With respect to national emergency plans, I inherited some plans when I took on the role of the Defense Commissioner. CIB is reviewing and updating these plans. Any plans will be coordinated with NCS. As I stated earlier, it is premature to make even educated guesses on where our efforts in contingency planing will best be served, but I will work with NCS and the industry in this regard.

ACTIONS THAT THE CONGRESS AND THE ADMINISTRATION SHOULD TAKE TO FACILITATE YEAR 2000 COMPLIANCE EFFORTS

Without a doubt, the legal liability issue is one of the most serious impediments that continues to impede the flow of timely and candid information. Concerns with respect to releasing information related to Year 2000 compliance have been raised at every one of our informational forums. The concerns proffered by industry are associated in part with issues of product disparagement, antitrust violations, third-party liability, carrier-vendor contractual relations, and so on. Consequently, some companies have been reluctant to divulge information due to concerns about liability.

We support the efforts to pass legislation that would promote the exchange of information by limiting the way such information could be used against the company. Respondents to FCC requests for information have requested confidential treatment, invoking 47 CFR §0.459. Several others have labeled their submissions to the letters "proprietary information." Others have expressed reluctance at our sharing this information, despite having not made an explicit confidentiality request. Another factor that interplays is the Trade Secrets Act, 18 U.S.C. §1905, which provides criminal penalties for unauthorized disclosure of information. Thus, I believe there is a significant role to be played by the Congress and the Administration with regard to the legal liability issue and other barriers to the information flow.

CONCLUSION

As we move closer to the Millennium, all of our concerns become more acute. Our efforts so far have begun to establish the kind of inter-company and private/public partnerships that will facilitate the flow of information and get it to those most in need. It will also permit the government to become aware of and respond to needs of the industry as they arise. Our national well-being is dependent upon the reliability of all the nation's telecommunications networks, and government and industry must work together to ensure that whatever disruptions occur do not lead to wide-

spread outages and failures. To that end, the FCC is committed to taking whatever actions it can to facilitate information sharing and industry compliance efforts.

I would be happy now to answer your questions.

APPENDIX A.—OVERVIEW OF THE YEAR 2000 PROBLEM IN THE COMMUNICATIONS SECTOR: CONCERNS AND ACTIONS

COMMON CARRIER BUREAU

Biggest concerns

—Upgrading network switches (although manufacturers are on schedule to provide fixes).
—Upgrading Customer Premises Equipment (CPE), voice mail systems, Private Branch Exchanges (PBX's), ensuring interoperability with the network.
—Ensuring telephone companies (telcos) cooperate fully with major customers and each other to facilitate Year 2000 interoperability testing.
—Ensuring small telcos have the resources and expertise needed to fix the problem.
—Dealing with billing and other internal systems.

What the FCC is doing

—Held roundtable forum, entitled Wireline Telecommunications Networks and the Year 2000 Problem on June 29, 1998. In attendance were representatives of users and user groups, large local exchange carriers, and smaller independent carriers, as well as long distance carriers, trade associations, the Telco 2000 Forum, ATIS and equipment manufacturers. The purpose of the forum was to facilitate the sharing of solution to Year 2000 problems and to identify barriers to solving Year 2000 problems.
—Held meeting at the FCC of the Telecommunications Subcommittee of President's Conversion Council on Year 2000, on July 17, 1998, in which representatives from the telecommunications industry including trade associations and industry groups, such as the Telco 2000 Forum were deputized to ensure efficient and responsive industry input to Conversion Council on Year 2000 issues.
—Met with large and small telcos, telephone trade associations, switch manufacturers, financial interests (banks and clearing houses) and other major users.
—Met with Year 2000 project managers from manufacturers and telcos to impart the Commission's concern and to obtain additional information about their Year 2000 programs.
—Requesting information from telcos, equipment manufacturers, trade associations and Bellcore; and encouraging the sharing of Year 2000 information among industry participants.
—Assessing possible regulatory actions to facilitate Year 2000 readiness, including requiring detailed information on Year 2000 compliance, if necessary.
—Sharing information with other Federal agencies, and improving the FCC Year 2000 website with updated information and links to other Year 2000 websites.
—Analyzing responses to detailed information requests sent to all local exchange carriers and interexchange carriers, as well as to some smaller carriers, and to the major telephone equipment manufacturers on their Year 2000 efforts. Responses have begun arriving. As of June 11, 1998, nineteen companies had filed responses. These efforts will help develop a clearer picture of the Year 2000-readiness of the telecom sector.
—Encouraging companies and industry trade associations to make more information about their Year 2000 efforts available to the public through their websites.
—Continuing outreach efforts to ensure that all companies understand the seriousness of the problem, as well as monitoring to obtain as much information as possible.

What industry is doing

—Participated in FCC roundtable discussion on year 2000.
—Deputized representatives from telecommunications industry on Telecommunications Subcommittee of President's Conversion Council on Year 2000, in meeting held at FCC on July 17, 1998.
—Major telephone companies have been devoting significant resources to ensuring that primary telecommunications networks continue to function on and after January 1, 2000.
—Eight regional telcos have formed the Telco Year 2000 Forum to share information and facilitate intranetwork testing of remediated systems.
—The Alliance for Telecommunications Industry Solutions (ATIS), funded by exchange and interexchange carriers, is undertaking the development of labora-

tory tests (now scheduled for January–February 1999) of inter-network interoperability of remediated systems.
—Bellcore is providing expertise, leadership, testing facilities and technical standards for Year 2000 compliance.
—U.S. Telephone Association sent out an advisory to its members in mid-1997.

CABLE SERVICES BUREAU

Biggest concerns

—Power system failures could disrupt cable service, including the cable system's emergency alerting system messages.
—Timed controllers used for pay-per-view and other video programming, commercial insertion, local origination equipment and converter boxes are examples of equipment which may malfunction.
—Billing systems could generate faulty data.
—Satellite telecommunications links could be disabled.

What the FCC is doing

—Sent inquiries to major cable television companies, cable equipment manufacturers and cable trade associations regarding Y2K.
—Posted questions on the internet regarding Year 2000 problems in cable systems to more than 1,500 cable engineers and technicians.
—Conferred with CableLabs, the research arm of a consortium of cable companies, which has established an industry task force to address Y2K issues. Will continue this dialogue.
—Trained Cable Services Bureau telephone contact representatives to answer questions from the public and operators regarding Y2K problems and compliance.
—Conducted six workshops on Y2K issues at the annual Cable Tec Expo in Denver this June, which was attended by approximately 9,000 technicians, engineers and information technology specialists. Also, discussed Y2K concerns, possible disruptions and potential remedies with 37 equipment manufacturers and vendors, programmers, a city official and large and small cable operators on the exposition floor.
—Held a closed forum for the cable industry and will hold an open forum for the public and the cable industry.
—Developing a cable Y2K fact sheet to be placed on the FCC Year 2000 website and distributed to the public and the cable industry upon request.
—Continuing dialogue with cable operators and equipment manufacturers, including informal sessions with multiple system operators (MSO's).

What industry is doing

—CableLabs has formed a Year 2000 working group that consists of the major cable multiple system operators. These MSO's encompass a significant number of cable subscribers and a large majority of the nation's cable systems. Cable operators who are not members of the Year 2000 Working Group will still benefit from the group's efforts because CableLabs is conducting a nationwide assessment and will share information with all cable operators.
—To our knowledge, the CableLabs group intends to meet every two months to monitor the progress of the industry and to provide the industry with CableLabs' research. In addition, CableLabs will monitor the equipment of cable suppliers to determine Y2K compliance. In September, 1998 in Denver, CableLabs plans to hold a cable vendors conference at which cable equipment suppliers, cable billing systems vendors, and vendors of television commercial insertion equipment are invited to attend and confer on their progress in achieving Y2K compliance.
—Many cable associations, including NCTA, the Cable Telecommunications Association (CATA), and the Small Cable Business Association (SCBA) are actively involved in collecting and disseminating Y2K information and solutions to its members.
—Many cable operators, independent of their activities at CableLabs, are also actively working with equipment vendors to resolve Y2K concerns for their systems equipment.

MASS MEDIA BUREAU

Biggest concerns

—Emergency Alert System may fail just when it is needed most.
—Lack of broadcast news may result in misinformation and mass panic.

—Old transmitters with embedded microprocessor chips and stations with customized transmitter control systems may be hard to test or fix.
—Power system failures could disrupt broadcast service.

What the FCC is doing

—Speaking out on Year 2000 issues at National Association of Broadcasters (NAB) convention and other fora.
—Writing to broadcasters networks and trade associations. Responses received indicate dedicated staff and high priority to minimizing disruption of on-air operations.
—Writing to largest radio and television station group owners, which account for the majority of broadcast stations.
—Meeting with broadcasters and equipment manufacturers.
—Held Y2K forum with representatives of radio and television broadcast associations, networks and large and small broadcast station owners to discuss Y2K challenges to the broadcast industry.

What industry is doing

—NAB has created a website on Year 2000 issues and assigned a Senior Vice President to work on the issue.
—NAB is covering the issue in publications, addressing state broadcast association conventions and planning seminars for its own future conventions.
—Equipment and software vendors are contacting customers with information on which equipment or systems are Y2K compliant, which need hardware upgrades or software updates and which equipment or software is so old or obsolete it is no longer being supported and must be replaced.

WIRELESS TELECOMMUNICATIONS BUREAU

Biggest concerns

—The public safety wireless community has only recently become aware of the Year 2000 problem; and while most modern radio systems in use by police, fire and other emergency services are not expected to experience problems, the pervasive use of computers in support roles such as computer-aided dispatch and the use of older radio equipment raise questions of the vulnerability of these important emergency services.
—FCC requires illumination of certain antenna structures or towers where there is a reasonable possibility that a tower may cause a hazard to air navigation. Potential failure of the power grid in addition to the impact of possible Year 2000 problems in the equipment that monitors, alarms and controls tower lighting raises the possibility of a threat to air safety from unlit towers.

What the FCC is doing

—Writing the major wireless companies, radio equipment manufacturers, frequency coordinators and wireless community associations.
—Convening roundtable discussions with the public safety community, the commercial wireless community and the private wireless community.
—Encouraging wireless industry and trade association publication of articles on Year 2000 problems and experiences.
—Reviewing options to alert and educate the tower lighting community, which includes registered tower owners, equipment manufactures and also licensees; and to assure responsive action assessing the potential for failure and preparing for remedial action.

What industry is doing

—Radio manufacturer have surveyed their equipment, indicated that most of the current equipment is compliant and made information available to licensees for fixes, where necessary.
—The larger commercial wireless communications carriers have surveyed their own equipment and the equipment and services of suppliers and contractors for compliance; they are in the process of taking remedial action. Future testing is planned.

INTERNATIONAL BUREAU

Biggest concerns

—Whether foreign telecommunications companies, especially large segments of the developing world, will be able to provide service on January 1, 2000. This could have a huge impact on international trade, foreign investment, the global economy, and even national security.

—Whether the operability of the global telecommunications network, which is critical to public safety, emergency preparedness and personal communications will be jeopardized.
—In many foreign countries, particularly in Asia and Africa, telecommunications companies are only now becoming aware of the Year 2000 problem and they lack the resources to fully address it.
—We are concerned that some telecommunications carriers have not yet taken the necessary steps to prevent system failures.
—We are concerned that international economic challenges may prevent foreign carriers and users from addressing the Year 2000 problem, (e.g., in Europe, whether carriers and users will be ready for the conversion of the Euro and still be able to implement Y2K compliance efforts and in Asia, whether the current recession and economic difficulties could prevent carriers and users from addressing the Y2K challenge).
—We are concerned that terminating calls overseas, which relies on the networks of foreign Public Telecom Operators (PTO's) could be a problem.
—We are concerned about the Y2K readiness of satellite systems. The primary concern regarding satellite systems appears to relate to the earth stations, which control the satellites from the ground, rather than the satellites, themselves, which generally are not date-dependent.
—We are concerned whether revenue streams will be curtailed by operations/support systems (billing) problems associated with telecom networks and earth to space degradation and/or complete failure.

What the FCC is doing

—Writing to international telecommunications companies and satellite and HF service providers.
—Publishing letters in industry publications and ITU publications.
—Increasing international awareness through the International Telecommunications Union's Year 2000 Task Force and providing direction on Year 2000 readiness. Working with the ITU to educate and motivate foreign telephone companies.
—Actively working with the ITU's Year 2000 Task Force to increase international awareness and provide direction to member governments and companies on Year 2000.
—Planning roundtable discussions to raise awareness seek solutions, and informally survey progress of industry's efforts to ensure that industry is doing all it can to avoid any disruptions in service. A roundtable with international telecommunications carriers was held on June 29. One for the satellite industry was held on July 14.
—Raising issues with foreign delegates, in tandem with these roundtables, in the context of the FCC's Visitor's Program and Foreign Regulator Workshop.
—Speaking out about the Year 2000 problem at international telecommunications meetings in bilateral talks and international fora.
—Writing a letter to foreign regulators from Chairman Kennard and Commissioner Powell discussing the Y2K problem, providing information and asking about their needs.

We are considering

—Encourage companies, service providers and manufacturers to complete the ITU questionnaire.
—Play a more active role in the ITU's contingency planning subgroup of the year 2000.
—Work with our regulatory and governmental counterparts to get them to press their PTO's to act more effectively and quickly.
—Play a coordinating role in the Year 2000 testing for U.S. international carriers.

What industry is doing

—Telecommunications companies are working hard to fix Year 2000 problems.
—Most, if not all, U.S. telecommunications companies have established Y2K czars and offices for Year 2000 compliance, and are dedicating considerable resources to the issue.
—Satellite companies have set up "war rooms" to deal with the Year 2000 problems.
—A number of U.S. international companies have ambitious programs underway to work with suppliers, customers and vendors to address the problem in conjunction with well-designed contingency programs. They have dedicated considerable revenues to such initiatives. Some are scheduled to do Year 2000 testing in 1999 before the Year 2000.

—A few U.S. international carriers plan to complete inventory assessment and remediation by 1999 and dedicate 1999 to sample testing with customers..
—Several countries, including the United Kingdom, Canada, and Australia have high-profile efforts under way to tackle the Year 2000 bug, and their telecommunications companies (e.g., British Telecom) are working with foreign partners on the problem.
—U.S. and foreign carriers are working actively in the ITU Task Force on Y2K and participating in subgroups pertaining to the Task Force. Responding to the ITU Questionnaire on Y2K compliance.
—A couple of foreign carriers (e.g. DT) have established testing through the assistance of the ITU.

COMPLIANCE AND INFORMATION BUREAU

Biggest concerns

—Ensuring that internal database systems and equipment used by the Bureau for enforcement purposes is Year 2000-compliant.
—Preparing the National Call Center to collect data and respond to inquiries relating to Year 2000.

What the FCC is doing

—Checking CIB database software and computers used in the enforcement program, such as mobile and fixed direction finding systems, Global Positioning System (GPS) receivers and the software used to operate these systems.
—Preparing to collect data regarding calls received by the National Call Center and to provide information to the Call Center personnel from other Bureaus and Offices to use in responding to incoming Year 2000 calls.
—Developing plans for continuity of operations, emergency authorizations, and national emergency preparedness.

OFFICE OF ENGINEERING AND TECHNOLOGY

Biggest concerns

—Telecommunications share best practices; appropriate telecommunications network testing be conducted; appropriate real-time telecommunications network monitoring take place.
—Telecommunications equipment testing labs not close down or generate faulty data due to Year 2000 problems.

What the FCC is doing

—Working with member companies of NRIC to define NRIC role that adds value to existing activities.
—Letters sent to more than 300 testing labs.Office of the General Counsel

What the FCC is doing

—Reaching out to the Communications Bar to increase their awareness of Year 2000 issues and urge them to press telcos to increase their efforts to address the problem.

OFFICE OF PLANS AND POLICY

What the FCC is doing

—Examining whether the Internet will be affected by Year 2000 problems.
—Contacting Internet organizations and Internet equipment vendors.

OFFICE OF INSPECTOR GENERAL

Biggest Concern

—The possibility that the Commission's mission-critical systems will not be Year 2000 compliant.

What the FCC is doing

—Participating on a Year 2000 task force addressing the Commission's mission-critical information systems and Information Technology infrastructure.
—Participating on a Year 2000 task force monitoring the telecommunications industry.
—Monitoring the activities of other Inspectors General, the Office of Management and Budget, and the General Accounting Office.

APPENDIX B

§ 0.181 The Defense Commissioner.

A Defense Commissioner and two Alternate Defense Commissioners are designated by the Commission. The Defense Commissioner directs the defense activities of the Commission and has the following duties and responsibilities:

(a) To keep the Commission informed as to significant developments in the field of emergency preparedness, defense mobilization, and any defense activities that involve formulation or revision of Commission policy in any area of responsibility of the Commission.

(b) To represent the Commission in national defense matters requiring conferences or communications with other governmental officers, departments, or agencies.

(c) To act as the Defense Coordinator in representations with other agencies with respect to planning for the continuity of the essential functions of the Commission under national emergency conditions, and to serve as the principal representative of the Commission to the Interagency Emergency Planning Committee of the Federal Preparedness Agency/General Services Administration.

(d) To serve as the principal representative of the Commission to the Interagency Civil Defense Committee of the Defense Civil Preparedness Agency of the Department of Defense.

(e) To serve as the principal point of contact for the Commission on all matters pertaining to the National Communications System.

(f) To take such measures as will assure continuity of the Commission's functions under any foreseeable circumstances with a minimum of interruption.

(g) In the event of enemy attack, or the imminent threat thereto, or other disaster resulting in the inability of the Commission to function at its offices in Washington, D.C., to assume all of the duties and responsibilities of the Commission and the Chairman, until relieved or augmented by other Commissioners or members of the staff, as set forth in §§ 0.186 and 0.383.

(h) To approve national emergency plans and develop preparedness programs covering: provision of service by common carriers; broadcasting facilities, and the safety and special radio services; radio frequency assignment; electromagnetic radiation; investigation and enforcement.

(i) To perform such other duties and assume such other responsibilities related to the Commission's defense activities as may be necessary for the continuity of functions and the protection of Commission personnel and property.

[29 FR 14664, Oct. 28, 1964, as amended at 41 FR 31209, July 27, 1976]

RESPONSES OF COMMISSIONER MICHAEL K. POWELL TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. I know that the telecommunications industry like other industry sectors this Committee has reviewed suffers from a lack of status information. Having said that, What is your assessment of the preparedness of the telecommunications industry? Will there be outages? What are the biggest Year 2000 vulnerabilities in the public-switched networks?

Answer. The Federal Communications Commission's ("FCC") overall assessment of the wireline telecommunications industry continues to be positive. Based on our current assessment of personnel resources dedicated, financial resources allocated, time spent combating the problem (on average, 2–3 years), and the sophistication of assessment and execution plans devised, we currently believe that major U.S. carriers (who, on average, have spent $300 to $400 million) and equipment manufacturers are aggressively attacking the Year 2000 Problem. We are also relatively confident of the carriers' representations that they are engaged in remediation efforts that will provide users of telecommunications services with as close to the same level of quality and reliability on and after January 1, 2000, as they do today.

As I stated to the Committee on July 31, 1998, the Commission sent inquiry letters in late April 1998 to the top 20 domestic telecommunications carriers, accounting for more than 97 percent of the country's total access lines, asking them to report on their critical systems. We learned that, generally, those carriers have completed their review of the Year 2000 Problem on these systems, and have set dates for remediation, testing and integration that are scheduled to be completed by the end of the second-quarter of 1999.

The information we have received suggests that the major U.S. equipment manufacturers also will be able to meet projected demands for upgraded equipment. The major manufacturers have had extensive Year 2000 programs in place for some

time, and have been working closely with both local and long distance carriers to develop strategies for Year 2000-readiness. Manufacturers report that most of their software and hardware products are already Year 2000-ready and have been made available to customers. They have targeted end-of-year 1998 or first-quarter 1999 for general availability for all Year 2000-ready products.

Domestic wireline carriers are also cooperating on interoperability and end-to-end testing. The Telco Year 2000 Forum (which includes Ameritech, Bell Atlantic, BellSouth, GTE, SBC Communications, Southern New England Telephone Company, and U.S. West) has contracted with Bellcore and has already begun to perform integration testing on some equipment. The Alliance for Telecommunications Industry Solutions ("ATIS"), a domestic wireline telecommunications industry funded organization whose mission is to advance new telecommunications technologies, will conduct inter-network interoperability testing in January and February 1999, and is also working with Bellcore. According to ATIS, the interoperability tests should encompass network configurations that serve over 90 percent of the country.

It is important to note that there are more than 1,300 small to mid-size companies that serve many rural and insular parts of the country. We have a lesser degree of confidence about their Year 2000 readiness efforts. But that pales in comparison to our concern about international telecommunications carriers, especially those in developing countries, that have not yet taken the necessary steps to prevent system failures. Because global telecommunications rely upon the seamless interconnection of many different networks, the international dimensions of the Year 2000 Problem are especially significant. We note, however, that U.S. international carriers are active participants in the ITU Y2K task force, its working groups, and its correspondence groups, where their contributions are substantial. Also, we are considering playing a more active role in the ITU's contingency planning subgroup of the ITU's Year 2000 task force.

The Commission is also concerned about Year 2000 effects on Customer Premises Equipment ("CPE") that permit customers to access the public switched telephone network. It is also important to note that CPE is not part of the public switched networks that are operated by telephone companies, but instead is owned by public and private entities that must assume the responsibility for insuring that their CPE will be Year 2000-ready. This concern extends more generally to all internal communications networks, and especially to those communications networks and systems that connect with public switched networks. Private Branch Exchange ("PBXs"), CPE, internal networks and connections, telephone systems and all other privately maintained telephone equipment must be Year 2000-ready and able to access properly the telephone network. Equipment manufacturers have stated that they are ready to work with their customers on these systems, but have expressed concern that not all customers are taking steps to insure that their equipment and systems will be Year 2000-ready.

Finally, the Commission is concerned about the proper functioning of the national power grid which supplies, in the first instance, electricity for all telecommunications carriers. Telecommunication carriers are, however, developing contingency plans in the event power supply failures occur.

Question 2. It seems to me that the FCC has been very slow to respond to Y2K and its impact on communications. Furthermore, the Network Reliability and Interoperability Council's (NRIC) report on the implementation of the Telecommunications Act of 1996 which was completed on July 15, 1997, devoted only 3 sentences out of 266 pages to Y2K. I commend you on the excellent choice of Michael Armstrong, CEO of AT&T, to head NRIC. It is imperative at this late date that they get to work. What is the status of the NRIC tasking? Why was NRIC not tasked earlier? Would you please say more about NRIC's plans to assess the impact of Y2K on all aspects of the communications industry (voice, data, wire, broadcast, radio, wireless cable and satellite)?

Answer. I share the disappointment of some members of the Committee that prior to 1998 the Network Reliability and Interoperability Council ("NRIC") devoted relatively little attention to the Year 2000 Problem. As originally chartered to implement the Telecommunications Act of 1996, the NRIC was directed to provide recommendations both for the Commission and to the telecommunications industry to assure optimal reliability and interoperability of, and accessibility and interconnectivity to, public telecommunications networks in an increasingly competitive environment. The focus of the NRIC's recommendations was to ensure the ability of users and information providers to seamlessly and transparently transmit and receive information between and across telecommunications networks. As a consequence, the NRIC focused on its overall mission of network reliability, interoperability and interconnectivity, rather than focusing exclusively on the Year 2000 Problem.

We have been working to direct the focus of a newly constituted NRIC to address more aggressively the Year 2000 Problem. Part of that effort was the selection of C. Michael Armstrong, Chairman and Chief Executive Officer of AT&T, as the NRIC Chairman. Another significant component of that effort was the creation of a staff group dedicated to the Year 2000 effort, headed up by A. John Pasqua, Vice President-Corporate Year 2000 Program, also from AT&T.

The newly constituted NRIC—which will include representatives from all the communications industries, including broadcast and cable, as well as equipment manufacturers and Internet Service Providers ("ISPs")—will play an important oversight role with respect to interoperability and end-to-end testing. We believe that this organization will be invaluable in coordinating the overall testing, collection and dissemination of information, in addition to advising the Commission on the status of industry readiness, and facilitating the development of contingency plans.

We have been working with the NRIC to develop a plan for addressing the Year 2000 issue. The Council will be broken down into a series of focus groups, each with a prominent leader/coordinator, that will look at specific Year 2000 issues (i.e., assessment, network interoperability, and end-user specific problems). Announcements regarding this organizational approach, as well as the date of the re-chartered NRIC's first meeting will be made shortly. Work on these interoperability, interconnectivity and reliability issues, however, is proceeding daily.

It is important to note, however, that the NRIC is only one of the many tools the Commission is using to assist it in its effort to address the Year 2000 Problem. There are also several prominent telecommunications organizations that are actively engaged in addressing the issue of testing and contingency planning. The Telco Year 2000 Forum, ATIS and other industry groups are providing valuable assistance in facilitating information sharing, building private partnerships, and coordinating testing and contingency planning. The Commission will continue to work with and rely upon these industry organizations.

Question 3. We understand that FCC will eventually ask NRIC to assess the impact of the Year 2000 Problem on our nation's network, to encourage sharing of information on solutions, and to facilitate end-to-end testing of networks. We understand that NRIC is not yet engaged, but does FCC have any preliminary results in these areas?

Answer. Yes. The Commission is engaged in its own assessment of the various communications industries. As stated in response to Question 1, our current assessment of the wireline telecommunications industry is relatively positive. That assessment is based on the responses—of major U.S. telecommunications carriers and manufacturers—to our written inquiries and is also based upon the numerous informational meetings and forums that have been conducted by the FCC's Common Carrier and International Bureaus.

It should be emphasized that the Commission has taken its responsibility to monitor the pace and extent of the telecommunications industry's Year 2000 compliance efforts seriously since first becoming aware of the problem several years ago, and has been working to ensure that the Year 2000 challenge is properly addressed. For example, the Commission started to examine and fix its internal computer systems in 1995. In early 1997, the FCC's Bureaus and offices made a coordinated effort to find out what the telecommunications industry was doing about the problem, and continuing efforts have been underway to update and improve our understanding of the nature, and extent, of all of the issues that need to be addressed.

Question 4. Could you tell us, as the Chairman of the President's Year 2000 Conversion Council Telecommunications Working Group, has the Group developed a strategy and an action plan for assessing the Year 2000 readiness of the telecommunications sector?

Anwer. In late April 1998, at the request of FCC Chairman William E. Kennard, I agreed to oversee the Commission's Year 2000 efforts and represent the agency on the President's Council on Year 2000 Conversion, which was established on February 4, 1998. Immediately following my selection to the Council, I was asked to co-chair with Dennis Fischer of the General Services Administration ("GSA") the Council's Telecommunications Sector Group.

One of my first priorities upon assuming leadership was to devise a sector outreach plan for the Commission and to use that document as the model for the entire Telecommunications Sector Group. In brief, that plan has contained three distinct, but interrelated operational concepts: (1) outreach and advocacy, (2) monitoring and assessment, and (3) contingency planning.

One of the primary objectives of the Commission's effort has been to encourage private-sector Year 2000 compliance and to foster information sharing. As part of its outreach and advocacy initiative, the Commission has set up a special Internet site (www.fcc.gov/year2000/) and sent over 200 letters to major companies and orga-

nizations in all sectors of the communications industry—including wireline telephony, terrestrial wireless, radio and television broadcast, cable television, satellites, and international telecommunications. Chairman Kennard, myself, the other commissioners, and Commission staff are all emphasizing the importance of this problem in speeches and in meetings with leaders in the telecommunications industry.

Another critical obligation of the Commission is to monitor industry Year 2000-readiness efforts and to assess the pace and extent of the implementation of remedial actions. In June and July alone, the Commission organized eight roundtables with representatives of different sectors of the communications industry to facilitate information sharing and see how the Commission can assist industry efforts in addressing the Year 2000 Problem. The Network Reliability and Interoperability Council is gearing up to advise the Commission on technical issues and to take steps to foster industry cooperation on Year 2000 compliance testing and other related problems.

Finally, the FCC is engaged in an effort to make sure that the Commission is ready to continue operations in the event of a Year 2000 event, and is committed to working with the National Communications System ("NCS") and the communications industry to facilitate the development and, if necessary, execution of contingency plans in the event that a major service disruption should occur.

Question 5. I understand that, FCC has requested detailed information from over 200 telecommunications companies, equipment manufacturers, trade associations and contractors, but has only received 19 responses. How do you account for this less than 10 percent response rate? What are you doing to improve responsiveness?

Answer. The Commission has received 82 responses to the 200 inquiry letters that were sent. While the letters to the wireline carriers, manufacturers and related organizations mandated a response, the letters to the other industries requested responses on a voluntary basis, thus accounting for, to some degree, the difference between the wireline and non-wireline response rates.

The comparatively low response rates that we have received from the non-wireline sectors of the telecommunications industry has helped us to understand that there needs to be a much more dramatic outreach effort. In this regard, we are in the process of redoubling the efforts of each Bureau to increase outreach efforts, especially in the wireless area, and we have been working to improve the usefulness of the information that is available on the Commission's Year 2000 Internet site (www.fcc.gov/year2000/). The Commission also intends to send additional letters to U.S. international telecommunications carriers and organizations, and to all wireline telecommunications carriers, by the end of September 1998, and to initiate a second round of assessments across all industries.

Question 6. You note in your testimony that FCC's power to force carriers, manufacturers and telecommunications users to address the Y2K problem is limited. What specifically are the FCC's regulatory powers? What can the FCC do to ensure that the telecommunication industry will be ready in time? Will this be enough or does the FCC need more authority?

Answer. The Federal Communications Commission has broad regulatory jurisdiction over interstate and foreign (international) telecommunications carriers (i.e., common carriers), whether such service is provided by radio or wire. This includes, for example, the authority to adopt rules and impose conditions in the public interest, see, e.g., 47 U.S.C. §§ 154(i), 201(b), 303(r); the authority to issue radio licenses and common carrier certificates in the public interest, 47 U.S.C. §§ 214, 309; the authority to revoke radio licenses, 47 U.S.C. § 312(a); the authority to issue cease and desist orders, 47 U.S.C. § 312(b); the authority to impose forfeitures, 47 U.S.C. § 503(b); and the authority to collect information, see, e.g., 47 U.S.C. §§ 218, 308(b), 403, 409(e).

We do have some concerns, however, that an overly regulatory approach could undercut more productive cooperative efforts by the carriers involved. Consequently, the Commission has initially implemented a Year 2000 effort designed to work cooperatively with the carriers to help accomplish Year 2000 compliance. In this regard, we have been working with each sector of the telecommunications industry to promote a collaborative, "mission-oriented" partnership to ensure that users of telecommunications services enjoy as close to the same level of quality and reliability before and after January 1, 2000, as they do today. We are taking a similar approach with other industries regulated by the Commission (e.g., radio and television broadcast, cable television).

Nevertheless, we continue to evaluate various regulatory options and will not hesitate to use those that appear productive. While we believe our existing jurisdiction over interstate telecommunications carriers should be sufficient for any regulatory steps ultimately deemed appropriate for such carriers, to the extent Congress wishes the FCC to have unambiguous authority in this area with respect to intra-

state common carrier service as well, legislation would be advisable. In addition, while the FCC does have ancillary jurisdiction to take certain regulatory steps with respect to telecommunications manufacturers and users, see generally 47 U.S.C. § 151; *United States* v. *Southwestern Cable Co.*, 392 U.S. 157 (1968), to the extent Congress wishes to ensure that the Commission has unambiguous jurisdiction to take any regulatory steps that may subsequently be deemed necessary in this area with respect to manufacturers and users, legislation would be advisable.

Question 7. Testing has been described as a critical component of Year 2000 risk management strategies, and some have said that one should plan on testing everything that you possibly can. Yet telecommunications service providers have previously stated that, due to its very nature, it is simply impossible to recreate an "off-line" public switched network and therefore complex Year 2000 interoperability must be tested in pieces by various companies separately. How will this critical testing be performed, who will do it, and when will it begin? By breaking network testing into different service components and chunks, what are the limitations on the results of these test activities? How, if at all, can one ensure that the full range of activities? How, if at all, can one ensure that the full range of risks posed by Year 2000 to the public switched network have been effectively and appropriately addressed? How involved is the FCC in monitoring the testing of end-to-end connectivity?

Answer. Telecommunications service providers oppose "live" testing of operating telecommunications networks because of the risks that such testing poses to the continued provision of service to their telecommunications users and users of interconnected telecommunications networks. As a consequence, efforts have been underway for some time among manufacturers, testing labs such as Bellcore, carriers through the Telco Year 2000 Forum, and industry organizations such as ATIS which anticipate that arrangements for interoperability testing for its members will be completed before the end of this year.

Because wireline carriers are on different schedules for Year 2000 remediation of equipment and systems, schedules necessarily vary with respect to when they will be able to engage in interoperability testing. AT&T, for example, states that it expects to complete its remediation efforts by the end of this year, so that it will have all of 1999 available for testing.

In addition to efforts by the Telco Year 2000 Forum and ATIS, one of the functions of the newly rechartered NRIC will be to coordinate the efforts of the various groups currently testing and facilitate the sharing of that information so that carriers, and other interested parties, will be able to use the results of those tests to further their remediation efforts and to develop contingency plans—especially by those carriers that will not be as far along in their remediation efforts. We anticipate that the most critical interoperability testing will occur first, with less critical systems being tested later. With respect to the issue of comprehensive testing to insure that no service disruptions will occur, it should be recognized that it is not possible to ensure that all conceivable tests of all potentially interactive combinations of equipment and software will be performed. For example, one large carrier estimated that the number of tests that would be required to test all combinations of its equipment and operating systems would be exceptionally high—1029. Attempting to perform that number of tests in the time remaining is simply impossible, even if adequate test beds and other facilities were available to facilitate such testing.

The FCC's monitoring efforts have been directed to regular discussions with testing organizations and carriers.

Question 8. Your testimony describes contingency planning as a key component of FCC's approach to the Year 2000 Problem. What is the current status of contingency planning in the telecommunications sector?

Answer. Effective contingency planning requires in-depth knowledge of the different types of Year 2000 disruptions that can occur from each piece of equipment, and each software system, operating individually and interactively in the unique environment of each carrier, as well as knowledge of the likely nature of Year 2000 disruptions that may arise from interconnected carriers. As a consequence, detailed contingency planning depends, to some extent, on the completion of Year 2000 assessment and remediation efforts by each carrier.

Most of the carriers with whom we have discussed contingency planning have stated that their efforts at this point are necessarily focused on Year 2000 remediation efforts. Many companies have existing contingency plans that will be used as inter-company procedures in the event of a Year 2000 incident. Such plans include: (1) recognition of the need for company-wide plans to handle Year 2000 incidents; (2) the need for staff supplementation for troubleshooting Year 2000-related incidents; (3) the acquisition of alternate suppliers and the development of alternative deployment plans in case of third party failure to meet commitment schedules; (4)

the need to expand network capacity to address network overloads or peaks that may result from Year 2000 disturbances; and (5) reserves for additional resources of electrical power (i.e., diesel generators).

We will coordinate through many groups, including the NRIC, to assess regularly the progress of contingency planning and to help build private partnerships needed for effective national responses.

Question 9. Executive Order (E.O.) 12472 requires the FCC to perform functions during non-wartime emergencies. The FCC's rules accordingly assign the FCC Defense Commissioner the specific duties of assuring continuity of the Commission's national security/emergency preparedness (NS/EP) plans and programs. Has the FCC developed the plans and programs to the potential situations associated with the Year 2000 Problem? If not, why not? Isn't this also contingency planning?

Answer. As the FCC's Defense Commissioner, I have endeavored to make sure that the Commission is ready to continue operations in the event of a Year 2000 incident. In this regard, our Compliance and Information Bureau ("CIB") has been revising the agency's continuity of operation plan to ensure that the agency will continue its work in the event of an emergency that affects our Washington, D.C. headquarters. The revised plan was developed with the help of an expert from National Communications System ("NCS") who was detailed to the Commission to help with this project.

Moreover, CIB has recently reviewed and evaluated its plan to handle emergency authorizations and other industry-related needs if an emergency were to occur after business hours. In general, this procedure grants CIB the authority to authorize special temporary authority for services requested that it believes are necessary to ensure safety and the continued operation of the network.

With respect to national emergency plans, CIB is reviewing and updating these plans, and the Commission will coordinate with NCS.

Question 10. An issue which has prevented organizations to openly share information relating to Year 2000 is the legal liability. What is your opinion/recommendation on this issue? Will the President's proposed "safe harbor" legislation be sufficient to stimulate information exchange?

Answer. Without a doubt, the legal liability issue is a significant barrier to the flow of information. The concerns proffered by industry—some that appear to be overstated and some that appear to be legitimate—are associated in part with issues of product disparagement, antitrust violations, third-party liability, carrier-vendor contractual relations, just to name a few. As a consequence, some companies have been reluctant to divulge information pertaining to their Year 2000 vulnerabilities and, additionally, have been largely unwilling to guarantee or certify Year 2000-readiness due to concerns about liability.

The Commission constantly deals with the anxiety that various portions of the telecommunications industry, and its suppliers, have about legal liability. In its collection of information from carriers and equipment manufacturers, some respondents have requested confidential treatment, citing Title 47, Section 0.459 of the Code of Federal Regulations. Others have labeled their responses as "proprietary information," and still others have expressed general reluctance at sharing this information.

We believe there is a significant role to be played by the Congress and the Administration with regard to the legal liability issue and other barriers to the information flow. We thus support efforts to pass legislation that will promote the exchange of information by limiting the way such information could be used against entities that provide such information.

I do not know whether the Administration's "Good Samaritan" legislation or Congressman Dreier's legislation will eliminate all the barriers to information exchange, but am sufficiently confident that the proposed bills will advance the effort. Additional measures, however, may be needed.

Question 11. As noted in your written testimony, the response to the International Telecommunications Union's (ITU) questionnaire was, in your own words, "poor." I understand that US companies were queried, but few responded. Would you comment on this? Also, as noted in your testimony, the ITU is re-doubling its efforts to mobilize governments to put pressure on operators to respond to this questionnaire. Will the FCC be doing this for US carriers?

Answer. Responding to the ITU's questionnaire was not mandatory and, given the lack of authority of the ITU over the actions of its membership (which is consensual), the disappointly low response rate is not, in some respects, surprising. Also, we note that the ITU staff explained the low response rate in part by acknowledging that the letters were sent without adequate information on Year 2000 contacts—in fact, this is the thrust of the first few questions on the ITU questionnaire. We have taken steps to encourage domestic international carriers to respond to the ITU ques-

tionnaire and will continue to do so. We are also encouraging them to take all other actions that may be necessary to avoid Year 2000-caused disruptions in service. It should be noted that U.S. international carriers are active participants in the ITU Year 2000 task force, its working groups, and its correspondence groups, where their contributions are substantial.

In addition, as part of its advocacy and outreach effort, the FCC is working to: assume a more active role in the ITU's contingency planning task force; coordinate with our regulatory and governmental counterparts abroad to encourage them to press their telecommunications carriers to act more effectively and quickly; play a coordinating role in testing for U.S. international telecommunications carriers and be instrumental in urging other U.S. government agencies to reduce legal barriers to communications. (Companies state that they feel constrained by current laws and rules relating to sharing of information among companies.)

Question 12. With respect to International telecommunications services, it appears as though some foreign carriers' networks may not be fully Year 2000 Compliant by January 2000. What risks, if any, does that pose to other networks that may be linked to that non-compliant infrastructure? What cascading effects, if any, might be expected? What other risks could arise because of the failure of foreign carriers to ensure that their networks and supporting business systems are Year 2000 compliant?

Answer. The Commission currently has no information to suggest that there will be significant problems with international telecommunications service. U.S. international telecommunications carriers and equipment manufacturers that participated in the June 29, 1998 informational roundtable convened by the FCC's International Bureau and other various meetings seemed to affirm this current assessment.

Of course, at this juncture, we cannot specifically report on whether the foreign telecommunications carriers' networks will be Year 2000-ready by January 1, 2000. However, we are still investigating the ways in which the failure of one piece of the global telecommunications network could trigger failures elsewhere.

The global telecommunications network is a very complicated and interdependent thing and consequently it is difficult to predict with any level of certainty potential Year 2000-related risks. For example, small, sporadic outages distributed across the globe could theoretically arise and affect voice and data service. These relatively isolated incidents could arise on January 1, 2000 or several days after. Furthermore, massive redial attempts and disabled central office switches (due to power outages and related reasons) could result in increased and unexpected traffic transiting through a foreign carrier's remaining operational central office switches and impair service. Moreover, there could be problems associated with billings, accounting and data records (e.g., maintenance, performance information), or service (i.e., activation or transfer of services) may be temporarily delayed or interrupted.

Question 13. What is FCC's role in handling problems such as the recent AT&T frame-relay outage and the Galaxy satellite paging system problem? Did these problems provide FCC any lessons learned for handling of potential Y2K problems?

Answer. Under Section 63.100 of the FCC's rules, 47 C.F.R. § 63.100, wireline telephone carriers are required to report to the Commission network outages of a certain size and duration—those outages affecting the ability of at least 30,000 customers to make a call for a minimum of 30 minutes. Although the outage reports are required by the Commission, the information is reviewed primarily by the Network Reliability Steering Committee, or NRSC. The NRSC was created by ATIS for that specific role upon the recommendation of the NRIC.

The NRSC makes the outage information available to industry, in order to ensure continued network reliability, and so that future outages may be avoided. The creation of these industry mechanisms followed a number of highly publicized outages in the early 1990s, which had different root causes but were the result of a market failure: lack of information. Although the Commission has an outage reporting requirement, the information submitted by industry, in response to Section 63.100, is intended primarily for industry. Of the two recent outages mentioned above, only one was required to be reported under Section 63.100—the AT&T frame relay outage—whereas the Galaxy IV satellite paging failure was not (because there is an exemption in Section 63.100 for satellite systems). As a result, the Commission is looking into the need for a more comprehensive reporting requirement.

Both the AT&T and PanAmSat outages highlight how various systems can be affected by the failure of a single piece of hardware. However, communications networks are also designed to be fault-tolerant, robust and redundant, and there is no reason to believe that Y2K-related failures could lead to a chain reaction that could disable large parts of the nation's telecommunications networks.

Question 14. In the June 16 hearing of the House Subcommittee on Oversight, Committee on Ways and Means, the General Accounting Office (GAO) testified that telecommunications readiness was critical, yet the status of the industry is essentially unknown. What is your response to that observation? What's the current status?

Answer. We do not agree with the assessment of the General Accounting Office ("GAO") that the status of telecommunications Year 2000-readiness is unknown. For the convenience of the Committee, I am appending to my post-hearing responses a summary of how each of these different industries may be affected by the Year 2000 Problem and what industry and the FCC are doing to address these problems. Again, as I responded in several questions above, our current assessment of the telecommunications industry (i.e., in terms of inventory, assessment, remediation, testing, and integration efforts) remains relatively positive.

In addition, we have had several meetings with GAO in which we have provided brief summaries of the responses to our Year 2000 inquiry letters as well as summaries of the informational meetings and forums that the FCC's Bureaus have conducted.

Question 15. Much of the discussion of the Y2K impact on the telecommunications sector has focused on the steps that service providers are taking to ensure that their respective systems and networks are compliant, and that they will not experience major service disruptions. However, there are considerable Customer Premise Equipment, i.e., PBX machines, office LANs, and voice mail, with known problems. In other words the long distance carriers may be ready, but if the office telecommunications networks and devices are not, the call won't go through. Has FCC done anything to alert businesses and corporations to this potential problem?

Answer. As I stated in my response to Question 1, the Commission shares the concern about the Year 2000 effects on CPE that access the public switched telephone network. As part of its continuing outreach and awareness initiatives, the Commission intends to host a public forum on the effect of the Year 2000 Problem on CPE and other ancillary equipment and services. We expect to convene the public forum during October 1998. We should note, however, that we do not regulate these areas of the network.

Question 16. While one's telecommunications equipment suppliers and manufacturers may have contacted their customers and advised them of any potential risks, I understand that there is a large re-sale market for this equipment. To your knowledge, are the suppliers taking any steps to ensure that these secondary market customers are notified of potential Y2K problems with their equipment?

Answer. Yes, some are, but as one would expect, they are encountering difficulties stemming, frequently, from their inability to determine who the current owners of those systems are.

PREPARED STATEMENT OF A. GERARD ROTH

Chairman Bennett and members of the Committee, my name is Gerry Roth. I am responsible for GTE's Corporate Year 2000 Program Office, and I am here on behalf of the Telco Year 2000 Forum. The Forum commends the Committee for conducting this hearing, and I would like to submit the following written testimony on the purposes and activities of the Forum to address Year 2000 issues in the telecommunications industry

BACKGROUND

The Year 2000 issue is a worldwide concern, which has been identified by many industry experts as the largest single project that companies will have to face. Many aspects of technology will be affected including a variety of computer systems, hardware, operating environments and networks.

As the end of the 20th Century approaches, it is becoming more evident that the Year 2000 will cause problems for some systems due to the limitation of the date field on some "legacy" and other older systems. In a number of these older systems, the developers used a two-digit year field with the assumption that the century is nineteen (19). With the turn of the 21st century the need to differentiate between the 20th and 21st century (19 versus 20) will be required in some applications.

The Chief Information Officer (CIO) Forum sponsored by Bellcore has been considering the Year 2000 issue at its meetings for some time. The Telco Year 2000 Forum was created as an outgrowth of these Bellcore CIO Forum discussions. The Telco Year 2000 Forum was created to focus and share information on a common, industry wide issue: the potential impact of the Year 2000 on the telecommunication industry.

TELCO FORUM PARTICIPANTS

The Telco Year 2000 Forum was formed with participation from some of the largest U.S. telecommunication companies. The current participants include the following companies:

Ameritech Corporation
Bell Atlantic
BellSouth Telecommunications, Inc
Cincinnati Bell Telephone Company
GTE
SBC
Southern New England Telecommunications Corporation
US West Communications Group, Inc.

The Forum has also invited AT&T, MCI/WorldCom, SPRINT and USTA to be participants in the Forum activities. In addition, it has invited some of the major telecommunications equipment suppliers to attend the Forum meetings to discuss mutual concerns and issues.

The Forum acts as an informal working committee to address Year 2000 issues in the telecommunications industry. Its purpose is to share relevant Year 2000 information, and the discussions are focused exclusively on issues relating to the technical or operational aspects of the Year 2000 problem. The intent of this information sharing is to identify potentially common challenges and solutions to address Year 2000 issues and thereby facilitate and accelerate necessary responsive actions by each of the member companies.

A principal activity of the Forum is to pool and share testing resources for common network components and to perform network interoperability testing.

Although the companies share relevant Year 2000 information, each company is responsible for its own Year 2000 plan and activities. Each member company has a very detailed and company specific plan to address its particular Year 2000 issues.

TELCO FORUM STRUCTURE

The Forum meets approximately six times a year. Sub-groups are established to focus on some of the major issues in a more timely and efficient manner. At the present time there are sub-groups in place to address:

—Network issues
—Information technology issues
—Communications issues

The entire Forum and/or its sub-groups also participate in conference calls to address specific issues or concerns between its regularly scheduled meetings.

NETWORK INTEROPERABILITY TESTING INITIATIVE

A major initiative being undertaken by the Telco Year 2000 Forum is the Network Interoperability Testing Project. This intra-network testing initiative is a voluntary project, which is entirely funded by the member companies to test the network and various services for Year 2000 readiness. Its purpose is to verify the operation of a multi-vendor, multi-company environment.

The goals of the testing project are to:

—Minimize risk of network failures
—Minimize risk of service failures
—Test the functionality of date/time sensitive operations

The testing initiative is based on Bellcore's GR–2945 which has emerged as an industry standard for telecommunications products for the Year 2000 issue. The participating company laboratories are configured for Year 2000 Interoperability testing to include:

—Emergency services
—Basic, enhanced, and intelligent services
—Network management systems
—Data networks

Within these test configurations, a number of individual services such as 7-digit calls, 1+ 10 digit calls, operator-handled calls, 800 calls, etc. will be tested and documented. The test configurations will test the Year 2000 readiness of approximately 21 suppliers and 82 network elements and/or management systems. Collectively this equipment represents the suite of equipment commonly deployed in the network for Northern America.

The Forum has already contracted with a project manager and has concluded contract negotiations with an independent testing laboratory to validate and document the test results. Detailed schedules are being developed with the member company test laboratories and the equipment suppliers to test the Year 2000 ready releases.

It is anticipated that the testing will be conducted in the 3rd and 4th quarter of 1998.

Testing is being conducted in five separate "labs" established within our members' facilities. These test labs allow the Forum to test the interoperability and compatibility of the major North American suite of network and operational support equipment in a Year 2000 environment prior to nationwide deployment. Currently, the Forum expects to test 16 separate configurations of network elements and data transactions and 40 unique network management configurations. These test configurations are made up of 82 commonly used telecommunications products from 21 suppliers.

Actual network testing began on 6 July 1998 with the test of our first management configuration dealing with the interaction of operational support systems to discrete network elements. Data transport testing began on 13 July 1998. Testing of Network Element to Network Element configurations is expected to begin in August.

All tests to date have been successful, and active testing so far is proceeding on schedule. We anticipate completion of all tests by December 1998 with a final report in early January 1999.

In addition to this testing initiative, Forum participants' laboratories will be used to support some of the inter-network testing being performed by the Alliance for Telecommunications Industry Solutions (ATIS) through its National Test Committee (NTC). The co-chair of the NTC is also a Telco Forum participant working on the Interoperability Testing Initiative. This will help ensure that there is a linkage between the two testing initiatives, which are intended to be complementary. Additionally, the Telco Forum will be formally represented as a member of the ATIS National Test Committee. All companies participating in the Y2K Forum are also members of the ATIS. ATIS will be testing the internetworking aspects of the Public Switched Telephone Network (PSTN)—focusing on time-critical network events on 31 December–1 January to model and monitor potential network congestion, Year 2000 interactions with local number portability modifications, transmission of voice and data from local exchange to inter-exchange carriers, "800" number access, and network management and control.

The benefit of the interoperability testing approach is that it helps speed the deployment of Year 2000 ready products. It reduces the need for each company to test every aspect of every new release and permits each company to focus work efforts on its unique requirements to deploy Year 2000 ready equipment. As noted previously, the interoperability testing initiative is a completely self-funded, voluntary undertaking. It will supplement individual supplier testing and individual company testing of critical network elements and systems.

In addition to the major interoperability testing efforts of the Forum, some of the other on-going activities and accomplishments of the Forum are outlined below.

Sharing information regarding best/representative practices

This is the purpose and major activity of the Forum. The sharing of information on best/representative practices facilitates and accelerates responsive actions by each of the member companies. The sharing of information regarding the approach being used to take responsive action and/or test some of the "industry standard" systems permits individual companies to focus their resources on company unique systems.

Working with major equipment suppliers

The Forum has met with and/or contacted some major telecommunication equipment suppliers regarding their Year 2000 Ready Releases. It has worked with some of these suppliers to improve delivery dates and/or for an earlier testing date on some of their products. The Forum plans to continue to work with suppliers to address identified Year 2000 equipment issues.

Sharing information regarding network products

The network representatives on the Forum have developed an internal data set of suppliers' Year 2000 ready releases and their availability dates. This data set contains approximately 93 vendors and 470 network elements. The database is a valuable resource to help ensure that all participants are receiving and using consistent information regarding Year 2000 product release and availability dates.

Meeting with various government and industry groups

Forum participants have met with various government and industry groups to share the Forum's concept and benefits. It has been useful to demonstrate the cooperative efforts being undertaken by the industry to help minimize the risk of network or service failures. The Forum is currently a member of the President's Year

2000 Telecommunications Task Force, chaired by John Koskinen and Federal Communications Commission (FCC) Commissioner Michael Powell.

Starting discussions on contingency planning

Although the individual members are responsible for their own Year 2000 plan and activities, the Forum has recently started discussing the issue of contingency planning. Also, since GTE has a close affiliation with the Canadian telecommunications industry, it has been able to share some of the contingency planning concepts being used there. It is expected that the issue of contingency planning will be addressed in greater detail in the months ahead.

YEAR 2000 INFORMATION DISCLOSURE ACT

The Telco Year 2000 Forum supports the goals of the Administration's *Year 2000 Information Disclosure Act.* We believe that it is important—to our customers and to the public—to provide relevant information regarding the Year 2000 readiness of telecommunications equipment and the network. The proposed Act would help allay some concerns about the legal liability associated with the disclosure of Year 2000 Information. As such, it should help promote disclosure of Year 2000 information readiness information in a more timely fashion.

The Forum believes that the proposed Act will help foster cooperation and information sharing within the industry and across industry borders regarding the Year 2000 issue. In so far as the sharing of Year 2000 information is the primary purpose of the Telco Year 2000 Forum, it supports the objectives outlined in the *Year 2000 Information Disclosure Act.*

CONCLUSION

The Year 2000 issue represents a significant challenge to business, its customers, and the government. As noted at the outset, it is a matter of worldwide concern, which has been declared by many industry experts as the largest single project that companies will have to face. It requires cooperation within the telecommunications industry and across industry boundaries. It also presents an opportunity to work with others on a common challenge. The Telco Year 2000 Forum is a cooperative effort governed as a limited liability corporation actively working to address the Year 2000 issue in the telecommunications industry.

The members of the Telco Year 2000 Forum believe that this cooperative, voluntary effort will go a long way toward removing public anxiety over the Year 2000 status of the Public Switched Telephone Network (PSTN) in the United States. Despite the fact that this network cannot be 100 percent tested in advance of the Year 2000, we believe our individual and collective actions in Year 2000 remediation and subsequent test and validation provide a basis for continued confidence that the telephone and data networks will continue to operate and provide the outstanding services we have come to expect.

Mr. Chairman, I thank you for this opportunity to present this testimony on behalf of the Telco Year 2000 Forum.

RESPONSES OF A. GERARD ROTH TO QUESTIONS SUBMITTED BY CHAIRMAN BENNETT

Question 1. What percentage of the U.S. telecom industry is represented by the Telco Year 2000 Forum?

Answer. Current participants in the Telco Year 2000 Forum include the following companies: Ameritech Corporation, Bell Atlantic, BellSouth Telecommunications, Inc., Cincinnati Bell Telephone Company, GTE, SBC, Southern New England Telecommunications Corporation, and US West Communications Group, Inc. While it is impossible to provide a precise percentage of the telecom industry represented by these companies, one measure of industry representation is access lines served. Collectively these companies provide service for approximately 145 million access lines, a substantial majority of the switched access lines in the nation.

Question 2. We understand that the Telco Forum will be examining the emergency "911" system. What have you discovered in your assessment and testing to date?

Answer. The emergency "911" service interoperability testing has not yet begun. The testing of the various "911" configurations is planned to begin in late September. The Forum will be pleased provide the Committee information on this aspect of testing when it is completed.

Question 3. A major initiative being undertaken by the Telco Forum is the network interoperability-testing project. This intra-network testing initiative is a voluntary project. Its purpose is to verify the operation of a multi-vendor, multi-com-

pany environment. Although several of the regional Bell companies are participating, the long distance carriers are not.

—How do you account for such limited participation?

Answer. We cannot agree that there is "such limited participation" in the Forum. Most of the equipment used in the North American Public Switched Telephone Network—including equipment deployed by smaller, regional telephone companies—is represented through the participating local service companies. As you know, we have extended invitations to major long distance carriers as well as USTA. To date, USTA citing primarily logistical difficulties resulting from a large and diverse membership, has been unable to agree to certain confidentiality and information sharing guidelines required of all Forum members. These agreements are intended principally: (1) to prevent inappropriate use or disclosure of company proprietary material which has been made available to assist in Year 2000 remediation and testing; (2) to protect sensitive information provided by industry suppliers and testing services vendors which would otherwise be unknown to Forum members except for their cooperation on Year 2000. With respect to long distance carriers, we have been told by some of these carriers that it is simply a resource allocation issue. Also, as discussed above, long distance carriers are participating in ATIS testing and they anticipate that there will be considerable interaction and information sharing between ATIS and the Telco Forum. In any event, our invitation to those groups remains open.

—What are the pitfalls involved in such testing?

Answer. The Telco Forum has attempted to include those date-sensitive network elements and management systems that interact directly with the network and that are broadly deployed in North America. The testing does not—and cannot—include all deployed network elements and management systems or each combination thereof because of time and cost constraints. It should be noted, however, that the Forum's interoperability testing project is over and above the product-specific testing being performed by individual suppliers and operating telephone companies.

Also, the Telco Forum's testing efforts must be accompanied by other testing to insure inter-network performance. All of the Forum members, for example, are members of and active participants in the Alliance for Telecommunications Industry Solutions (ATIS). Importantly, some of the individual Forum member companies are providing their labs and lab personnel for the Year 2000 testing being performed by ATIS.

The benefits of testing are many while the pitfalls are few. Any failures found and fixed now only enhance, rather than distract from, the industry's overall readiness for Year 2000.

—Have industry-wide standards for testing been established?

Answer. The Telco Forum is using the Bellcore GR 2945 "Year 2000 Generic Requirements: Systems and Interfaces" as the basis for its interoperability testing project. As noted by Dr. Judith List in her testimony before the Senate Special Committee on the Year 2000 Technology Problem these generic requirements have evolved as important, de facto standards for Year 2000 on the Public Switched Telephone Network.

—How accurately will Telco's testing conditions predict actual conditions in the public network?

Answer. The Telco Year 2000 Forum is performing the tests in a number of separate labs provided by its members. The testing will involve the use of real equipment and systems in the test participants' laboratories rather than simulators. The test cases may also involve the use of select live data and live calls.

Because Forum members are continually deploying switch generic upgrades and major new equipment in their network infrastructure, upgrading network and management systems for the Year 2000 issue, while broader in scope, is essentially conducting business as usual. The test facilities being used in the Telco Forum's interoperability testing project are the same as those used by the participants for testing purposes before deploying switch generic upgrades or major equipment in the live network.

—How is your proposed testing different from that proposed by the Alliance for Telecommunications Industry Solutions' (ATIS) testing?

Answer. The testing being performed by the Telco Year 2000 Forum and the Alliance for Telecommunications Industry Solutions (ATIS) through its National Test Committee (NTC) is intentionally complementary. Furthermore, both bodies share membership and test laboratories. The Co-Chair of the NTC is also a Forum participant working on its interoperability testing initiative. Otherwise, the Telco Forum is exclusively Year 2000-focused, while ATIS has a broader industry-wide scope, which has been expanded further to include Year 2000 operational testing.

The focus of the Telco Forum's intra-network testing is on the interoperability and compatibility of the major network and operational support components in a Year 2000 environment and as they are configured by the operators of the network. The participating company laboratories are configured for interoperability testing of:

—Emergency services
—Basic, enhanced, and intelligent services
—Network management systems
—Data networks

Within these test configurations, a number of individual services such as 7 digit calls, 1+ 10 digit calls, operator-handled calls, 800 calls, etc. will also be tested and documented. The test configurations will test the Year 2000 readiness of approximately 21 suppliers and 82 network elements and/or management systems. Collectively, this equipment represents the suite of equipment most commonly deployed in the network for North America.

Once that has been accomplished, the inter-network testing planned by ATIS will determine the extent to which the Public Switched Telephone Network operations, under operational load as the millennium date change occurs, continue as normal. ATIS testing will thus focus on time critical events on 31 December–1 January to model and monitor potential network congestion, Year 2000 interactions with local number portability modifications, transmission of voice and data from local exchange to inter exchange carriers, 800 number access, and network management issues.

Lastly, individual company testing and operational performance verification after the January 2000 transition will monitor and analyze any potential ″gradual degradation″ due to subtle system dysfunction from latent Year 2000 impacts.

—Wouldn't it be more efficient for the Telco Forum and ATIS to join forces?

Answer. In fact, we have "joined forces" in terms of the overall architecture of domestic telecommunications network testing. ATIS testing will use aspects of the Telco Forum's efforts. However, each sub-component of the overall testing effort is being handled by those with the greatest knowledge of the equipment and services under review. The testing being performed by the Telco Year 2000 Forum and ATIS through its National Test Committee (NTC) are both necessary and complementary. As noted above, the Co-Chair of the NTC is also a Forum participant working on its interoperability testing initiative. The Forum also has formed a sub-committee to formalize its linkages with the ATIS Year 2000 testing.

Several of the individual Forum member companies are providing their labs and lab personnel for the Year 2000 testing being performed by the ATIS and, all of the Forum members are participants in ATIS.

The Telco Year 2000 Forum started to work on its interoperability testing initiative in the early fall of 1997 with the issuance of a Request for Proposal for the project. The test plans and test cases for most of the testing have been prepared and actual testing has already begun. It is expected that the testing will be completed in December 1998 with a final report in early January 1999. This would be the wrong time to start restructuring the testing or testing administration.

Finally, much of testing being planned by ATIS was in the Telco Year 2000 Forum's original RFP for the interoperability testing work. It was removed because ATIS took the lead and was better positioned to handle this aspect of the testing work effort. Since the actual ATIS testing is planned to be initiated in January 1999, the Forum believes that from a practical standpoint the industry has joined forces in its efforts to address the Year 2000 issue.

Question 4. GTE currently offers its customers a wide range of services: local and long-distance switched voice services; wireless voice and data services; Internet and other data communications services; as well as paging services.

—What are the specific Year 2000 issues and potential impacts to those services?

Answer. GTE believes, as does the other major telecommunication carriers, the United States Public Switched Telephone Network (″PSTN″) will continue to operate with no major service disruptions due to Year 2000 issues. Specific concerns do arise with respect to supplier continuity and international response.

Telecommunication companies depend heavily on their suppliers actually delivering on schedule the Y2K solutions to which they have committed. These companies also depend upon their suppliers' ability to sustain technical support and performance through the Year 2000 transition. To address this concern, GTE has established a Supplier Management Program, headed by a vice president in GTE's corporate Year 2000 Program Management Office. This unit tracks the thousands of products acquired by GTE and promotes the timely delivery of Year 2000 compliant versions. This organization also has the responsibility, and authority, to negotiate appropriate, Year 2000 compliance terms and conditions in contracts with its suppli-

ers, and is responsible for assessing the quality and completeness of Year 2000 testing of third-party supplier products.

Otherwise, while the U.S. and Canadian telecommunications industries are working closely to address and test Y2K readiness, the international response to date has been inconsistent across the industry and countries. Because of the global nature of the telecommunications business and its customers, we must strive to ensure Y2K awareness and enable full international network interoperability assurance. Thus, GTE has been working through the Telco Year 2000 Forum and otherwise (e.g. the Canadian Telco Y2K Forum and the ITU Y2K sub-group) to promote Y2K information sharing and, possibly, interoperability testing on an international basis.

—What are the Year 2000 issues and potential impacts that threaten the proper functioning of the business systems that support those services?

Answer. Because the operation, administration and maintenance systems of telecommunications carriers do include date-sensitive information for functions such as order-entry, billing, network management, and administration, GTE prioritized and inventoried its major support systems for Y2K conversion. Based on our planned schedule, GTE currently expects its key legacy and support systems code to have been Y2K converted (if necessary) and returned to production by January 1, 1999. Full system enterprise testing is presently scheduled to be completed by June 30, 1999.

—What steps should your users and customers be taking to ensure that their services are not disrupted?

Answer. Residential Customers: Because most residential telephones do not process date-sensitive information to enable basic telephone service, residential customers will generally not be required to take any steps to ensure uninterrupted service. However, residential customers having more advanced equipment such as answering machines, facsimile equipment, modems, etc., should contact their equipment manufacturers regarding the Y2K compliance status of their products. While the potential exists for these products to be impacted by the Year 2000 (such as date displays and time stamps), it is unlikely to prevent placing or receiving telephone calls.

Private Network Customers: Customers that operate more complex premise equipment interfacing with the PSTN should, as part of their Year 2000 compliance programs, conduct an inventory of that equipment and work with their service providers and equipment suppliers to determine the Y2K compliance status of their products and systems.

Question 5. Many federal, state, and local government agencies, private businesses, and other entities operate their own networks.

—Do you have a sense of whether private versus public networks are being addressed for Y2K problems?

Answer. To the extent this question refers to testing efforts by the Forum, mainstream equipment is used in both public and private networks. Therefore, any Telco Year 2000 Forum testing and other Year 2000 work with equipment vendors would, necessarily, benefit the owners of private networks.

—If a private network is not Y2K ready, could the interface of a non-compliant private network result in the degradation of public telephone service?

Answer. The Forum does not believe that the interface of a private network would pose any greater risk to the public telephone service network than it does in today's environment. Obviously, a company relying on private non-compliant network might need to secure an alternative means of access to the public telephone network.

—Will extensive use of the Internet in any way degrade public telephone service?

Answer. The Forum does not believe that the use of the Internet would pose any greater risk to the public telephone network than it does in today's environment. The network has various management systems in place to deal with traffic congestion. Some of these systems will be tested as part of the Telco Year 2000 Forum's and ATIS complementary testing efforts.

Question 6. I see that the Telco Forum supports the "goals" of the President's Year 2000 Information Disclosure Act and believes it will help foster cooperation and information sharing. Your words sound skeptical. Do you believe it will really result in better information disclosure?

Answer. We believe that the enactment of legislation reducing liability concerns for disclosure will enhance the free flow of testing and product readiness information. The President's Year 2000 Information Disclosure Act is clearly helpful in this regard and would result in better information disclosure.

—Are there other deterrents to disclosure?

Answer. Yes, ordinary commercial concerns, such as customer relations and competitive issues, also play a large role in disclosure decisions. In addition, disclosure

activities are to some extent impacted by resource constraints in companies, with many companies focusing on their own internal remediation efforts.

—What more can be done to encourage disclosure?

Answer. In addition to the legislative efforts above, it would be helpful to have disclosure related activities made more efficient and effective. For example, a uniform approach to information gathering by Federal and State authorities would allow companies on remediation and would promote disclosure in a useful and consistent fashion.

PREPARED STATEMENT OF SENATOR GORDON SMITH

Thank you Mr. Chairman.

I would like to thank all the distinguished witnesses before us today for taking the time to help us address the challenges facing telecommunications as we enter the year 2000.

Today's hearing is extremely important because our lives have become intertwined with technology that runs our phones, banks, electric power and way of life.

Did you know that at this very instant many long distance carriers have not yet determined how to solve billings problems that affect the amount you are charged for your long distance calls? I caution you to stay off the phone at the stroke of midnight at the turn of the century unless you are certain the computer bug has been addressed by your carrier. You may be charged for talking on the phone for over a century.

I make light of an enormous challenge the telecommunications industry is facing.

I remember when a satellite stopped transmitting information earlier this year, affecting thousands of people who relied on telecommunications technology. Many Oregonians complained that their pagers, cell phones and the local ATM's were no longer working. Little did they know that the satellite that many of their daily activities had changed its usual orbit. Much like this incident, imagine how our daily lives would be altered if the chips in our satellites aren't ready for the year 2000.

It is for this reason that we are here to discuss ways to prevent this computer problem from bringing our nation to a halt and I look forward to hearing about progress being made to avoid that end.

In talking to experts in the telecommunications field, I have learned that the dial tone will most likely not be affected by the arrival of the new millennium. We have received several calls from large and small businesses who are trying to run tests on their networks and are unable to. So my question to the panel is, what kind of network components are susceptible to year 2000 errors? Subsequently, what are you doing to address these problems? How will these potential problems affect the speed of placing phone calls or making internet connections?

Are equipment vendors supplying networks with the most recent software that will protect them from any Year 2000 problems?

I'm also curious about how your efforts as an industry are being coordinated. I understand the Federal Communications Commission has been studying this issue, but can the network service providers rely on the FCC for help?

As a member of the Senate Foreign Relations Committee, I am very concerned that we will not be able to maintain communication with other countries across the border and around the world. If we are cut off from communicating with other nations, issues such as national security, trade, information exchange and financial services will become the headliners of our society. I'm hopeful that someone is currently focusing on how to coordinate our systems with foreign countries.

If there is no primary point of contact for the telecommunications industry, I hope this hearing will provide direction for the entire telecommunications industry so that all interested parties will know where to turn for help.

I also understand that some legislation has been recently circulated by the President regarding the "Year 2000 Information Disclosing Act" that will offer legal protection to those who share information on Year 2000 fixes, service opportunities and products. I understand that the telecommunications industry was actively involved in the negotiations with John Koskinen and the Office of the President on this legislation, and I would be interested in our panel's comments on this subject.

Again, thank you all for coming today. I look forward to learning more about the specific challenges you are facing and specific steps you are taking to meet them.

Thank you Mr. Chairman.

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

STATEMENT FROM HEWLETT-PACKARD MEDICAL PRODUCTS GROUP

RATIONALE FOR HEWLETT-PACKARD STATEMENT

Hewlett-Packard Company is a leading global provider of computing, Internet and intranet solutions, services and communications products, and measurement solutions, all of which are recognized for excellence in quality and support. HP Medical Products Group (HP Medical) is one of the world's largest suppliers of medical devices. HP is pleased to have been invited to contribute to the Congressional deliberations on the healthcare industry's readiness for the Year 2000, specifically related to Y2K issues in medical devices. As the clock continues to advances towards midnight, December 31, 1999, the sense of urgency grows, particularly for medical devices for which date processing could represent a serious threat to the safety of patients.

During the last year, HP Medical has worked closely with the FDA, the Veterans Health Administration of the Department of Veterans Affairs and the Department of Defense to better understand their needs, requirements and issues related to Y2K. It is our position that the more information we can make available to our customers about Y2K issues in our medical devices, the better we can help them prepare for the millenium.

HP Medical's primary concern with the Y2K issue is patient safety. We were invited to submit this statement because of our proactive and cooperative approach to helping our healthcare customers make a smooth transition of their HP medical equipment to Y2K-compliant status. HP Medical has been actively addressing Y2K issues, allocating dedicated R&D resources to perform in-depth assessment and/or testing of our products. We are also actively communicating with our customers to inform them of Y2K issues related to HP medical products.

HP'S COMMITMENT TO MEDICAL CUSTOMERS

HP is making the following commitments regarding Year 2000 compliance for our medical products:

—All HP medical products that are currently shipping, or will ship in the future are already Year 2000 compliant, will be certified as Year 2000 compliant as of their next revision, or at the very latest, will be certified by the end of 1998. Any upgrades or modifications required will be made available to our customers at no cost.

—All HP medical products that are no longer in production, but are still eligible for HP support as of January 1, 2000 are being evaluated for Year 2000 compliance. In some cases, a simple "workaround" solution (such as a manual reset) may be identified. In the cases of products for which an acceptable workaround solution cannot be identified, HP will make available an upgrade or upgrade path. In some cases, there may be a cost associated with the upgrade or upgrade path.

—HP medical products that are obsolete and are no longer eligible for HP support as of January 1, 2000 will not be brought into compliance by upgrades or modifications. In some cases, products may not be affected because there are no date processing requirements. HP will recommend replacement products for those non-compliant products that are beyond their support life, as well as providing risk assessment information for those obsolete products that contain date processing functions.

TESTING MUST BE THOROUGH AND COMPLETE

Any Y2K program must be based on evaluation and testing of the date processing functions of equipment and systems. When patient safety is at stake, care must be given to ensure that the testing is adequate and robust. HP Medical believes that

it is not enough to set the date in the device to December 31, 1999 and run through the normal operating performance. As a result, we have implemented a two-level testing and Y2K certification process for all current products.

The testing protocol adopted by Hewlett-Packard Company on a company-wide basis involves testing of all current products for Year 2000 compliance based on multiple dates and functional sequences (see Attachment A). This functional testing takes into account leap year calculations, as well as the transition between December 31, 2000 and January 1, 2001.

In addition to the protocol above, HP Medical is also testing all current products by performing a thorough review of software code, carried out by a qualified HP medical device engineer. This additional level of testing helps ensure that performance will not be affected by dates embedded in the software that are not visibly apparent in the normal operation of the devices.

This two-level testing and Y2K compliance certification is consistent with the FDA's new Quality System Regulation. To date, HP Medical has completed testing of 97 percent of all current products.

OBSOLETE PRODUCTS ARE NOT IMMUNE

In the healthcare environment, it is not unusual for medical devices to be in use for ten, fifteen, even twenty years—long after the manufacturer has declared the product obsolete and discontinued support on the product. For example, a patient monitor originally purchased for the Intensive Care Unit could still be in use in the Emergency Department twenty years after its purchase.

HP is concerned about obsolete equipment that may still be in use throughout the healthcare system, and we are taking steps to ensure that our customers are aware of which HP medical devices are out of their support life and will not be brought into Y2K compliance by HP. In addition, we intend to help our customers understand potential patient safety risks that may be present if obsolete devices continue to be used after the rollover to the Year 2000.

As a result of this concern, HP Medical is in the process of performing risk assessments on obsolete devices for which the Y2K issue could pose a threat to patient safety. As assessments are completed, HP will make the results available to our customers, via our Y2K website, along with attractive financial and support programs to help our customers upgrade or trade-in those products that are deemed non-compliant. HP expects to complete all necessary risk assessments and make the results available to our customers no later than June 1999.

COMMUNICATION IS KEY

HP believes that communication and access to information is absolutely critical to helping our customers ensure that their HP medical devices function properly during the transition to the millenium. We have implemented a number of communications programs to notify customers of the compliance status of their products, and to make it easy for them to get information from HP.

HP has initiated the following communications programs to help our customers understand Y2K compliance of their installed HP products:

—A comprehensive worldwide website which includes compliance status, required actions and recommendations on all HP medical products, as well as hotlinks to other Y2K information sources, such as the FDA Y2K site (see the worldwide web at <http://www.hp.com/go/healthcare2000>);

—Response to all customer inquiries on Y2K status by providing complete listings of testing status, compliance status, actions and recommendations, as well as Y2K warranty information;

—A process in the United States for responding to customer inquiries about HP medical products within five working days;

—Mailing scheduled for August 1998 to 7,000 U.S. healthcare locations to make them aware of our Y2K website;

—A second mailing scheduled for November 1998;

—Attractive financial and support programs to help customers to upgrade or trade-in non-compliant HP medical products.

Similar programs are being undertaken by HP Medical's geographic operations outside the United States.

We believe that full cooperation and open communication between device manufacturers and healthcare customers is in the best interest of our ultimate customer—the patient. It is our belief that as a responsible supplier, HP must engage in an open dialogue with our customers about Y2K issues, rather than approaching this issue defensively.

HP commends President Clinton's proposal to seek legislation that will help protect businesses that proactively address Y2K issues with their customers from future costly litigation arising from Y2K issues. We view the President's proposal as a good first step toward dealing with the broader Y2K litigation issues that may be discouraging the business community from taking a more aggressive approach to the Y2K problem in a number of sectors of the U.S. economy.

HP also commends customers such as the Veterans Health Administration, the Department of Defense, and Columbia/HCA for their approach to Y2K issues with their suppliers. These customers have engaged key suppliers like HP with a partnership approach to resolving Y2K issues in their healthcare organizations, rather than addressing suppliers in an adversarial manner. HP welcomes this open dialogue, and has engaged in face-to-face meetings with several customers to help them understand firsthand the vigor and breadth of our Y2K testing and compliance programs.

IN CLOSING

HP Medical Products Group is concerned and proactive in addressing and communicating Y2K issues. HP believes that there are three essential elements to ensuring that the healthcare industry will be fully prepared to face the Year 2000. Those elements are:

—Y2K compliance programs should include thorough and robust testing of the functional performance of medical devices for which date processing could represent a potential patient safety issue. Ideally, this testing should include detailed review of software code to identify embedded date processing.

—Full testing protocol and compliance status information should be readily available to healthcare customers.

—Congress should take steps to encourage open dialogue between manufacturers and customers in all sectors of the U.S. economy.

It is our belief that if medical device manufacturers and healthcare providers collaborate and cooperate to identify and resolve Y2K issues, the public will be able to approach the millenium with confidence in their safety should they require medical attention.

ATTACHMENT A.—HP YEAR 2000 COMPLIANCE DEFINITION

YEAR 2000 COMPLIANCE DEFINITION

If an HP product processes date data, then it is considered to be Certifiably Year 2000 Compliant if the following conditions are met:

1. It processes date data accurately from, into and between the twentieth and twenty-first centuries. This includes, but is not limited to, calculating, comparing and sequencing dates, including leap year calculations, when used in accordance with its product documentation, and provided all other products used in combination with the product properly exchange data with it.

2. It has successfully passed each test case listed in Table 1, and the product's test suite permanently incorporates Table 1's test cases and conditions.

3. It has successfully passed a review based on the checklist given in Table 2.

TABLE 1.—MANDATORY TEST CASES FOR A PRODUCT TO BE CERTIFIABLY YEAR 2000 COMPLIANT

Date data [1]	Testing criteria
Dec. 31, 1998 to Jan. 1, 1999	Test for border line (beginning and ending of a year) for year prior to year 2000: System rollover in both powered-up and powered-down states, or Program rollover in both executing and non-executing states.
Sept. 9, 1999 to Sept. 10, 1999	Tests related to 9–9–99: System rollover in both powered-up and powered-down states. System date can be set to before date. System re-initializes from cold start on before date, or Program rollover in both executing and non-executing states. Program retrieves/accepts before date in executing state. Program re-initializes from non-executing state on before date.

TABLE 1.—MANDATORY TEST CASES FOR A PRODUCT TO BE CERTIFIABLY YEAR 2000 COMPLIANT—Continued

Date data [1]	Testing criteria
Dec. 31, 1999 to Jan. 1, 2000	Test for critical transition of 1999 to 2000: System rollover in both powered-up and powered-down states. System date can be set to both before and after dates. System re-initializes from cold start on both before and after dates, or Program rollover in both executing and non-executing states. Program retrieves/accepts both before and after dates in executing state. Program re-initializes from non-executing state on both before and after dates.
Feb. 28, 2000 to Feb. 29, 2000	Test to verify year 2000 is identified as a leap year: System rollover in both powered-up and powered-down states. System date can be set to after date. System re-initializes from cold start on after date, or Program rollover in both executing and non-executing states. Program retrieves/accepts after date in executing state. Program re-initializes from non-executing state on after dates.
Feb. 29, 2000 to Mar. 1, 2000	Another Year 2000 leap year test: System rollover in both powered-up and powered-down states, or Program rollover in both executing and non-executing states.
Dec. 31, 2000 to Jan. 1, 2001	Test for transition from 12–31-OO to 1–1–1: System rollover in both powered-up and powered-down states, or Program rollover in both executing and non-executing states.

[1] Testing is conducted in this range of dates.

TABLE 2: MANDATORY CHECKLIST FOR A PRODUCT TO BE CERTIFIABLY YEAR 2000 COMPLIANT

Components	Specifics
Basics	1. Data Structures Within the Product: a. Database Structure. b. File System Structure. c. Holding or Working fields. 2. Date Manipulation Routines. 3. Called System Intrinsics. 4. Date Comparison Routines. 5. Date Fields on Reports.
Module Interfaces; Internal Date Data Exchanges	6. Data Structures for Interfaces Inbound to each Module. 7. Data Structures for Interfaces Outbound from each Module.
Product Interfaces; External Date Data Exchanges ...	8. Data Structures for Interfaces Inbound to the Product. 9. Data Structures for Interfaces Outbound from the Product.
Product Environment	10. Third Party Utilities or tools used by/with the Product. 11. Date Logic Embedded in the JCL or Run Logic of the Product.

STATEMENT OF SANDIA NATIONAL LABORATORIES

We are pleased to be given this opportunity to submit some thoughts to the committee about how the Year 2000 problem might impact telecommunications and to recommend some actions that might lessen the severity of that impact.

Sandia is the DOE laboratory responsible for the ordnance engineering for all U.S. nuclear weapons. Our responsibilities comprise the design, certification, and assessment of the non-nuclear subsystems of nuclear weapons, including arming, fuzing, and firing; safety, security, reliability, and use-control; issues associated with the production and dismantlement of nuclear weapons; and surveillance and support of weapons in stockpile. We also perform substantial work in programs that are closely associated with nuclear weapon research and development, including nuclear intelligence, nonproliferation, and treaty verification technologies.

We are, however, a multi-mission laboratory. Ten percent of our work supports DOE's responsibilities for environmental remediation and waste management, and another ten percent supports Department missions in energy science, research, and development. When appropriate, we also perform work for other government agencies, particularly the Department of Defense, in programs where our unique capabilities, built to support DOE's Defense Programs responsibilities, can be of value. Increasingly, we are being called on to support other federal agencies, such as the

FBI, the National Institutes of Justice, NIST, and NASA, where we have areas of expertise that can be of assistance.

The surety of the nation's telecommunications infrastructure is absolutely essential for our national security. All businesses and essential services require telecommunication for their operation. The banking and finance sector exchanges billions of dollars a day across telecommunications links. The ATM machine at the mall requires operating phone lines to validate its transactions, as do the credit card readers at the department store and the corner gas station. And of course the whole spectrum of emergency response organizations, from the National Guard to FEMA to police to hospitals, requires reliable telecommunications to do their job. The Y2K crisis may require the assistance of many of these organizations, and an additional Y2K-induced failure of the telecommunications infrastructure during an emergency would be catastrophic.

We've divided this document into seven parts: Public telephone networks, data networks, satellites, international telecommunications, dependencies of telecommunications on other infrastructures, other issues, and finally recommendations. In each section, we discuss potential Y2K vulnerabilities and mitigating actions that could either prevent a failure or gracefully handle failures when they occur.

1. PUBLIC TELEPHONE NETWORKS

Local phone companies

Over 1200 local telephone companies [1] provide the primary customer interface to the national telecommunications infrastructure. These companies provide access not only to voice telephone service, but also to the Internet for dialup users. Most of the larger local companies, and certainly the Regional Bell Operating Companies (RBOC's), are actively working Y2K issues.

These companies use switches and equipment made by a variety of manufacturers such as Lucent, Nortel, and Siemens. All of these manufacturers have made Y2K compliant upgrades to their major products available, and most of the larger local phone companies are upgrading or have already upgraded. While there is always the possibility for hidden failures, the sensitivities in telephone switch gear that have been located so far have had to do not with basic functionality but with administration, management, and maintenance issues, as Dr. Judy List of Bellcore has already testified.[2] Such failures do not affect dial tone, but can interfere with proper billing of call time, for example. Thus, in older equipment that has not been upgraded, Y2K failures are not likely to cause the local telephone system to go down, but they may cause billing and revenue problems for companies that don't upgrade. This may be a bigger problem for smaller local phone companies because they are more cash-flow sensitive, and also because, being resource-limited, they are less likely to upgrade their equipment in the first place.

Again, we cannot be certain that basic system functionality will not be compromised, because the variety of equipment that is critical to call processing is too great and it has not all been analyzed as of today (July 1998). The only way to be absolutely certain is with a full-up system test, and that is impossible with the telephone network.[2] The telephone network cannot be taken offline for testing, and even if it could, it contains embedded processors for which it will not always be possible to manually roll the date forward. Partial testing may be an option for certain critical nodes, but anything less than a full system test is not guaranteed to catch the more insidious bugs that are the whole reason testing is necessary. Absent tests, the only alternative may be to do as much preventative repair as possible and have well-oiled backup systems and well-trained repair crews in place on January 1, 2000.

Major trunk carriers

Major trunk carriers such as Sprint, Worldcom, and AT&T carry telephone traffic and data between the local phone companies. The failure of even one of these carriers would be catastrophic. Because of their interoperation agreements, a carrier experiencing difficulty can route its traffic through the others. However, if a carrier fails completely, the impact of all of its traffic suddenly being routed to the others might cause an overload which, if not controlled quickly, could conceivably bring down the others as well.

All the major carriers are spending millions of dollars working the Y2K issue, and are deeply aware of the implications of failure. So far, most of their equipment has the same Y2K issues as we discussed above: it is less likely to affect basic service than administration, management, and maintenance. Because of this and because all of these companies are large and well-capitalized, total failure of the major trunk carriers due to direct Y2K effects does not seem very likely.

However, we do find it plausible that Y2K could cause failure of the telephone system through another mechanism: loss of electric power. (More on this below.)

Wireless

Cellular phones, PCS phones, pagers, and other wireless mechanisms that interface to the public telephone network must be examined for their own Y2K vulnerabilities at the level of the equipment itself, the transmitters/receivers (cells) and the interface points to the network. We presume that the cellular providers are working the issue, but we do not have any data at this point.

Local emergency and public safety organizations, such as police, fire and EMS need to make sure that their wireless systems will operate. We don't know their current status, but suspect that many may be unaware of their Y2K vulnerabilities. These critical first responder organizations need to be educated quickly and get their equipment upgraded where appropriate.

Amateur radio operators must also examine their Y2K status. Hams are frequently the only means of communication after a disaster, so it is extremely imporant that their equipment operate correctly. The American Radio Relay League and AMSAT, the Ham satellite organization, have reported to us that most Ham equipment, as well as their satellites, are not Y2K sensitive, and that they are updating software that is. "One of amateur radio's strengths is our adaptability," one of the members of AMSAT told us. We find this encouraging, and believe that Hams will be ready if there is a telecommunications emergency.

Customer-owned equipment

Much of the telephone system is customer-owned equipment installed at the customer's premises. PBX systems, ISDN phones, answering machines, voicemail systems, etc. are produced by myriad vendors and largely are not under the control of the phone companies. Most of this equipment is installed in businesses. While many vendors have produced Y2K upgrades to their equipment, it is probable that a large fraction of their customers have not upgraded, either because they are unaware of the Y2K vulnerabilities in the equipment or because they cannot afford to upgrade.

If this equipment goes down because of Y2K problems, companies who own it and depend on it will certainly be at risk. But Y2K rarely impacts a business in isolation; if a business goes down because of Y2K and it's a critical customer or supplier of other businesses, it may take the other businesses down with it, even if they are Y2K compliant.

Small-to-medium enterprises (SME's) are likely to be hardest hit by this, because large companies will upgrade and can absorb the loss of some trading partners. Loss of telecom and Internet equipment is one of the most serious threats facing SMEs because this equipment is at least as mission-critical as their computers and it is probably more sensitive to Y2K. Encouraging SMEs to upgrade and encouraging vendors to provide upgrades to SMEs at favorable terms should be strongly considered. Because of the deeply interconnected nature of systems vulnerable to Y2K failure, virtually all businesses must be compliant or none are compliant.

911 call processing in public safety organizations must be evaluated and upgraded where necessary. Because 911 processing usually involves special equipment and is date-sensitive, it needs to be checked carefully.

Indirect effects

Widespread outages in any of the infrastructures as a result of Y2K, or widespread receipt of incorrect bills, could result in thousands of complaint phone calls, which tie up the system. Procedures are available to ensure that these calls do not block emergency users, and the telecom system operators need to be prepared to invoke them if necessary.

2. DATA NETWORKS

The Internet

Five years ago, the impact of losing the Internet would have been minimal. Most users of the Internet were academic and government organizations, and the loss of the Internet would have been a nuisance at worst. Today, however, the Internet has become a business tool almost as essential as the telephone. Many large companies today depend on email and the Internet's ability to quickly move large quantities of information between company sites. Some companies such as Yahoo! and amazon.com derive virtually all their revenues through their Internet services. The 1997 10–K filing of amazon.com states:

> Amazon.com has grown rapidly since first opening its Web site in July 1995. Through December 31, 1997, the Company had sales of more than

> $164 million to approximately 1.5 million customer accounts in over 150 countries.

The mail order company Land's End now takes orders over the Internet. Mike Smith, their president, states in their annual report:

> One area we will be spending more resources on is the Internet. We feel the Internet could generate significant sales in the future and will be investing accordingly. Obviously, the sooner this medium takes off, the faster our payback on this investment.

Besides the Internet-based merchants and advertisers, there are also thousands of Internet Service Providers (ISPs) that exist solely to connect customers to the Internet. The Internet has become an extremely important engine of commerce. The loss of the Internet would certainly have major economic consequences if it happened today, and the consequences will be even greater on January 1, 2000, given the continued exponential growth of the Internet between now and then.

But the Internet is also a social phenomenon. It began as a convenient mechanism to allow computers to communicate. Today, it is an essential mechanism to allow people to communicate. Continuing the quote from amazon.com's 10–K filing:

> Amazon.com strives to offer an online shopping experience that involves discovery and fulfillment for its customers. The Company believes that the sale of books and other products and services over the Web can offer attractive benefits to consumers, including, without limitation, enhanced selection, convenience, ease-of-use, competitive pricing, depth of content and information and personalization. Customers entering the Amazon.com Web site can, in addition to ordering books and other products, purchase gift certificates, conduct targeted searches, browse highlighted selections, best-sellers and other features, search for books by subject category, read and post reviews, register for personalized services, participate in promotions and check order status. The key components of Amazon.com's offerings include browsing, searching, reviews and content, online community, recommendations and personalization, a gift center and an out-of-print book service.

This description hints at what the Internet is becoming: an information mall; a centralized collection of information-related services upon which people are learning to depend. It combines the telephone, fax machine, television, and radio into a single two-way information appliance in which the whole is greater than the sum of its parts. This sounds like hyperbole, but the bottom line is that the Internet is becoming an essential component of people's lives. The Internet is a critical infrastructure, the surety of which must be maintained both domestically and internationally.

The Internet is not centrally controlled or regulated. It is largely governed by loose cooperation among its major stakeholders, and by some informal policy-making and engineering committees. The self-governing aspect of the Internet is one of its great strengths, but it makes it difficult to study its vulnerabilities in detail or to mandate remedial actions.

The Internet is heavily dependent on the public telephone networks, especially the major trunk carriers. If they go down, the Internet as we know it goes down too. The Internet is also dependent on the other two pieces of the public telephone system: local phone companies and customer-owned equipment. Local phone companies provide dialup service to millions of individuals who access the Internet from home. They also frequently provide connectivity for the lowest-tier ISPs and for businesses that connect at higher bandwidths. (Even when they are not the connectivity provider in name, local phone companies frequently own the physical cable or fiber connection which has been leased by another provider and resold to the ISP or end customer.) Therefore, if local phone companies go out, they won't take down the whole Internet the way the major trunk carriers might, but they will create islands of Internet disconnection. In areas served by Y2K-affected local phone companies, virtually no one may be able to connect to the Internet.

ISPs and Network Access Points (NAPs) must themselves have Y2K-compliant equipment and like the small phone companies, the smaller ones may be less likely to upgrade. ISP facilities also need to have back-up diesel generators to cope with power failures. Today, ISPs do not routinely install back-up generators the way local telephone central offices do.

Most of the Internet actually resides inside corporate Local Area Networks (LANs) that are dependent on privately owned equipment. If this equipment is not upgraded for Y2K it may fail and not only disable a business' connection to the "main" Internet, but take down the corporate LAN as well. Again, the result is serious.

Hundreds of people lose access to the Internet, a business potentially grinds to a halt, and its trading partners lose a valuable customer or supplier.

There are other pieces of the Internet that have no counterpart in the telephone system, and which are critical to the Internet's operation. The Domain Name Service (DNS) system comes to mind immediately. If DNS is taken out by Y2K, the Internet becomes unusable. In principle, it's a single point of failure. One master DNS machine controls the whole system, and DNS tampering has taken down the Internet in the past. In practice, DNS is probably more vulnerable to terrorists and hackers than to Y2K. The systems are largely Unix-based and so are unlikely to experience Y2K bugs, and new servers can be switched in quickly if one fails. As long as the DNS servers are adequately protected by backup electric power (not just battery-based UPS systems, but generators with many days' capacity), DNS is not likely to experience long-duration outages due to Y2K.

Specialized routers, bridges, concentrators, etc. are also used for the Internet but not for the telephone system. All these pieces of equipment must be checked and upgraded where necessary, and again, the larger providers are more likely to have repaired their vulnerabilities than the small players are. Provided the phone system remains operational, the Internet will likely stay operational with localized outages. If there are localized outages of the phone system in addition to outages in the Internet infrastructure proper, the problem could be much worse. Getting the system back online might then take much longer because problems that are the fault of the Internet equipment could be blamed on the phone system, and only after the phone system is back online would it be possible to fix the Internet problems.

Other data networks

Almost all other data networks such as the Virtual Private Networks used by private companies and governments rely on leased capacity from the public telephone network, and they die if the telephone network dies. Such networks may be even more critical to the nation's security and economic health than the Internet simply because they have been in use longer. Once again, upgrades to customer-owned equipment are very important for maintaining these networks.

3. SATELLITES

Satellites are vitally important to the world's telecommunications capabilities. Although there is a trend to move two-way telecommunications away from high-orbit satellites and onto terrestrial cable, fiber, and new low-orbit satellites (because of the time delay inherent in high-orbit satellites), they are all, nevertheless, still important. Even though many satellites like GPS, sensing, military and others are not involved with telecommunications per se, they all need to be evaluated for Y2K vulnerabilities.

Three aspects of satellite systems are potentially vulnerable to Y2K: platforms, payloads, and ground stations. Potential Y2K vulnerabilities exist in all three places. A failure in the platform may result in decreased orbital control, for example. In extreme cases it could cause the satellite to drift so much it would have to use a substantial amount of fuel to return to station, thus dramatically decreasing its lifespan. A failure in the payload may result in loss of service. A failure in the ground station may result in either loss of control or loss of service.

The satellite platforms frequently contain older embedded processors that may contain Y2K vulnerabilities. We have heard that the satellite manufacturers have certified the platforms as Y2K compliant, but as Senator Bennett has said, we should not accept the first "comfort letter" from the manufacturers. More investigation should be done. The payloads vary tremendously and must be examined case-by-case. If hardware Y2K vulnerabilities are found in the satellite platforms or payloads, they will be virtually impossible to repair. We do know something about the ground control stations. Many ground control stations use 1970s vintage mainframe technology and almost certainly will have problems. There are a limited number of these stations; their use is shared among the satellite owners and prioritized according to the criticality of the satellite. If several satellites have station-keeping problems simultaneously, the wait to use the control stations will be long. If the wait is too long, a satellite can drift away and become temporarily lost and may have to be located again by radar. Signal uplink/downlink ground stations, on the other hand, are very numerous, but they are operated by a multitude of organizations and almost certainly will have Y2K problems as well.

The week register rollover problem with GPS satellites is by this time well known and should not be a problem for newer GPS receivers.

Extremely new low-earth-orbit (LEO) communications satellites like Iridium and Teledesic are probably Y2K-compliant, but we haven't confirmed this yet. If they are

compliant, they will be useful as backup communication mechanisms for critical users if land-based telecommunications fail.

4. INTERNATIONAL TELECOMMUNICATIONS

If phone service is lost in other countries, we will be unable to communicate with them, and that fact alone will have serious financial repercussions. But the domino effect that is so prominent between businesses with Y2K applies here between nations: even if the U.S. telecommunications network is Y2K compliant, it could be jeopardized by interactions with noncompliant networks.

The telephone companies in other countries buy switches from many of the same manufacturers as do U.S. companies (as well as from several others), and so theoretically they should be Y2K compliant as long as they upgrade. But realistically, the response of other countries to the Y2K situation varies dramatically, especially in the developing world. Some countries have been very proactive at attacking Y2K, but most have not. For those that have not, one way to measure a country's potential telecommunications problems with Y2K might be to track its economic prosperity over time.

The building of national telecommunications infrastructure tends to be correlated with economic prosperity. Nations who became wealthy selling national resources, for example, are likely to have built state-of-the-art infrastructure at the time they became wealthy. During a period of low economic prosperity—after the resources ran dry, for example—a country would be unlikely to upgrade its infrastructures. So countries that were wealthy in the 70s and 80s but are not so today are likely to have Y2K problems, because they probably have not upgraded their equipment. Countries that are prosperous today are less likely to experience Y2K issues. Countries that never were very prosperous are unlikely to have Y2K-telecom problems, because they're probably still using mechanical switchgear. Economic prosperity trends (perhaps as collected by the CIA) might thus be a useful starting point in gauging the Y2K status of telecommunications in the developing world. Beyond that, coordination with the ITU seems the best approach.

The Internet in other countries depends on telephone systems like it does in the United States, so keeping the phones working there is necessary for keeping the Internet working. The loss of the Internet in other countries would be acutely felt by U.S. organizations that depend on its ability to move data internationally. But we don't think it's likely that an outage in another country would create a "bottleneck" in the United States since the United States already handles a large percentage of the world's Internet traffic anyway. The ripple effect of noncompliant Internet networks in other countries interacting with ours and jeopardizing our functionality is certainly possible, but the likelihood is difficult to predict without further analysis.

5. DEPENDENCIES OF TELECOMMUNICATIONS ON OTHER INFRASTRUCTURES

All telecommunications mechanisms depend on electric power. Most have some power backup capacity, but if the electric grid in a city, state, or nation goes down and stays down, virtually all telecommunications there will go down soon after. The reliance of global telecommunications on electric power is probably a more immediate Y2K threat than that of direct Y2K-induced failure of telecommunications systems. This is not a big problem with "normal" outages, where electric power is restored quickly after an incident like a lightning strike and telephones continue to work as if nothing happened. But because Y2K will affect several infrastructures simultaneously, over a wide area, nonlinear effects may cause outages to be longer and more widespread than normal. Nonlinear effects simply mean that if it takes 1 day to recover a system after 1 incident, it may 4 days, not 2, to recover from 2 simultaneous incidents. The delays are not additive but multiplicative. The problem is greater than the sum of its parts, but we cannot be sure how much greater. Nonlinearities occur frequently in complex interconnected systems, of which the infrastructure is a prime example. Nonlinearities are one of the principal reasons why talk of Y2K contains such an atmosphere of speculation, with phrases like "likely"or "possible" or "effect X may happen." Exact prediction is not merely difficult; it is impossible.

In the United States, most local switches are backed up by batteries which last for a few hours, and by diesel generators that last from a few days to a week or so. If electric power is off for a week or more, and if diesel fuel cannot be replenished because the transportation infrastructure is also affected by Y2K, the phones will go dead, as will the Internet and all the other networks that depend on the telephone system. Thus for telecommunications to survive Y2K, it's absolutely criti-

cal that the electric power grid survive Y2K, and if it does not, it is critical that fuel for generators be available where it is needed.

Note that if the power grid goes offline, the electric company will need communications to bring itself back online. Typically, it will rely on its own private communications network (again, with power supplied by temporary generators), but some electric utilities it may be almost wholly dependent on the public telephone network. Thus, there is a subtle and vicious cycle at work here. If power stays off so long that the phone company runs out of diesel fuel, and the power company runs out of fuel for the generators that power its own communications network (or it is dependent on the telephone company), it may be impossible for either power or telephones to be reactivated. Power needs communication to restart, and communication needs power to work. Keeping fuel flowing for emergency generators should be a top national priority.

Another way to break the cycle is to emplace photovoltaic renewable power systems at critical communications nodes. Because these systems convert sunlight to electricity, they can provide virtually permanent, free electricity with no external fuel requirement. From an engineering point of view, they are a good match for telephone equipment because the direct-current (DC) energy they supply is perfect for recharging the battery bank that is already in place at the equipment. From an economic point of view, PV power is usually too expensive where cheap, reliable grid power is available. But in developing nations where grid power is less stable than in the United States, and even in the United States at sites that are remote and difficult for repair crews to reach in an emergency, the promotion of PV power to telecommunications sites for Y2K reliability (and for reliability in general) makes sense.

6. OTHER ISSUES

Common natural disasters such as earthquakes, ice storms, and the like could compound the Y2K crisis if they occur near January 1, 2000. The Leonid meteor storms which occur in November 1998 and 1999 will be the most intense meteor showers in 30 years, and there is a possibility that they will damage satellites.[4] Man-made events like strikes, war, etc. would also cause our Y2K remediation efforts to be spread thin.

Thinking that we will be so preoccupied with Y2K that we would not notice deliberate malicious intent, terrorists, hackers and other criminals might see Y2K as a prime opportunity to attack pieces of our infrastructure. Or they might use Y2K-induced infrastructure failures as cover for theft, arson, bombings, etc. We must be watchful of such groups in the months leading up to Y2K and we must be especially careful when monitoring the crisis as it occurs to discern deliberate intent. New, automated indications and warnings mechanisms could be useful for this purpose, and would continue to be useful after the Y2K crisis for monitoring deliberate sabotage.

7. RECOMMENDATIONS

Run system tests that exercise as many components of the system as possible. A little planned pain now, while we have the time and resources to fix problems, is better than a lot of pain on January 1, 2000 when repair crews already have their hands full.

Insist that all emergency response teams and public safety organizations evaluate their Y2K status and upgrade immediately. Drill emergency response teams with and without conventional telecom capability. Recent experiences suggest that well-trained and well-drilled ER teams work much more efficiently than those that do not drill.[3] At the same time, drill the ER teams whose job is to fix the public telecommunication systems themselves, and perform extensive scenario planning with them. (Utility companies that don't have ER teams must establish them.) Much like the Pentagon stays prepared to fight two wars simultaneously, we should be prepared to respond to widespread outages in at least two major infrastructures simultaneously.

Encourage private businesses—especially small-to-medium enterprises—to upgrade their Y2K-sensitive equipment, including privately owned telecommunications and Internet equipment. This effort must of course include smaller phone companies and Internet Service Providers who are especially critical to overall telecommunications functionality.

Encourage other countries to upgrade their telecommunications networks and indeed all their infrastructures to Y2K compliance. Provide assistance where possible.

Ensure backup systems are in place and working, especially at the more critical sites. Batteries should be fresh, generators maintained (and themselves checked for

Y2K compliance), and plenty of fuel should be on hand. Allowing the stockpiling of extra fuel for the Y2K emergency should be considered, even if it means suspending environmental regulations to the contrary.

Keep oil wells, refineries, and fuel trucks running. They are critical not just to telecommunications, but to all the Y2K-impacted infrastructures.

Encourage solar-powered backups for critical remote sites and foreign telecom systems where grid power is spotty anyway.

Install indications and warnings (I&W) systems at critical sites to detect malicious sabotage and monitor Y2K cascade failures.

Finally, there are legitimate national security concerns that make it necessary for the government to have access to detailed information about the nation's telecommunications infrastructure, for Y2K preparedness as well as other threats. We must encourage the telecommunications companies to supply data (under nondisclosure agreement of course, and without fear of having the information used against them in litigation), so that the government can continually evaluate the national security posture of its telecommunications networks.

CONCLUSIONS

Telecommunications is essential to our functioning as a nation, as are all the other major infrastructures. The good news is that major telecommunications outages resulting directly from Y2K are unlikely, at least in the United States. The bad news is that Y2K has a good chance of disrupting accounting and billing at telecommunications companies, and without a stable revenue stream, those companies cannot stay in business. Also, telecommunications is deeply dependent on other infrastructures, which are much more likely to experience Y2K-induced failures. Providing adequate slack and backup in all the critical infrastructures will lessen the duration of outages and minimize the ripple effect where one infrastructure takes down another.

The most important thing to remember about the Y2K crisis is that people created it and people will solve it. It is fundamentally a social problem, not a technological one. Since it is too late to prevent all Y2K disruptions, the best way to prepare for them is to fully disclose to the public what to expect and to practice scenarios with the people who will be the first responders to the crisis.[3] If those first responders are prepared, and their families and personal infrastructures are secure, they will be able to do their jobs and get our infrastructures back on line quickly, with a little help from all the rest of us.

REFERENCES

[1] http://www.telecompolicy.com/whoweare/

[2] Testimony of Dr. Judith List, Bellcore, July 31, 1998 to the Senate Year 2000 Committee.

[3] Petersen, Wheatley, and Kellner-Rogers "The Year 2000: Social Chaos or Social Transformation?" Global Business Network, http://members.gbn.org/index/epress/multipleAuthors/jul98/y2k.pdf

[4] http://cnn.com/TECH/space/9804/27/leonid.meteor/index.html

○