
# THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION

## PUBLIC MEETING

## LOS ANGELES, CALIFORNIA

## MARCH 13, 1997

A transcript of the President's Commission on Critical Infrastructure Protection Public Meeting, commencing at 10:00 a.m., at 200 Spring Street, Public Works Hearing Room, Room 350, Los Angeles, California.

COMMISSIONERS PRESENT:

ROBERT T. MARSH, Chairman
DAVID V. KEYES
WILLIAM J. HARRIS
STEVAN D. MITCHELL
PETER H. DALY
BRENTON C. GREENE
NANCY J. WONG
WILLIAM B. JOYCE

CONTENTS

LOS ANGELES, CALIFORNIA

THURSDAY, MARCH 13, 1997

10:00 a.m.

THE MODERATOR: Good morning, and welcome to the meeting of the President's Commission on Critical Infrastructure Protection. I'm JoAnne Aplet of the Los Angeles League of Women Voters. The League is honored to have been asked to moderate the discussion of this important topic, and we're pleased that the first meeting of this distinguished Panel is being held in Los Angeles.

Later in the program, Los Angeles City Council President John Ferraro will join us to officially welcome the Panel to Los Angeles. But before we begin, I would like to introduce the Panel and then set forward the ground rules that we'll be following today.

The members of the Panel are the Commission Chairman, Robert "Tom" Marsh, and seven members of the Commission. Mr. Marsh is going to briefly describe the goals and work of the Commission before we take testimony from the audience. I will discuss his background briefly just before he talks.

But first, I would like to introduce the seven members of the Commission who are here with Mr. Marsh. The Commissioners are William Joyce from the Central Intelligence Agency, where he was deputy chief of the Foreign Broadcast Information Service Engineering Group. Pardon me, but these are complicated titles for some of these people. Nancy Wong, who is from San Francisco, represents the private energy sector. She is the director of PG&E's Computer and Network Operations.

Peter Daly, who served in key positions in his 31 years in the U.S. Treasury Department.

Dr. William "Bill" Harris, who has a distinguished career in the transportation field, including serving as Assistant Director of the Texas Transportation Institute.

Steve Mitchell, who comes to the Commission from the U.S. Department of Justice Criminal Division's Computer and Intellectual Property Section.

Brent Greene, the director for infrastructure policy within the office of the Under Secretary of Defense for Policy, the DoD.

David Keyes has been an agent in the Federal Bureau of Investigation for nearly 26 years specializing in high technology security issues.

Following Mr. Marsh's remarks, the invited speakers in the audience will address the Commission according to a prearranged agenda. The members of the Commission are here to listen. While they may ask questions for clarification, they are not here to make presentations. They wanted to hear from you. Each speaker will talk for up to ten minutes. In order to allow additional time for additional speakers from the audience, the speakers are asked to limit themselves to this time and also asked to speak directly into the microphone because the acoustics in this room are not good.

I will signal each speaker somehow when they have one minute left, and the purpose of limiting the time for each speaker is to assure that there is time after 12:15 or so, when the last scheduled speaker is supposed to be through, to allow time for other people in the audience to also present their testimony.

You will receive or have received forms in the back to fill out if you are interested in speaking, and I will call your names in the order received.

The meeting must end at 1:00 sharp because the Commission has other appointments. The Commission will be glad to take written testimony from anyone who either doesn't have time to speak or prefers to give written testimony rather than oral testimony, and they also welcome receiving additional background information from anyone who is presenting testimony.

There is a court reporter present recording all testimony, so there will be a record.

I would now like to turn the meeting over to the Commission Chairman, Mr. Marsh, who has an extensive background in aerospace. He's a graduate of West Point with a Master of Science degree from the University of Michigan. He is a retired Air Force General and served as the first chairman of Thiokol Corporation from 1989 to 1991.

He is also currently board chairman and member of the board of several high technology and Government institutes. He will briefly present to you the work of the Commission, and then following his presentation, we will call on the members of the audience who are scheduled to speak. Thank you.

MR. ROBERT T. MARSH: Thank you, JoAnne. Well, it's really a great pleasure for all of us to be here, a great pleasure for all of us to be here in Los Angeles today. And we're very pleased that you all consider this effort so important as to devote your time and energy to it.

I'm Tom Marsh, Chairman of the President's Commission on Critical Infrastructure Protection. And our purpose here today is to build public awareness about what I describe as America's life support system, our critical infrastructure, and to hear your views on what we should or should not do to prevent interruption of these vital systems. Last July 15th, President Clinton signed an Executive Order that begins with this sentence: "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." And that Order created the President's Commission on Critical Infrastructure Protection. The principal purpose of the Commission is to recommend to the President a national policy and implementation strategy for protecting the Nation's critical infrastructures and assuring their continued operation.

What are the critical infrastructures that we're looking at? Well, they fall into five basic groups. First are the systems we term vital human services, such as water supply systems, fire, police, and medical services and other federal, state, and local government services that protect our freedom and help provide us our quality of life.

Then there's the entire financial services industry where trillions of dollars literally move through the electronic and other systems daily. The impact of destruction there would be severe. The infrastructures include the introduction and distribution of electric power, natural gas, and petroleum, critical systems that provide our light, heat, and cooling, make us the most mobile people on earth, and run the equipment that powers the American industrial machine.

The newest and fastest growing infrastructure segment involves the electronic distribution of information. We've pioneered tremendous advances in communications technology and reap extraordinary benefits. However, our reliance on these systems exposes infrastructures in new ways and creates new vulnerabilities.

And the final infrastructure capability which we term “fiscal” includes all the means by which we transport and deliver our products and services. Why are they critical? It goes back to the words that the President used when he created the Commission last July. Their loss or incapacitation would have a debilitating impact on the defense or economic security of the United States.

The time for a Commission such as this is now, before a serious problem develops. These infrastructures are America’s life support systems. Many companies such as utilities, as well as all of you who live and work in many parts of California, are very familiar with natural hazards, but today we’re facing a new set of man-made hazards.

Technology has created an interconnected world. Each connection, however, creates new exposure and risk. Companies are becoming increasingly vulnerable to theft, unscrupulous competitors, malicious hackers, insiders, cyber attacks and plain criminals. The tools to exploit these vulnerabilities are readily available. In some cases, all it takes to penetrate automated systems is a PC, a phone, a modem, and skills that many fourteen-year-olds seem able to master.

The Commission’s mission then is to assess vulnerabilities and threats to infrastructures, identify relevant legal and policy issues and assess how they should be addressed, recommend to the President a national policy and implementation strategy for protecting these critical infrastructures, and propose any necessary statutory or regulatory changes.

Cooperation between the public and private sectors is essential to the success of critical infrastructure protection. We are vitally interested in what the private sector has to say because it owns and operates most of the critical infrastructures.

Furthermore, government relies on that private infrastructure for essential services and for national defense. Together the public and private sectors can develop solutions for the future, but everyone needs to be involved. We need the best thinking up front. So I encourage your input, and that’s why we’re here today. It’s the only way we will achieve solutions that work for everybody.

Furthermore, should you wish to talk to us at any time, please write or visit us on the World-Wide Web at the address shown on the screen [http://www.pccip.gov/], and I personally want to thank you very much for your participation in this important work.

THE MODERATOR: Thank you very much, Chairman Marsh. Our first speaker today is Mr. William "Bill" Baker representing the Motion Picture Association. Mr. Baker.

MR. BAKER: Commissioners, in my last job in federal government, I was responsible for criminal investigations conducted by the Federal Bureau of Investigation, and part of that included the Counter Terrorist Program. Part of that Counter Terrorist Program's responsibility, especially during Desert Wind and Desert Storm following the invasion of Kuwait in August of 1990, was to work with other agencies in the United States and identify key infrastructures that were vulnerable in the event of war, terrorist attack, or criminal extortion. And much of the FBI's initiative during that period went into that type of work.

That is why I'm particularly pleased to see that your quiet efforts in continuing this important work of our Government is ongoing and why I welcome the opportunity to spend some time with you today. My purpose before you is not to be presumptive enough to suggest to you that the motion picture industry fits squarely into the peg of key infrastructures, but I want to leave you with two thoughts today. One is that with the scope and breadth of our industry, I'd like you to note that in protecting the content of our industry, especially in the digital environment, there is indeed a link with your important work.

Secondly, I would like to leave you with a thought that because digital delivery knows no territorial borders, and because the buzz word today in digital communications is the word "convergence," a solution to the protection of these vital arteries of our country's everyday existence should encompass the hardware industry, the software industry, the content providers, both for the global and for the national information infrastructure and GII and NII work that's ongoing.

And, therefore, I'd suggest that any solution to girding up these vulnerabilities and protecting our infrastructure should be international in scope, especially in the telecommunications area, and especially because of the digital environment, and really should include our planet and the air and space around it.

As I said, your definition of telecommunications and the work of the motion picture industries are not a square fit, but in this environment of the digital age, I find the link.

As to the scope of our industry, last year in the United States, we produced 421 new films. 216 of those came from the seven major production companies that our Association represents, and the other 205 from the independents. But this is a tremendous export internationally. Theatrically, for instance, over 50 percent of the total revenues in our film industry come internationally.

Because of the huge cost of producing the motion picture, on average of $70 million for a major picture to produce, advertise, and distribute it, because of that huge cost, there is a need to protect and allow for the full exploitation of that product which includes television, Pay-Per-View, and the new Video One demands, newer Video One demands and, yes, the use of satellite delivery and the use of cable systems and, soon, the Internet. I say "soon" because the capability will shortly be there.

Of interest, getting beyond the theatrical, there are 95.9 or almost 96 million television households in the United States that you would have to communicate with in emergencies, and they are serviced by 1,181 television stations. Of those, 63 million households are reached via about 11,600 cable systems. On an average night, the six major networks in the United States reach 44 million people, and our member companies are very active in this distribution of news, sports, and entertainment via the television system.

Importantly, the entertainment industry consistently maintains a positive trade balance bringing billions of dollars back to the United States, even while creating hundreds of thousands of jobs abroad and leaving billions of dollars to nurture foreign economies.

But there is a dark undercurrent to the success of our industry, and it's made more apparent by the digital environment that we're entering today, and that is the illegal interception and illegal duplication and distribution of copyrighted product. Jack Valenti — my boss and the chairman — has often said, "If you can't protect what you own, you own nothing at all."

And that's what we're faced with today; the need to develop a proper protection system for the digital environment so that indeed copyright can be protected.

Now, an important part of the Motion Picture Association's efforts and budget goes to addressing worldwide piracy. And we last year were involved in 25,000 investigations

and raids which seized over four million pirate videocassettes belonging to our members. But that's in the analog world, and I think the importance of the work you're doing and where, again, we fit in now is in the digital world. Because in the digital world, the ten-thousandth copy is as pristine and clear as is the first master. And once it's out, it's out for good.

So in summary, the Motion Picture association of America is pleased to cooperate with your important work, and we recognize the link between your protection mandate and our industry which includes vast cable and satellite TV systems as well as our celebrated films.

So I thank you for this opportunity to make a presentation, but I think, like in most contacts, the important thing is that I've left copies of my presentation with you, and I've left a list of our member companies and resource persons, persons who would volunteer to have further contact with you. I remain one of those, but we have a vast industry, and we very much would like to be involved in your important work.

Thank you.

THE MODERATOR: Thank you, Mr. Baker. Thank you for staying within the time limits. Our next speaker is Mr. Nick Christenson of the EarthLink Network.

MR. CHRISTENSON: Good morning. I'm Nick Christenson. I'm the senior architect at EarthLink Network, one of the nation's largest Internet service providers. I'm here to represent EarthLink's interest, in particular, and informally the Internet service provider community, in our opinion, about the Internet and Internet service as a critical information infrastructure.

The EarthLink delivers Internet service to home and business use. Our perspective is that today the commercial Internet as we deliver it is probably not on the same part as critical an infrastructure as, say, power or water, but within five years, it certainly will be. So that now is absolutely the right time to start thinking about Internet service as a critical infrastructure.

The new medium of Internet is far more complex than most of the other media that we have available to us today. The individual subscriber or person at the other end of the line has a lot more interactive capability with the rest of the medium. So his or her impact

on performance and robustness is much greater than every other media. The growth is also phenomenal, and 90 percent of our efforts is spent merely keeping up with the demand and providing a reliable service to the membership.

The medium is also very new. Commercial Internet service is maybe a six-year-old industry as a viable industry. Compare that to its ubiquity now or market penetration compared to phone service or television service over the same initial six-year commercial time span, and you can understand some of the problems that we face.

Another big problem is that because of its complexity and its growth, finding qualified people who can address critical infrastructure issues within the industry is difficult. These people are all sorely taxed and, you know, working 80-hour weeks just to keep their own service expanding at market rate.

Also, the medium is completely international in nature, and any sort of solution that we address locally also needs to be addressed internationally. The types of threats that the Internet, Internet services, and infrastructure faces are national causes combined with non-malicious attacks.

The Internet is obviously vulnerable to accidental outage or overloading. I think the overloading is mostly due to unprecedented demand issues. We've seen, during times when our growth has been relatively slow, a consequent great increase in the service reliability. We think these things will work themselves out as we approach market saturation and as the industry, as a whole, matures. And there is a great deal of effort underway to make sure this is going to be the case.

On the other hand, it is more complex than other issues. We have had incidences in our companies where keystroke errors and things like that have brought down services for hours or sometimes days, and this is something that needs to be addressed very carefully within the industry. It's a critical direction.

Another type of threat is what I would define as vandalism, which is to say a small group of minimally-financed people with no necessarily clear agenda for what they want to do. These folks, as we've seen if you have been reading the newspapers, can cause some serious problems. New technology can help in this.

However, it's harder to defend against this in an interactive medium like the Internet than it would be in something like television or power and water, which is essentially a one-way sort of medium. Nonetheless, there are technologies in place to do this. The question is: Are both the providers of the technology, the computer vendors, network manufacturers and the Internet providers inset enough to deal with them?

The third-class of threats is what I would define as sabotage, which is a large group of high-financed people with great resources. Internet, at this point, is probably not much more vulnerable to these than the technologies that is being carried on, for example, in telecommunications. And as I know you are all aware, it's a very difficult problem to solve.

The Internet service providers realize how important this is becoming. We're now looking at a phase in the Internet's growth as a market of increasing cooperation and realization between Internet service providers. We have to band together in order to provide reliable service for everyone. This is a lesson, for example, that the phone company learned quite some time ago.

Most long service providers have agreements to carry each other's traffic in times of outage, and the Internet service providers are starting to work along the same lines. And I think this is something, like the phone companies of the industry itself, needs to work out, and we would like to see the Government support us in our efforts to do so as these come to fruition.

In addition, the computer network equipment vendors currently don't ship products that lend themselves easily to a secure infrastructure. The main reasons are, one, it's very difficult to do so, and the second reason is there is really no incentive for the purchasing market. We buy computers from large computer vendors, and they know they ship insecure products, but the market has not demanded that they do so.

And so we have to go through a great deal of effort in order to maintain their integrity. Now, it's impossible, on a system like that, to ship something like that completely bug-free. However, the resources are being developed and are being pushed into new production, and that is what the market demands rather than making the products that exist more robust.

There is also, as I mentioned before, there is very little — or not very little — but not sufficient emphasis on infrastructure protection among the players. There are few people available who can solve these problems. The infrastructure vulnerabilities are not a strong incentive used to solve those in the current market, and there are also relatively more using and managing the technology.

This is also true in other infrastructural areas. Very few people in this country, I think, are aware of the fragility of the phone system, potentially, to sabotage or attacks, and I think a general education effort is also of good use and service.

We believe that the marketplace wants to take care of these problems, and the industry is best equipped to solve these problems. What we would like to see is the Government help and incentivize us to make the right decisions. So what we recommend is to support industry to help solve the problem, support efforts to help educate the public on computer security, and reward vendors and providers who employ good infrastructure practices using affirmative rewards rather than penalties.

Let industry supply the solution and provide help and implementation. And I also ask the Government to please resist the urge to blindly legislate. There are a lot of computer laws on the books which are very well-intentioned but, in functionality, are not the desired effect. I know in speaking for industry we are more than happy to help work with the Government to help provide meaningful and affirmative and appropriate assistance in this manner in any case.

It's a pleasure to talk to you guys. I think this is exactly the right approach and on a very important issue, and EarthLink and the Internet service provider community are more than happy to do our part to assist you guys in new efforts.

Thank you very much.

THE MODERATOR: Thank you very much. Our next speaker is Councilman Hal Bernson of the Los Angeles City Council who is also vice chair of the Council's Transportation Commission.

COUNCILMAN BERNSON: Yes. Thank you.

Members of the Commission, I'm going to be here this week on behalf of local government and some of the things we've learned through our experience. I also serve on

the State Seismic Committee Commission and serve as a board member of the Southern California Regional Rail Authority, Metrolink, the successful commuter rail system we have in California. It is in five counties now as well.

One of the things we have learned through bitter experience in Los Angeles from disasters such as the Northridge earthquake is that while you can't predict a disaster that may occur, whether it's a earthquake, flood — maybe we can predict flood and flood plains — but I am not going to deal with that aspect of it. This is earthquake country, and there is obviously the danger of sabotage, and those things cannot be predicted.

But what can be achieved is mitigation through preparation. We have learned that the effects of the worst disaster can be lessened by being properly prepared, No. 1, in your Codes, for example, that protect your building and infrastructure facilities, and No. 2, in response and training, and we went through strenuous bills for many years here in Los Angeles prior to the Northridge earthquake, and it paid off. Fortunately, we were very fortunate of the time it occurred, otherwise, the loss of life would have been probably ten times what it was or more.

But the lesson is that if you're prepared and the population of the people you deal with are educated in how to deal with a disaster, you can mitigate and make it less and also plan for recovery. Recovery is a very important issue. For example, our freeways were down. How do you get people to work? How do you get people to respond to emergency situations? Those are things that local government as well as state and federal governments need to have plans for in advance. After the disaster happens, it's too late. You need to have advance thinking and planning, and those things should be coordinated at all levels of government with each other.

We were very fortunate. We were very quickly supported by FEMA and other government agencies such as Transportation and Housing. Capitol members were here in Los Angeles. I don't know if it was the same day, but it was certainly that night we had assistance on the way, and there were plans to bring the relief in, and it came. These things are important.

I just want to stress that I think that this same theme holds true whether it's transportation, whether it's a facility such as your public buildings, schools, whatever they may be.

If you prepare for serious problems in Codes, if you prepare a plan for dealing with it ahead of time so people are educated and know what to do, if you have a means of dealing with the response to that emergency when it happens, you are going to be able to handle it a lot better than if you are not.

There are obviously things that are an act of God that we don't have control over. All we can do is prepare ourselves.

But the three levels are basically, No. 1 is preparation as far as mitigation and all the things that you can do before the event. The second is training for response, and the third is recovery. And particularly, most people just think that the impact or economic loss to a community or to the nation is with the event itself. That's really basically not true. The major effect of a major disaster economically is the aftermath and recovery period.

And we are now in our fourth year of recovery from Northridge, and our community has still not totally recovered. We're on our way, thanks to a lot of help we have had from people like FEMA and the Office of Emergency Services in California. But there's a bitter lesson to be learned by some of these events.

I particularly recall, as a member of the Seismic Safety Commission visiting San Francisco following the Loma Prieta event and seeing what the impact of the freeways being down there, where they virtually had no means of getting from one side of the Bay to the other. It was a tremendous disaster. These are the type of things that local government in conjunction with state and federal government needs to think of in terms of future.

I thank you for giving me the opportunity to speak.

THE MODERATOR: Thank you very much, Councilman Bernson.

MR. DAVID V. KEYES: JoAnne, could I ask a question, please?

THE MODERATOR: Sure.

MR. DAVID V. KEYES: Councilman, may I make just one quick request to you. The City of Los Angeles has been very, very helpful to the Commission by providing us examples of those emergency plans that you just alluded to pertaining to physical damage. If there are any similar models pertaining to cyber emergencies, attacks on information

infrastructure, we would be equally pleased to receive those kinds of plans. I am not asking you to detail them here, but we would be happy to receive them.

COUNCILMAN BERNSON: We'll be happy to communicate with our Communications Department and see that whatever is available is forwarded to you.

MR. DAVID V. KEYES: Thank you, sir.

COUNCILMAN BERNSON: Thank you. Any other questions?

THE MODERATOR: Our next speaker is Mr. Richard Rudman of KFWB and CBS Corporation who is also the head of Los Angeles Emergency Preparedness.

MR. RUDMAN: Good morning, Commissioners. I'm Richard Rudman. As you already heard, I am with KFWB Radio and have been director of engineering since 1975. My full comments have been filed with Elizabeth and are available for you. I am just going to read excerpts from them.

Broadcasters could become key components of a terrorist strategy to the detriment of the public. If nothing else, please remember that the first target in hostile government overthrow campaigns is often the broadcast media.

Security at broadcast studio and transmitter facilities is often nonexistent or weak at best. Despite a chain of major and minor incidents and FCC rules that mandate certain levels of security, my industry has not learned its lesson. Major broadcast facilities simply have to become more security conscious before they become targets themselves. Government emergency managers should work with the industry to enhance security when threat levels rise and form contingency plans if the worst happens, and a key broadcast facility actually becomes a target.

Recently Channel 9, owned by Disney, saw a disgruntled citizen hold their entire facility hostage by a truck with a dummy bomb. It can happen there or to somebody else nearby next time with a real device.

Some of our other threats, I think, have combined to help us do a better job to deal with upcoming threats, and even the threat of seismic or terrorist threats we face in the region that Councilman Bernson so well talked about.

The region's seismic threat has forced everyone at all levels of emergency planning in the public and private sector to a level of preparedness that can only be compared to

regions in the country like “tornado alley” or parts of the Eastern seaboard that have hurricane threats.

Now, we know terrorism must be added to nationwide threat assessment. This will ultimately spur many unprepared regions to start thinking like we do. What lessons can they learn from us that might help us be better prepared for terrorism? I think we do have those lessons, and we can help.

First, there has to be an agreement that the broadcast media play a part in any emergency as far as a public emergency is concerned. This is true even if the media is kept in the dark like the proverbial mushroom. When this happens, of course, media does what it usually does when it does not have accurate information. We speculate.

I think this can be avoided. How do we avoid this, though? I think it’s by building trust that lead to partnerships that form during emergencies. If some level of trust can build toward an emergency government/media partnership, government can minimize potential speculation and replace it with a stream of accurate information, directives to the public to do things that will enhance their survival and safety, and even messages that can deal with out-and-out rumors.

No major urban center that I am aware of has as close a need for emergency preparedness and response as do we here in Los Angeles County and the City of Los Angeles. Over a decade of meetings, joint projects, and major emergencies we all face together, through those, many broadcasters and emergency managers can drop the day-to-day adversarial relationship when we have to, especially when it gets in the way of helping the public.

We have an atmosphere where the County Office of Emergency Management, the Los Angeles Sheriffs Department, City of Los Angeles, and our Technology Advisory Group that I chair can plan for what some people believe is a major enhancement to the discipline of emergency management. Basically trying to integrate emergency public information with the whole discipline of emergency management, something that heretofore really has not been done, in my opinion.

There are huge benefits that can accrue from this linkage of partnership during response and recovery. The most important of these is delivering to the public better and

more effective information. Effective local public information should convey many important messages that can be grouped under certain key categories.

And I have listed those categories. The key ones are basically trying to get information to the public based on the policy decisions that the emergency managers are making at any given time. The horse's mouth theory, if you will. It also can go to the other extreme of trying to figure out the best strategy for giving unpleasant news out and trying to assess at the top level of emergency management what effect that bad news might have on people and what other steps might have to be done to take that into account.

I want to talk a little bit about a communications lesson we learned from the Los Angeles riot. We have, in this event, validation of the precept that the public must have faith in governments ability to take control during major emergencies and how broadcasters can play a role in that.

Several broadcasters, faithfully reporting the facts, literally did commercials for looting from several stereo stores. They said words and showed pictures that said, "There are no police here, and people are walking out with stereo equipment."

And some of us are watching television and, of course, the Porsches and Audis that we saw after seeing reports were probably not driven by people harboring a deep desire to right political and social injustice.

Radio remains as the most reliable means within the United States for the general public to receive emergency public information after events that disrupt commercial power to television and cable service. Even though many radio stations were off the air or not supplying relevant information after the Northridge quake, enough survived and were broadcasting so everyone with a battery-powered radio had at least one station to listen to at 4:31 on January 17th.

I want to just go over a couple of overall conclusions. Again, this is detailed out in my full testimony that's provided for you.

Key lifeline components in the broadcast communications infrastructure must be protected better against a wide range of threats. Utility and other essential services for those elements so identified should be restored as rapidly as possible, taking into account all priorities for restoration in the whole community.

Special security measures should be planned to secure key broadcast facilities against hostile takeover. A special partnership must be developed between various levels of emergency management and lifeline broadcast resources that activates during a crisis.

The entire range of communications technologies should be employed to make sure lifeline broadcasters have access to public information officers at a major incident or at the emergency broadcasting center that is being covered. Broadcast communications experts and government terrorist experts should work together to counteract counter-terrorism strategies.

Planning for pool coverage and local Joint Information Centers should be done as a part of the overall strategy to combat whatever strategy and tactics terrorists might employ to tear at the fabric of public confidence. The role of public information officers within the EOC should be overhauled so that public information officers literally become reporters creating proactive information.

And after the initial alert, there is a need to tell the ongoing story of an emergency. And I detail out what I consider the NASA Mission Control model as one possible way to do this.

I want to thank you very much for this opportunity. I'm open to testify before your group. Any questions?

I guess I answered everything.

MR. DAVID V. KEYES: Thanks.

THE MODERATOR: Thank you very much. Our next speaker is Frieder Seible from UC San Diego who is a speaker on transportation.

PROFESSOR SEIBLE: First, I have to apologize. I did bring some overheads for today's presentation, but it's not possible to show those. So I have five copies of my book which I will give to Chairman Marsh.

MR. ROBERT T. MARSH: Thank you.

PROFESSOR SEIBLE: I am a professor of and chairman of the Department of Structural Engineering at the University of California San Diego, and I am also the director of Structural Research Laboratories, which are the nation's largest structural and testing complex for the actual testing of buildings and bridges under extreme loads. We

have tested at our Laboratories up to five-story full-scale buildings and have simulated full-scale bridge structures, so we are intimately involved in infrastructure protection.

Today I want to primarily talk about transportation infrastructure and the critical problems we have in our transportation infrastructure. I am wearing another hat today, namely, a new partnership which was just recently formed, namely, a partnership for innovations in the transportation infrastructure. This is a partnership between academia, government agencies, and the industry.

From the academia side, we have, in addition to the University of California at San Diego, four other major research universities in Southern California as part of our group, namely, Caltech, UCI, UCLA and USC. We are also part of the PEER system, the Pacific Earthquake Engineering Research Center, which is currently being formed with help from the National Science Foundation.

In terms of government agencies, we work very closely with the U.S. DOT, with the Federal Highway Administration, with Caltrans, the Utah Department of Transportation, and the Washington State Department of Transportation. And industry partners, as part of our partnership, are SAIC, Science Applications International, Fluor Daniel, Inc., Bechtel, Hexcel, T.Y. Lin International, and XXsys Technologies.

Now, why do we need such new partnerships between industry, government, and academia? For our transportation infrastructure. I want to briefly go into four areas just to highlight some of the reasons here.

The first is our nation's aging bridge inventory. The second is California's seismic bridge problem. The third is the nation's aging aircraft fleets, and the fourth is California's water supply pipelines. These are just four specific areas in which I want to briefly highlight the problems we're having.

On the status of the nation's bridges, we have in the United States over half a million bridges, and 40 percent of these bridge structures are obsolete in terms of their functionality. And if we just wanted to bring the bridge structures up to their current demand, to current standards where we don't have to put postings on bridges, where we don't have to close certain ones, it would cost over $78 billion based on an estimate which was already made in 1993. So by now the numbers have probably gone up significantly.

So we are at a stage with our bridge infrastructure where the bridge infrastructure is coming to an age where we have to spend more money just to keep it at current service levels and not extending the service which we're getting out of our transportation infrastructure on the bridge side.

In California we have heard already testimony of the problems after Northridge and after Loma Prieta. We are currently in a major bridge retrofit program here in California where we are retrofitting over 3,000 bridges right now to the tune of $4 billion in California alone. The rest of the country is just starting into looking at seismic issues.

So, again, it's a major, major problem here. Here in Los Angeles you can see a lot of bridge structures which are currently being retrofitted with steel put around columns. This is all technology which was developed in our laboratories at the University of California, San Diego.

The nation's aircraft fleet is another major problem. Again, the majority of our military aircraft was put into service in the 1960s, and they are getting to the stage where they have reached their assigned life in terms of fatigue. Tests show fatigue cracks in the fuselage and the aircraft wings, and right now we do not have the means to properly predict the service life of our aircraft fleet, of our commercial and military aircraft fleet, and we do not have the necessary tools to repair some of these problems. Estimates are that we are looking at over $500 billion to replace our aircraft fleet.

The last problem is that of water supply, which is transportation of goods. Here in California, we have over 400,000 feet of large-diameter, large pressure water supply lines. These are 10- and 12-foot diameter prestress water supply lines which have, in some cases, a thousand feet of pressure on the pipeline. We have had to date, fortunately, only two blowouts, two failures.

The prestress are corroding, and the pipelines are coming of age, and when a pipeline with a thousand foot of head blows, it creates a crater with a 200- or 300-foot diameter. So far the blowouts have been in the Mojave Desert. If we had one of these blowouts in the City, we would have a major disaster on our hands.

Again, it requires new technologies, new efforts to remedy some of these problems before they actually occur.

Now, in summary, we are looking at an issue here where our transportation infrastructure — not just on the bridge side, not just on the aircraft side, not just on the pipeline side — all areas where it is at a stage where it is coming of age and needs renewal. So we are proposing, actually, in this partnership, a complete new program for transportation infrastructure renewal. They are from the university side and can help in actually creating a new discipline, namely, called Renewal Engineering. We need to train professionals who are skilled in nondestructive evaluation, damage protection, in retrofitting rehabilitation technologies.

Right now we are training thousands of engineers who never in their whole life faced any of these problems which the nation is currently facing. Also, we need our partnerships with industry and the Government to do the necessary research and develop innovative technologies to address these problems.

Thank you very much. Any questions?

MR. DAVID V. KEYES: Are there any of those high-pressure lines you spoke about blowing in the desert, are the pressures inside the City at the same level of pressure?

PROFESSOR SEIBLE: The level of pressure is lower in the cities, typically. We have the high pressure where we have to be over the mountains as part of the California Aqueduct, but you still have 200 to 300 psi. So it is still a major problem.

MR. BRENTON C. GREENE: Has the State of California instituted any individual programs in several of these areas or one of these areas that could be a prototype kind of model for looking at ways to prioritize the projects, initiate processes for establishing funding to support them, legislative initiatives to help focus the issues in that vein, et cetera?

PROFESSOR SEIBLE: So far in one of these areas, yes, we have had this happening with the seismic area and the bridge retrofit program; I think the seismic bridge retrofit which Caltrans initiated. It started already after the Landers earthquake, but was accelerated after Loma Prieta and has been in full swing ever since and will be completed by the year 2000 when all bridges in California will have been addressed in terms of their seismic safety and will have been retrofitted, and with the program which really relies on this prioritization where to spend the money first.

So that is a very good example. If the commission is interested, I can supply you with more detailed information in how that program is put together. Thank you.

THE MODERATOR: Thank you very much. Our next speaker or speakers — the first speaker will introduce the following one — is Mr. Laryamha with the City of Los Angeles Information Technology Agency.

MR. LARYAMHA: Mr. Chairman, members of the Commission, I would like to introduce the executive of the Information Technology Agency of the City of Los Angeles, Mr. Frank Martinez.

MR. MARTINEZ: I don't usually have somebody introduce me; I was just in another meeting, and I wasn't sure I was going to be able to get here on time.

But basically we have submitted a written report or fact sheet which identifies the areas that we're responsible for in terms of the telecommunications infrastructure for the City of Los Angeles. The Information Technology Agency provides a full range of telecommunications services to other City departments, and we are also involved in cable franchise regulation and oversight within the City of Los Angeles.

In our report, we identify four basic areas; telephone services, radio services, data services, and video services. In terms of the telephone system that we use in the City, we use primarily Centrex through Pacific Bell as well as GTE. We have 13 Centrex switches that we're hooked into. In addition, we own several of our own PBX switches located in various City facilities.

The majority of our voice communication is carried over those land-line telephone networks. Obviously, any disruption to that would have a major impact on our ability in governing or in dealing with emergency situations. We have had experience with that in the Northridge earthquake where some of those systems were damaged or they were over-loaded with either phones off the hook or people calling relatives and businesses, and so forth. And we had to then rely on cellular telephones and our own radio systems.

So any national infrastructure protection program, I think, needs to take into account the fact that most local governments for sure use both their own systems, and they are fully integrated into local carriers or other private carriers. So there needs to be an under-

standing of the connectivity between both the private systems as well as the government's own communications systems.

We also maintain the City's radio systems for both the Police Department, Fire Department, as well as our other City departments. There are three basic radio systems; one for the Police Department and one for the Fire Department, and then we have a radio system for the rest of the City departments. We maintain the mountaintop transmitter receiver sites as well and maintain the individual radios, whether they be handheld or mobile radios.

Those entire systems, of course, are critical to our day-to-day policing on public safety communications as well as our day-to-day operations. Those have held up very well during the earthquake. They held up very well. We use a mixture of microwave and fiberoptic and lease-line transmission modes. In general, they held up very well.

One thing we should again say, even though that's a City-owned system and we are responsible for it, if it were to fail, if major mountaintops were destroyed, it could quickly escalate into a major problem that could rise to a federal level in attention in terms of public safety and civil disturbance or control of the civilian population. So that's something we think should be integrated into an overall program.

We also maintain the City's data information system in terms of the mainframe data center as well as distributing networks. More and more of our operations are now carried electronically. Most of the City facilities and over 6,000 City employees are on a network system. A great deal of City businesses move across those networks, including critical police actions as well as the civilian side of the government.

To the extent those systems could be destroyed or damaged would have a great hindrance on our ability to continue to function effectively as a government. Again, we use a multiple transport network. In other words, we have fiberoptic in the ground and use microwave, and we also lease lines from the telephone company. So, again, it's an interconnected network.

The last area I want to talk about was the video system. As I said, we are responsible for the oversight and regulation of the cable franchises in the city, cable operators, who

service over 500,000 households. This is a very good information source for people, and I think it should be taken into account in any kind of infrastructure protection program.

In addition, I think as the industry changes and telephone companies get into video, and video companies want to provide telephone service, and vice versa, we are going to see a merging of the companies, merging of technology, and it would behoove you to look at the full range of the technology communications out there.

We also operate our own government access channel, L.A. City View, Channel 35, which is a City-intersected cable channel which we produce government-related programs and City Council meetings as well as other public affairs-type programming. That has and can be a very useful tool in getting information out to the public during an emergency.

And that's about all I have today. And I am available to answer any questions.

DR. WILLIAM J. HARRIS: In training your people with respect to the operation of these systems, especially the cyber systems, what emphasis do you place on security? On using all the techniques to prevent interference by unauthorized people in your system where all of that can apply?

MR. MARTINEZ: We have a unit established within our agency that deals with security for our networks, and we have engineers involved in construction of firewalls and other security mechanisms and, of course, since we are supporting the Police Department, and they have Department of Justice requirements and State of California requirements relative to security, we follow those requirements as well.

So I would say we have a very specific focus on improving security and establishing appropriate firewalls and control mechanisms.

DR. WILLIAM J. HARRIS: One more question: Have you noticed any trend in attempts to break into your systems? If not or if so, do you monitor those break-ins and try to look aggressively at the cause, the source, and the necessary measures you need to take to recognize that attempt to penetrate your system?

MR. MARTINEZ: We have not had, to my knowledge, major attempts to break into our computer system. We have noticed vulnerabilities, though, just in our own monitoring of the network. We have to be very careful because some aspects of the City's network are very public oriented. We want people to come in, for instance, to the library systems.

So when they hook into the network, we have to make sure there is proper protocol and firewalls.

I must say where we have seen a lot of problems, believe it or not, are the telephone sites. We have had people probe and break into our proprietary switches and then connect with long distance — not chat rooms — but long distance calling parties. And we have recently had kind of a low-tech, what we call "clip-on entry" where they go into a telephone clip-on and then sell long distance service.

We have had some of that, and we work with our carriers to help us detect that and eliminate that.

MR. BRENTON C. GREENE: Along a similar vein, have you looked at your systems, any vital leaks where there may be potential, single-point failures; that if it was either an accident or a material failure or what have you, or even an intrusion could deny your ability to use some of those critical systems?

MR. MARTINEZ: Yes, we have. As a matter of fact, part of our overall network design was to go through and review our existing infrastructure to determine single points of failure and vulnerabilities. Like many large enterprises, our network did not grow under a design completely laid out with redundancies, and so forth. It grew as funding was available. And funding came on, so we have identified single points of failure and are in the process of trying to build in redundancies, and so forth.

MR. DAVID V. KEYES: You raised the issue of telecommunication restoration. Has the City of Los Angeles maintained contact with the National Communication System of the Department of Defense?

MR. MARTINEZ: We have not up to now had a good relationship with them. However, our new general manager, John Block, formerly of FEMA, was very involved with that group, and we intend to pursue that.

In addition, we do have a very good relationship with our local carriers and our long distance carriers, and they actually have participated in our emergency operations exercises, and so forth.

MR. DAVID V. KEYES: Thank you.

MR. MARTINEZ: Thank you.

THE MODERATOR: Thank you very much. Our next group of speakers are Mr. Harry Sizemore, the general manager of the Los Angeles Department of Water & Power who will introduce Marcie Edwards, the director of Bulk Power for the Department, to speak on power issues, and Jim Wickser, assistant general manager, to speak on water issues.

MR. SIZEMORE: Good morning. My name is Harry Sizemore. I'm the general manager of the Department of Water & Power, and I want to thank you for inviting us here to this hearing this morning. The Department is the largest municipal utility in the United States, and we are happy to share our thoughts on the importance of protecting critical infrastructure.

Both water and power are essential to the safety, health and welfare of the citizens of Los Angeles, and maintaining and protecting that infrastructure is an ongoing priority with the Department. In the last decade, the Department, along with the rest of the City, has faced many disasters which have tested and often damaged our existing infrastructures. We have experienced fires, drought, floods, civil unrest, and a major earthquake centered in the heart of our service area. During these crisis periods, our employees and the community worked together to quickly restore essential services so that recovery could begin and help could be provided to those severely affected.

Serving the City of over three and a half million people requires an infrastructure that is enormous. This enormity in a disaster can become an advantage because only rarely does a disaster affect the entire system. Also, our system is designed with a considerable amount of redundancy in both water and power so that services can be restored fairly quickly.

To give you a feel before we go a little further on the size of our system, on the water side we have in our system over 100 reservoirs, 7,000 miles of water lines, and a daily average usage of about a half a billion gallons of water. On the power side, we have ownership rights to 25, in part to 25 power plants in four western states, and over 19,000 miles of transmission and distribution lines.

I have asked Jim Wickser from the water side and Marcie Edwards from the power side to address specifically the concerns of infrastructure protection. Both of them have

considerable experience, firsthand experience, over the last decade in dealing with these issues.

First, Jim Wickser.

MR. WICKSER: Good morning. Thank you for allowing us to participate in this. I just want to thank your elite staff, head staff, who met with my staff earlier. They were very helpful, and I think mutual gains in shared information were made. As Mr. Sizemore pointed out, nature has given us an opportunity to drill in terms of infrastructure disruption; both in 1971 where we suffered a near collapse of one of our major earthen-filled dams serving about 30,000 residents, and the more recent earthquake.

Our experience has led us to conduct annual drills with our folks to the extent where people come in on Monday morning and find a note on their desk indicating something has happened, several blind drills, and then we get together and discuss how things work. I think that through this we developed a very strong cadre of very well-trained, issue-oriented employees who know what to do. They have learned you cannot depend on telecommunication issues just because of the downed infrastructure.

So people have to know what bells to operate, what buttons to push, and how to get there. In the subsense, we are fortunate that our development of telemetering, and so forth, has lagged a bit, and so, consequently, it's more operation than operating facilities. In a time of emergency, we found that because of breakdown in communication lines, it's been necessary not to rely very much on that.

We also live in a large area where there are a lot of vendors, a lot of opportunities to rent equipment. In 1994 we rented a lot of water trucks in order to maintain a potable supply for our customers. We also have a lot of interconnections to other utilities, neighboring utilities. Once again in 1994, because we had more water out, it was imperative we connect with our neighbor to the south so that Los Angeles International Airport would have potable water for reloading all the planes; a shortage could have resulted in a shutdown at the airport which was far from our thoughts at the time.

We also had a mutual cooperation pact with California during 1994, folks from the Bay Area, East Bay Municipal Utilities in Oakland as well as Orange County from the south came up and helped us tremendously to repair our leaks. From the infrastructure

standpoint, we have really had quite a bit of experience. We have a good, solid work force and are capable of doing a lot of our own repairs and caused a very quick recovery in 1994 as well as 1971.

On the water quality side, we also have our own laboratory capabilities as well as contracts with government, with new facilities nearby and very well-staffed and qualified people. We typically run 147 samples a year, and we have significant capability to go into specialized monitoring upon advance notification that there's a reason to do so.

We also have eleven strategic locations in our system that are monitored on-line, including a couple of locations where we use local fish species to detect toxins in the water; sort of an early warning system. I think generally the area that we would find most helpful because we dealt with nature, it's the new concerns that we're not used to.

And the federal government could help us, I think, in trying to anticipate what we might expect, what type of issue we might want to monitor for in terms of what water quality as well as what type of issue might be expected in terms of infrastructure disruption.

I think, most importantly, our concerns center around advance notice of the possibility, and the type of things you might be aware would be necessary for us to try and prepare for, to be ready to deal with, and also whatever educational training you could provide for our employees through internal management, or whatever.

As I say, it is a very, very fortunate thing for the City of Los Angeles we have a very strong, well-trained, knowledgeable staff, and we have equipment and facilities. And we have, unfortunately, had the opportunity to drill a great deal in real-life situations.

With that, I would be happy to respond to any questions.

MR. BRENTON C. GREENE: Jim, to what degree are you using or shifting to increased automation in the water distribution and thus potentials for telecommunications or information intrusions that could deny water availability?

MR. WICKSER: We have been, over the last five years, adding quite a few of our stations to an information system. Much of what we're benefiting from, though, is information on the storage and flows and pressures as opposed to actually controlling valves, and so forth. We still, because of our work force, have substantial numbers of

people that can physically respond. We had some wind damage, which is not a big thing, but as a result, you lose power to some of your pumping stations.

So the immediate response shows up on the screens that we're losing water, and we dispatch the electrical or mechanical people to deal with the pumping plant as the case may be.

MR. DAVID V. KEYES: We very much appreciate the help Mr. Sizemore referred to previously for the Commission and applaud the assistance. Any additional assistance you can provide us with, data on attempted intrusions to your systems, would help us understand the threat model that we're examining there.

So in the event that information were to be available, we would be very grateful to receive it.

MR. WICKSER: Yes. I want to thank your staff because, upon your visitation, we immediately had somebody check the firewalls in our State system, and we think we're all right. But we certainly are much more sensitive to it than we would have been had you not been out here to visit us.

Thank you very much. With that, I think Marcie Edwards is here to talk about the energy side of the business.

MS. EDWARDS: Good morning. My name is Marcie Edwards, and I'm with the Los Angeles Department of Water & Power. I also thank you for the opportunity to present some of this information to you this morning. My comments are attempting to add to what we have provided in the written record.

Mr. Sizemore provided you with broad facts. Any greater degree of specifics that you require, please let us know, and we'll be happy to assemble that information and forward it to you after the fact. What I would like to focus on today are some recent facts concerning our power system and how we responded and the associate infrastructure implementations.

On August 20th, 1996, a wildfire north of Los Angeles interrupted all six of the major transmission circuits that were connecting our customers to a major electric facility up north. With some minimal warning, we managed to adjust system conditions such that our power system, power delivery system, was not affected and, basically, that outage,

which was a multiple outage utilizing six simultaneous contingencies, was not made aware to our customers. They never saw it.

August 10th, 1996, a tree in Oregon garnered national attention as the southern portion of the Pacific Northwest transmission grid collapsed. The response in the Los Angeles area was to automatically disconnect over 575,000 customers — that equates roughly to 1.5 million people — to avoid a total power system collapse. It took us less than an hour and 40 minutes to restore 100 percent of the customers that were disconnected.

January 17th, 1994. The Northridge earthquake resulted in the first full-scale blackout that has ever been experienced in the City of Los Angeles. Within about 40 minutes, our power system operators had begun restoring customer load, and within 24 hours, we had over 93 percent of our customers restored. We've had visitations from around the world in the earthquake or seismically active areas to discuss how we had prepared ourselves and our infrastructures since we were able to come back so quickly after such a significant amount of damage.

April 1992, civil unrest affected much more than just the social fabric in the Los Angeles area. At its height, there were over 400 structure fires, and thousands of customers were without power as a result. We were able to work in tandem with police and sheriffs that were brought in, and department volunteers went in to restore electric service.

The point being: What have we learned? It's obvious we have had a lot of practice in the last couple of years. The most incredible disasters that involve Los Angeles involve earthquakes. Despite many system upgrades after the 1971 Sylmar quake, the shaking involved in the 1994 earthquake was literally unprecedented. As a result, we redesigned our seismic standards which now take into account not only how hard the shaking is, but how fast it takes place.

We're approximately in the first third of a $150 million retrofit project to bring our transmission infrastructure up to this new standard. We have developed some new computerized support systems involving earthquakes. One is certainly the connection to Caltech, the "Q" system, which provides us within a matter of moments with the

earthquake's magnitude, size, and location. This is a great assistance to the power system because, right away, you can begin damage assessment without waiting for the specific report to come in.

In addition to that, we have developed another system. It's called a fragility index. It lists all our facilities, not just electrical, but our facilities that house personnel. It will give us a reading of all of our facilities ranked in likelihood of damage order. It takes into account the age of the station, the construction, and the equipment that's there. This is also real helpful in immediately assessing where you want to allocate resources for restoration.

We have partnered with representatives in Kobe, Japan, and in New Zealand, as I mentioned, very seismically active zones. We have reviewed their response to disasters, and we have amended our own local procedures as appropriate.

A good example in Kobe was the destruction that was wrought on the transportation network. It makes relocating personnel supplies and restoring electric service extremely difficult, and we amended our helicopter utilization policies and decided where those helicopters could put down, staging of remote repair resources in response to those reviews.

What do we do in an ongoing fashion to protect our systems infrastructure? Certainly we have a wide range of comprehensive emergency response plans. They range from not only electrical supply emergencies but also into bomb threats, sabotage, or any credible contingency. We have procedures developed, and they are cited at all the various locations in accessible positions.

We have developed and use an emergency command center function, most recently activated during the August 10th disturbance. This allows us a single point of coordination with the City's emergency operation center. This particular entity provides us with the most rapid methodology to respond in an emergency to have an adequate infrastructure response in terms of management, dissemination of the media, and prioritization of load restoration.

This command center is supplied such that it can operate in a completely isolated fashion under complete lockdown for up to five weeks. We have on-site fuel supplies,

separate water tanks, backup generators, and emergency supplies. The longest we have practiced a lockdown for was 10 days. So we have exercised that machinery.

To supplement our own internal emergency training program, we are also required to complete the standardized management emergency training that is provided by the State of California. Our in-house business units conduct periodic disaster drills, simulating — typically we practice earthquakes, obviously, more often than not. And in emergencies, our system operators are empowered to take whatever action is necessary to protect the electric infrastructure without having to go up the command chain.

We think this is very critical in the emergency circumstances. We have seen where it's impacted and caused cascade outages. As the time expands for action, so does the approval chain associated with it.

In addition, we have standing orders that provide for the restoration of the power system, even if the command and control structure within the Department is broken up. As an example, after the earthquake, obviously, our main office building was not immediately functional, and the command structures were broken apart. The power system response is such it will take place under standard conditions without a manager there defining the priorities. It will happen on automatic.

We have emergency mutual aid contracts established with our neighboring utilities. They extend not only into power system products like energy or system reserves, but they also extend to transmission towers and physical equipment. We have even been known to share trained work crews under an emergency.

Our command center also houses a Western States information system that connects the majority of utilities in the Western United States. One of the functions of this tool is that it's used for sabotage alert. Any suspicious activities or actual acts of sabotage that take place anywhere on the Western interconnection, we are subsequently alerted. Any of the FBI alerts that come out specific to utilities, our control centers know immediately, and they can readjust the power system depending on the type of perceived threat.

With regards to our power system, our main power system operating computer is housed separately from any information system or network or other main frame. That's the way in which we ensure security for such critical activity as we literally hold our

power control system powers separate. They are housed at our command center which is a secure facility, and they themselves are powered not only by a power system interconnection, but they have a backup generator, and they also have backup batteries. We test all those systems regularly.

There is also an alternate computer control system if both the normal and the backup power control systems fail and if, in fact, the facility itself is damaged. And if we've lost both the main and the backup and the alternate control methodology, we can still control the power system from an alternate location that's kept confidential.

Our communications systems are, by and large, also redundant. We use, as you heard earlier, microwave hard wire fiberoptic. While we do operate our own internal trunk line for telephone communication systems, we have satellite backup phones available. That's in addition to your base issue of radios, cell phones, and other means of communication. The satellite hookups are such that, even in a severe earthquake, they can be manually aligned to the satellite and establish a single line of communication into the critical facilities.

THE MODERATOR: One minute more.

MS. EDWARDS: Thank you.

Reliable electricity is a service which is largely taken to be available, as you are well aware, until it goes away. We believe the Los Angeles Department of Water & Power has taken effective and prudent steps to develop an electric supply infrastructure which is not only reliable but is resilient and capable of withstanding all but the most catastrophic events and are able to restore service very quickly when service is struck.

Any questions?

MR. BRENTON C. GREENE: Harry Sizemore has highlighted that Los Angeles has, because of the natural disasters, and you have illustrated very positive examples of how your organization has been able to mitigate and accelerate the restoration of power to the Los Angeles population and its impact. We would appreciate any lessons learned.

You have done very many positive things that have assisted that. If there are any lessons learned that are applicable on a far broader basis — clearly, you have exercised many common areas, and it's something that translates in a far broader scale nationally.

MS. EDWARDS: Oddly enough, in addition to some of the lessons learned that we have not mentioned, some of the most simplistic involved a venture you are familiar with, which is simply practice. So many of the procedures or policies that are in place are not practicable; as an example, a lockdown of our command center facilities.

Until you actually practice it, you don't recognize there are a few things that will keep you from doing it. Had we had to do it in emergency circumstances first, it would not have been successful. That's one. The validity.

Communication systems is another. That is why we have as many backups as we do. The point Harry mentioned earlier is that we're lucky in that our systems are spread very broadly so the disaster has a less likely effect to hit all our systems simultaneously, with the exception of the Northridge earthquake.

The infrastructure is where we had some problems. We lost all but our last one or two backups and have since then added, yet again, a few more, and typically it's the media — it's not having additional lines— it's the media by which they are transmitted, the geographical zone by which they are located.

Spreading out the resources, trying to anticipate in advance where you need them, remote siting of equipment you may need in an emergency if people cannot be relocated fairly quickly, there should be literal stashes of repair equipment sited nearby for various areas. Those are probably some of the major lessons we have picked up.

MR. DAVID V. KEYES: We would appreciate receiving your thoughts in written form on the relationship of deregulation to redundant pathways or reserve capacity and whether or not there should be some floor of redundancy in reserve capacity beyond which deregulation should not allow or the industry should not be driven below that floor, such as in the banking institution. Certain financial reserves are required.

So if you have the time, we would appreciate receiving your views on that in written form.

MS. EDWARDS: We've done a lot of work on that, sir. We'd be happy to provide it.

Thank you.

THE MODERATOR: Thank you, Miss Edwards. I would now like to introduce Los Angeles City Council President John Ferraro.

MR. FERRARO: Mr. Chairman and members of the Committee and the Commission, I just want to, on behalf of the City of Los Angeles, welcome you to City Hall, to our City, and I know you have very important work to do and very critical work. Mayor Riordan would love to be here, but he's at the present time debating an opponent whose name will be left unmentioned.

I would love to stay a lot longer — in fact, I would love to stay all day — but I do have a dental appointment at noontime. So that's why I can't stay — not because you are such an attractive group of people. I did want to personally come down and thank you for coming to our City and hope our people are treating you well, and if there's anything that needs to be done, let us know.

Thank you very much.

MR. ROBERT T. MARSH: We thank you as well. Your people have been treating us very, very well. We appreciate all the fine arrangements.

Thank you, sir.

MR. FERRARO: Thank you.

THE MODERATOR: Before I call on our next speaker, if there is anyone in the audience who wants to speak and has not yet turned in one of these blue cards, would you please pick one up at the back table and fill it out so we make sure that everyone is heard from that wants to be heard from.

Our next speaker is Mr. Joe Bonino who is from the Los Angeles Police Department and Chairman of the Advisory Policy Board to the Criminal Justice Information Services system.

MR. BONINO: Good morning, Mr. Chairman, and members of the Commission. My name is Joe Bonino. I come to speak to you today as the elected chairman of the FBI's Advisory Policy Board to the Criminal Justice Information Services.

The Advisory Policy was chartered under the Federal Advisory Act to give policy advice to the director of the FBI on how to run all of the law enforcement services agencies provided by the FBI; the federal, state, and local law enforcement agencies. These include, among others, all the uniform crime reporting systems, the National Crime Information Center, which has a plethora of databases, critical databases, which are

accessed by police officers and by courts and corrections, probation, and parole officers every day, the National Identification System, which averages between 60,000 to 70,000 requests for criminal identifications everyday. All of this is part of the basic service provided by the CJIS Division of the FBI.

Also, the FBI is engaged in building two brand-new systems, virtually paperless systems, to conduct criminal identifications for law enforcement within two hours real time. That's called the Integrated Automated Fingerprint Identification System which will be on-line in 1999. And a major rebuild of the National Crime Information Center is called NCIC 2000, which, again, is highly advanced and has capabilities all the way down to police cars, fingerprints, and mug shots.

To support this as well, the FBI has built a very, very complicated wide-area network called the CJIS WAN to support all these present and future information services provided by the FBI and state and local law enforcement. Now, those of us on the Board have had the responsibility for giving the directors of the FBI advice on how to secure the system over the last many years, and the security was viewed somewhat traditionally. This was a closed system, and our major concerns were dial-up access and background checks and authentication of the users. That really has all changed with the advent of modern technology, especially the Internet. The cyber threat is growing literally by the day.

About a year and a half ago, the National Security Agency did an audit, an advisory audit, for the FBI to look into the impact of technology on the ability of the FBI to deliver these services in a secure manner and pointed out the serious threat provided by the Internet, and specifically the threat is most concentrated in places where the services come down the hierarchy of the network from the FBI's computer to the 50 states.

There is a switch in the state. That switch then goes down to a county or dispatch center, from a county or dispatch center to a local police agency. At a point where these switches take place, there is a possibility that the governmental entity is switching over other information and becoming more and more on-line, and it never really dawned on the criminal justice agencies that they were exposed to such a threat with the advent of the Internet and took a liability threat and magnified it geometrically. The potential is there for misuse, for trap doors, for spoofing, for all kinds of things.

We on the Board have reacted very, very seriously with that to set up a special ad hoc committee to study this. We developed a number of recommendations and discussed them with Director Freeh. The first thing we were able to do was hold the State control terminal officers responsible for having adequate firewalls in place. I think firewalls, in our view, are a short-term measure. We need to think about a lot better security measures. I think we are also going to be concerned about — I will just talk a little bit later about end-to-end corrections and, substantially, end user authentications to the director of the FBI within this year.

Just to give you some idea of the threat — and I know you have been provided some of this information off line — but there have been some documented, very serious threats where hackers not even from this country have been able to penetrate the system and shut down systems and possibly alter some data. We only know of a few of these, but it's the ones we don't know about that really scare us, and the potential is growing, as I said, by the day.

Just to give you an example of some of the kinds of information that are at risk, in the NCIC, National Crime Information Center, there is stolen vehicle information, and we have rules and security procedures to make sure that this is valid and timely data.

But if someone were able to alter a vehicle record or delete a vehicle record, that presents a potential problem for an officer-citizen contact. Obviously, if a record were removed and the vehicle were stolen, and a very dangerous person were driving the vehicle, the officer wasn't aware, you would have a very serious officer safety situation. This could remove Wanted Person information, and I think the danger is obvious from the example.

In the future I think we are going to need to take a very, very serious look at substantially improving, as I said, encryption, end-user authentication and that, we believe, could go as far as smart cards and certainly much more elaborate password systems and possibly biometric identification to make sure the users are indeed the appropriate users of this data. We believe that this may well cost a great deal of money.

One of the things I bring to you is something we probably will be recommending to the Director; we seek some assistance from Congress to help pay for adequate security

now that we are increasingly aware of the substantial threat to this vital national law enforcement data infrastructure.

I would be happy to answer of any of your questions about that.

Thank you very much.

MR. DAVID V. KEYES: Thank you.

THE MODERATOR: Thank you, Mr. Bonino. Our next speaker is Susan Herman, former general manager of the Los Angeles City Department of Telecommunications and now a member of the National Information Infrastructure Advisory Council.

MS. HERMAN: Good morning. I'm here actually representing the National Information Infrastructure Advisory Council, a group which is composed of folks such as yourselves who are willing to give the time. They are chief executives of communications corporations, telecommunications, and a few of us in government. I represented all cities and counties in the National. That was my role.

I wanted to share with you some of our thoughts. First of all, not to be egotistical about information technology and telecommunications, we found that it was the common thread among all the critical infrastructure that you have here before you today. It is often the way in which those infrastructures become efficient or effective and often is the only form of replacing them in the case of a disaster or some other emergency.

The example, as you've heard many times today from some of the speakers, is the Northridge earthquake, where our transportation highway went bust but our information highway remained robust.

The Council, in considering the issues before them and in laying the foundation, looked to five goals they felt were critical, and those five goals were first to make technology work for all of us as Americans. In other words, to advance the American precepts, the constitutional precepts that we believe in and our nation is founded upon. To recognize the diverse cultural values that are our hallmark as an American society and to ensure that sense of equity which is what our founding fathers and mothers were so critically concerned about.

The second thing we felt was, a major goal was to ensure that getting on-line would result in creating stronger communities, not just within our neighborhoods, but also on a national level as a national community.

The third thing was to ensure that every person in every community has an opportunity to participate. That means wielding this infrastructure in ways which are affordable, easy to use, and accessible. Not just in terms of physical access, but also geographical.

Fourthly, we felt it was important to maintain our world leadership and to continue to promote the values that we believe in so dearly in this country of open and competitive markets as well as producing and providing the services that we are known best for our ability to do.

Last but not least — and I think this relates a lot to the subject matter that you're concerned about — is that all Americans have to take the responsibility here, and the responsibilities are serious as they relate to issues, for example, of intellectual property, security, and privacy.

Recognizing every American and every entity that's involved in this has four major roles they play with information — they create it; they access it; they transmit it, or they receive it. We looked at ways in which we can set rules of the road that might be informative in our life and in our work.

And so we laid out rules of the road in seven major categories: electronic commerce, health, education, lifelong learning, government services, emergency management, and public safety — and an area which Gladys Knight would probably not like me to call it — but "PIPS." I call it "PIPS": Privacy, Intellectual Property, and Security. I'm sure she had a different meaning.

I can make it available to you if you haven't seen it, but in light of the time here, I would like to focus on two portions. One is emergency management and public safety, and the other is the intellectual property, security, and privacy area, because I think you'll see a common thread.

In the area of emergency management and public safety, first of all, we recognize it is critical that the information infrastructure always has the qualities of reliability,

redundancy and recoverability. Those were critical. But in setting out policies, we gave some guidance to the Federal Government that they should convene a broad-based committee of public sector and private sector people involved in the standard setting and involved in technology development; that they should confer on those subjects so that the needs of the public safety community are actually met.

The second thing we recommended is that they should define the standards in order to achieve the common protocols as well as standards for interoperability which is so critical for emergency management and public safety as well as criminal justice users.

We also recommended regional boards that would be created to review and make recommendations on the federal level very similar to the Criminal Justice Information System Advisory System that you heard Joe Bonino talking about. These regional groups would be key, for example, for examining large spectrum allocation and use in regions, and they would make recommendations. Clearly, this would promote and strengthen regional cooperation and effectiveness.

The fifth recommendation we made was that the federal government should promote the establishment of a standardized emergency management system. The system is the model for that in California. You heard other people testify on that, how well it has worked. It basically involved common terminology, interfaces, common law justice and standard information flow. The deployment of resources and mutual aid rely upon a common strategy, and that's what the system in California offers.

We also recommended the involvement of local community groups. We found, for example, after the Northridge earthquake, that duly authorized community groups, about 110 of them, provided so much vital information that it actually allowed us to more effectively and efficiently deploy our resources to the places where there was real need as opposed to them following standard protocol.

Those community-based organizations, when duly authorized, gave us intelligence we could not possibly have had using our municipal resources. We also felt it was critical to involve the news media, meaning the Internet, those with cable television, and multi-media. These are part of the information infrastructure. They are new players and need to be involved in this collaborative process.

Last but not least, we talked about the critical importance of training and education. Many times over, training and education are themes that came across in all we said and felt was important from the examples we had seen from others who had been successful in dealing with emergency management and public safety.

Now, going over to "PIPS," the privacy and information and security issues, we found, given our goal to try and create and disseminate information and create a richer breadth of information for the public, we also need a very careful balance of the issues of intellectual property, security, and privacy.

And so we said, first and foremost, it is related to intellectual property, which is important to promote the value of intellectual property and bring to our country respect and adopt similar policies to what the United States might be doing, particularly because we are becoming a global community, and global commerce is a major part of this information infrastructure.

In the area of privacy, we said that the work that was being done by the information infrastructure task force, the privacy work group should continue, and that our recommendations should be interwoven with those. In the area of security, once again, we recommended awareness involving all multi-entities in that and did not prohibit or inhibit the development or deployment of encryption by the private sector.

We also weighed in on the subject of free speech, and on that subject, we said that government should not, of course, regulate content; that we should defer to the private sector in the filtering and reviewing and grading mechanisms of parental supervision. But, again, we felt it was critical there be a collaborative effort in setting standards when they are set.

Bottom line, I think there is a theme here, a common theme, and that is that there should be collaboration on the standards and policies and guidelines as well as elaboration. In other words, after you have brought the parties in, expound upon them, find workable solutions, reiterate them. In other words, promote them, teach them, and ultimately educate and inform; continue that process.

Following those sort of four steps, we found that all of our policies and all of our recommendations made sense, and as we tried to set that information infrastructure in place, you then get to do the important job of helping to protect that critical infrastructure.

I recognize your challenge, and I am in awe of what you have before you. It reminds me of an anecdote of a man who wanted to increase the productivity of his assembly line business, but he wanted to do it at no cost. So he went to a Confucian master and said, "What can I do to increase productivity but at no cost?"

The Confucian master said, "Oh, yes. Have each person in your employ grow an additional finger, and they will become more productive." The man was overjoyed.

As he walked away, he said, "Master, how do I get them to grow an additional finger?"

The master said, "Ah, I am in charge of policy. You are in charge of implementation."

Commissioners, I wish you well in your endeavor as you try to help implement the policies before us. But I know you will do well, and we are available as a Council to assist you in whichever way we can. Thank you.

MR. DAVID V. KEYES: Susan, thanks a lot.

DR. WILLIAM J. HARRIS: I have one question.

In the early part of your presentation, I saw a total focus on the United States. Toward the end you did mention the fact we are in a global economy. But it's difficult for me to understand how in the early part we can avoid recognizing the fact that other people are making progress in their own computer telecommunications end and our industries are dependent on interconnections and, as they grow into international companies, therefore, and expect to in the future, how do you — to reexamine the first part of your presentation — examine it to be sure it relates to the international dimension of current economy?

MS. HERMAN: I didn't mean to make so fine a line, Commissioner. Actually, we talked a lot about the global community, and in the body of our work, I think you will see that kind of a flavor. I think there was concern about the infrastructure that we're developing, first at the local level and then the state, and it is growing out that way and ensuring its integrity and sort of embraces of all the policies and guidelines set here.

But you are absolutely right. It is not as if there is this sort of veil that can't be pierced. That is what makes this both so exciting and so challenging and the threat so real.

DR. WILLIAM J. HARRIS: Thank you.

MS. HERMAN: Thank you.

THE MODERATOR: Our next speaker is Dr. Carl Rathmann who is Dean of Engineering at California State Polytechnic University.

MR. RATHMANN: Good morning, and thank you. I very much appreciate the opportunity to comment and spend a few moments with you to reinforce what I believe is an already identified potential threat to our survival as a functioning nation.

Almost two decades ago, I was active in investigating the effects of nuclear weapons, particularly concerned with the consequences of what is called electromagnetic pulse or EMP. At that time, the world was essentially bipolar, and most of such research was funded by the Department of Defense and the Department of Energy. Much of it was and still is classified.

At that time the probable source of the threat was identifiable, and there was some urgency to the research. With the political demise of the Soviet Union, however, it appears some of the motivation and urgency for identification and defending against EMP, among other threats, has dissipated.

However, political threats in the form of unstable governments and terrorist groups continue. Given that certain degrees of EMPs cannot be generated via non-nuclear means, all that is needed for these threats to become attacks is sufficient resources to buy or steal the necessary technology and the will to do harm.

Almost everything mentioned here is available in the public domain and is regularly discussed in the professional literature. My interest in identifying this problem arises from my unawareness of any continuing recognition of EMP as a real threat to our infra-structure.

The EMP phenomenon arising from nuclear explosions was not very well understood before the 1960s and much investigation continued until the late 1980s. There continues

to this day a much reduced effort, notably in some of the national laboratories and in some universities here and abroad.

Briefly, in a nuclear detonation, gamma rays interact with air molecules to produce Compton electrons which travel outward much faster than do the heavy ions. This charge separation generates an outward-traveling pulse in the electric field, characterized by a rise time of the order of one nanosecond to magnitudes of kilovolts per meter. The nuclear EMP can be thought of as an electromagnetic shock wave with the strength of the pulse and the distance it travels before decaying to sub-threat levels varying with the height of the burst.

It used to be popular to point out that it is quite possible for nuclear bursts at high enough altitude, the EMP could be the principal damage mechanism to our nation's communications and transportation systems and could affect our ability to even mount a coordinated defense against secondary attack. It is certainly possible that a single nuclear burst at a high enough altitude could effectively disable the entire communications infrastructure of the entire continental United States, while causing only limited physical destruction.

This threat, as I indicated, has been well recognized for a long time. What has intensified the problem in the last two decades, however, in spite of a drastically diminished nuclear threat, is our country's explosively growing dependence on electronic circuitry. Perhaps the most insidious effect of an electromagnetic pulse, no matter how it is generated, is its attack on nonhardened semi-conductor based components of electronic circuitry, although it can generate large currents in the long conductors of telephone systems, power transmission lines, and even railroad tracks which then effectively become conductors of the pulse themselves.

Rather ironically, EMP is not as effective on the old vacuum-tube based technologies as it is on modern semiconductor-based technologies. Computer chips are key to countless industrial processes, power switching gear, both hard-wired and cellular phone systems, radio and radar receivers, vehicles, all computers and their networks, of course, satellites. You can think of a long list of additional examples.

All of these are particularly susceptible to electromagnetic attack unless precautions are taken. My observation is that outside the military, such precautions have been only infrequently taken. The EMP attacks semiconductors in a fundamentally simple manner. Relatively large currents are induced in the devices, causing them to heat beyond the melting point of the material, leading to shorts and failures.

Techniques for hardening components against EMP effects are relatively simple in principle and are well known to undergraduates, but they can increase the economic cost of a hardened facility or component dramatically. And, frankly, survivability has rarely been a design criterion for circuitry.

As I implied earlier, there are other, less dramatic ways to generate EMP besides nuclear weaponry. Lightning naturally generates a lower level EMP, for example. The EMP can be generated and focused locally by a weapon of rather simple design. Such devices have been under development in this country and others for some time, and such devices can in fact be quite portable.

While the weapon's area effects make remote delivery preferable, it is quite feasible that a small electromagnetic "warhead" can be delivered on a local target in a bomb-laden vehicle which is remotely triggered, a favorite terrorist weapon against urban targets. For larger targets, cruise missiles and aircraft become feasible delivery systems.

Remember that these systems are weapons of mass destruction; that they are designed to incapacitate information systems, not kill people. The attractiveness to an aggressor is understandable when one realizes the enemy can be defeated without causing much, if any, loss of life using these weapons. In my view, the United States can currently be defeated in this manner. This whole new way of conducting warfare is discussed in articles and books appearing regularly and authored by quite competent and knowledgeable individuals. This may sound like the stuff of a Tom Clancy novel. It could be, I suppose, in that the technology seems to be quite available to the public.

Commercial computer equipment is particularly vulnerable to EMP since very little energy is needed to permanently damage or destroy Metal Oxide Semiconductor (MOS) devices. Even if the devices are not completely destroyed, their reliability can be seriously degraded. And the tendency toward miniaturization in the design of electronic

components in order to achieve operating efficiencies has concurrently made such crowded designs that much more certain to be killed in toto by an EMP, perhaps by a pulse as low as 50 volts.

Clearly, the premise here is that complex organizational systems cannot function without the flow of information; data, commands and directives, assessment, and decision-making. Stopping the flow of information paralyzes the system and prevents effective and timely resource management. Furthermore, such a goal offers a very high payoff to the attacker with minimal risk.

The potential threats to our infrastructure, I think, are obvious. In principle, it is relatively easy to harden an entire stand-alone electronic system against such attack. Generally, if you can imagine a closed surface — think of it as a metallic balloon that completely encloses the system — that system can be protected. If, however, any conducting projections of that system — an antenna or power leads, for example — penetrate your imagined balloon, then hardening cannot be guaranteed because these pathways conduct the EMP into the heart of the system, and hardening requires some kind of circuit interrupt on each pathway.

As dean of one of the two largest engineering colleges in California, I am keenly aware of the obligation that engineering educators have assumed to help produce engineers for tomorrow who are technically competent and socially responsible. We regularly stress system approaches to engineering design, but identifying all constraints is often an art and always brings competing goals into conflict. All engineering design is tradeoff in nature. Never can one be assured that a design has been optimized in some absolute sense. If and when survivability to EMP or any other kind of threat becomes part of the constraints that manufacturers accept, then hardened designs will become the standard. It is more a matter of national will than it is of technological know-how.

I wish the members of this Commission well. You are engaged in an incredibly important service to this country, and I salute President Clinton for initiating your efforts. What I stated was more or less common knowledge among those of the technical community charged with such issues. As is true for all other types of weapon systems, defeating them is possible, too. However, contrary to all previous manner of conducting

wars, information warfare is civilian-directed and infrastructure-directed rather than being a primarily military action.

In my view, the private sector must recognize that it will be the likely target in future wars and terrorist attacks, and then support efforts for its own defense.

Thanks very much.

THE MODERATOR: Our next speaker is Professor S. N. Atluri of UCLA.

PROFESSOR ATLURI: I am a professor of Mechanical and Aerospace Engineering at UCLA, and I also direct the Aerospace Research and Education Center at UCLA. I would like to share some things with you.

At UCLA in the Aerospace Research Center, the primary concern is transportation infrastructure, nanosystem infrastructure and nuclear infrastructure. Basically interest has been shown in the past five years since the advent of research in aircraft security and aviation security, and the first thing we are concerned about is trace protectors in airport detection, primarily in a chemical and biological context; that is, basically chemical and biological. We are called upon to detect one part in a trillion, and it is a fairly challenging logical problem, and we are interested in looking at microelectronic devices to detect traces of chemical and biological warfare. We are also interested in bagging technology, and so on and so forth; primarily, means of airport and aircraft security.

And we are looking into ways of hardening aircraft, hardening baggage containers as secondary defense mechanisms in aviation safety. We are also aware that the FAA will be spending about a billion or so more dollars in the National Air Traffic System and aid to the Traffic Management System which would involve large computer databases and large computer software to make the dream of free flight — free flight being a pilot can choose his own code over the National Aerospace System — and then in addition to that, is soft base habitat, a new ground threat. And we at UCLA are conducting research into software protection against sabotage. And we all seem to get materials into nanosystem pipelines infrastructure, and so on and so forth, new nanosystems which might be useful in the detection of specific BW/CW agents. We also are interested in nuclear fuel, and so on and so forth. As I said, very technical topics.

It may be of interest for you to know that in the last two weeks UCLA, in collaboration with the University of California at San Diego, has proposed to the National Science Foundation the formation of a unified research center with the title Infrastructure Renewal and Protection.

So this in Los Angeles came to me only yesterday, but I would be happy to give you a copy of this proposal. So that brings me to the final point; that national infrastructure protection as a cooperative private industry — perhaps we could include universities also — because places like UCLA have been thinking about these problems, and large numbers of faculty are very much interested in these technologies of seeking protection and detection.

Thank you very much.

DR. WILLIAM J. HARRIS: I have a brief question. Did I understand you in the beginning to say that you thought some of the new nanosystems might be useful in the detection of specific BW/CW agents, and that you have a chance to do that?

PROFESSOR ATLURI: That's right.

DR. WILLIAM J. HARRIS: How far along are you in that kind of analysis?

PROFESSOR ATLURI: Well, I think the new technology board might be able to provide assistance to do that. I also serve on the FAA Advisory Committee on Aviation Security and Safety. And there are other places in the country that are also involved in this nanosystem.

But we at UCLA, we believe in that.

DR. WILLIAM J. HARRIS: Thank you very much.

MR. BRENTON C. GREENE: I would be interested if you could submit to us in writing some more details about everything you are involved in. It sounds very interesting and unique to the things we have seen nationally.

PROFESSOR ATLURI: I would be very happy to send you a copy of that. Thank you.

THE MODERATOR: Thank you, Professor. I would now like to call on Nancy Markle from Home Savings of America who is going to talk on financial service threats as well as her recommendations.

MS. MARKLE: Good afternoon. I am going to focus my comments on the financial services industry in general and not particularly the company that I come from.

In today's world, the issues for the financial services industry are increasingly complex. We used to have the mainframe computer, and it was tightly monitored, and we had tethered to it terminals, and we had what we call a closed loop system. But in today's world, we have centralized processing. We are highly networked, and we have decentralized access as well as control, not only across our companies, but across the world. The world has grown increasingly complex, and the weakest link affects all of the networking and interactivity.

So what are those weak leaks and what are the responsibilities associated with them? First of all, they are the physical threats, the threats that we see everyday, the electronic threats. And then there are the hidden vulnerabilities, and I will talk about all of those and how they appear to us and some of the recommendations that we would like to suggest.

First, the physical threats. The first one, of course, is crime, and that's a very diverse area. Includes not only the hacking type of crime electronically, but physically, unauthorized access makes a lot of headlines. When we see crimes like the stealing of equipment, robberies, and killing like we saw with the North Hollywood bandits in the Bank of America situation, those are really horrifying, and they are very visible.

When we think about the impact of a stolen laptop from a salesperson or a customer service representative of a company, when that equipment is gone, all the information on that equipment is available to whoever has stolen it, and it may be important information of that company or the person or the customer.

Also, having to recuperate that information and get it back is of great detriment to the company and a real time-waster in productivity and a hindrance. When we think of national disasters such as earthquakes, fires, floods, hurricanes, et cetera, these are very serious impacts to our business as well as to our personal lives. And the sharing of information such as Florida used when they were — Florida has a very good hurricane situation where they can recuperate from hurricanes rather quickly. When the hurricanes hit the Northeast, and it was unanticipated that they would, a number of people from Florida went up to help in that situation; to help restore the services and the capabilities

of people. Sharing information in that way has been very helpful in the national disaster-type situation.

Of course, businesses have to also be prepared for disasters and have business resumption capability different, of course, by the business. In the financial industry, it is a very serious situation. A lot of money, time, and effort is spent on assuring that we can recuperate the business in the event of a disaster, either where we are currently operating or someplace else.

Terrorism is another form of physical threat, and that is one that makes us feel very vulnerable. We have witnessed the horror of airplane bombings, of building bombings, of mail bombs, and hostage taking. All of those are very frightening, and these are things that are facing businesses as well as government everyday.

Another is service interruption. All of us are dependent on utilities for electricity to keep our businesses running. What happens in the event that we don't have electricity, that we don't have access to transportation and other services that we take for granted? Putting physical threats aside and looking at electronic threats, this is a different world.

You have things like unauthorized access, people who are accessing your computer who have no business coming into your computer. This can be in the form of hackers, in the form of people who are just trying to do it for the fun of it, or people who actually want to do harm to your business and interrupt the capability of your business to operate.

One of the greatest exposures is ex-employees who know your business and know how you operate. A lot of the potential in ex-employees or even existing employees who are disgruntled is something that each company has to pay very close heed to.

Having insufficient security is also an electronic threat. And then the question occurs, of course, what is insufficient security? Because you no longer have a closed system, because you are so exposed, you are now operating not only within your own company, but you're working with other companies, suppliers of information.

For example, in a financial institution, you might be connected to Value Line or Knight-Ridder, or any one of a host of financial institutions. You also might be out-sourcing some of your capabilities and services, and when you're outsourcing you may be

connected directly through computer to computer to your outsourcing vendor. You also have the opportunity to be connected directly to your customers.

So we now have banking on-line as well as financial services on-line where customers can get on their own computers or, through the telephone, connect directly to a computer or a person at the other end and do their business. All of those have the opportunity for intervention that would be unauthorized.

Another is viruses and malicious codes that can infiltrate your computers. People are very concerned about viruses coming in through the Internet, and so forth, but what we are finding is that a lot of viruses are being introduced inadvertently by vendors, consultants, and people bringing information from their home computers.

And then there is electronic fraud: telephone, mail, the use of cellular and radio waves being accessed by people who have no business or are piggybacking on your particular telephone number and charging to your telephone number the services they are using.

So there are a lot of threats in the electronic world. The electronic world brings a whole new dimension of thinking. We are now crossing borders, we are crossing time, we are crossing laws, and we are crossing ethics. We are having to think about all of these in totally new and different ways than we thought of things in the past, and all of these things are moving very quickly.

For example, the electronic world is extremely discrete and knows no borders. When you send goods or services electronically, there is no Border Patrol that is going to examine and make sure that those goods or services are legal or that you are paying taxes on them.

In terms of time, in the fiscal world, when a crime is perpetrated, there is some time to examine the crime scene, to look for criminals, to look for people who might have seen it; but in the electronic world, time does not have a dimension. Electronically, you can perpetrate a crime in many countries to many businesses to many people all at the same time. In terms of laws, we have dealt with, in the fiscal world, laws that deal with our local environment, our state environment, our country. We don’t have laws that deal across the world, laws that deal when we cross all of these borders which law takes precedence.

Which is the governing body from between us and Russia for the hackers who hack into Citicorp? Who was the governing body there when those people did it when we knew or at least the governmental agencies tracking that crime knew it was going on? Citicorp knew it was going on, and nothing could be done about it because the laws in Russia did not accommodate this particular situation. We had to wait till the people left the country, and fortunately, they did.

And then ethics. We all have been taught as we grew up that to steal someone's wallet or to steal a purse is not good; that this is something that the people frown on. But how many of us have been taught that to take the diskettes that I have on my desk and put them in somebody else's computer and use them that that is also a crime? So we have a whole new way of thinking about things that haven't applied before, and we have to address these threats in cyberspace.

There is an additional vulnerability, and that is called the "Year 2000 Threat." And this is something that we believe is probably the most threatening and concerning of all the activities going on right now. And probably the one that is more often swept under the rug because people do not want to spend a lot of money on something that is not considered value added.

Now, it is important if you want to have continued business, but it does not add to your product a new service or value services. It just allows us to continue doing business. There is an article in *Information Week* from March 3rd, and it talks about some of the things that are going on from the Government's standpoint.

The White House says, "The Fed will be ready."

The General Accounting Office says, "I don't think so."

The Office of Management and Budget says, "All federal year 2000 fixes will be tested and done by late 1999 and will cost $2.3 billion."

Systems experts say, "We don't think so. The administration is vastly underestimating the cost and the amount of resources required to get the job done."

So we have a very significant threat, not only to our businesses, but to our government and to the ability of our businesses and our governments to interact, because we are all interdependent. When we look at the cost, some of the research numbers are coming

out $300 to $600 billion worldwide to fix the Year 2000 problem, and 60 percent of that is the United States, because we are so sophisticated, so technologically advanced, and so interactive, we are the country that is most vulnerable to this Year 2000 Threat.

Some of the recommendations that we have, first of all, is that government and business work together unfettered — and I know you are going to laugh at me — apolitical — the business initiatives — some of the business initiatives, and there are some really good examples; the secure electronic transaction, a payment protocol designed to protect the consumers bank card information. This has been developed by MasterCard, Visa, GTE, Microsoft, and Netscape working together in a collaborative effort.

This is an example of business and government setting standards and working collaboratively in a positive way. Today's *Wall Street Journal*, and I am quoting from "Personal Technology": "U.S. Robotics concedes that an old FCC regulation limits the legal maximum speed," and they are discussing modems to 53 kilobytes per second. So the limitations on our modem today is an obsolete law on the books.

There is information sharing, allowing businesses and government to share the information and knowledge that they gain. One example would be understanding what's happening in the criminal environment and sharing what's happening. Too often financial services organizations don't want to make very public the infringement on their security or robberies because it affects the trust of their customers. But we do share this information with some of the governmental agencies.

The question is: How can we share the information across business and government so that we can work together to be more secure as well as to fight crime across the country?

Another area is education. Being knowledgeable about how to deal with a problem where security is breached, what do you do about it? Just like in the hurricane situation where a group of people went from Florida to the Northeast, we also need to be prepared for when we are invaded with these threats, these electronic threats. How do we deal with it? What do we do about it and how do we coordinate a collaborative effort in terms of educating people to effectively utilize the knowledge?

Another area is on international laws so that we can impact when we have hackers or people perpetrating crimes in other countries. How do we deal with this internationally so that we are helping each other as country to country globally to be an asset to make sure that criminals are clearly punished; that they understand that these are crimes; that these are things that need to be addressed, and that they are punishable?

And the last consequence or last recommendation that we think is really important, and that is, we are a very innovative country. We have been a leader in technology, and this has largely been led by our Government. And we need to continue that leadership role. If we look at some of our security-type of events that have happened in the past, we look at encryption. Encryption came from government sponsorship. If we look at the Internet, the Internet was spawned through government sponsorship. These types of innovations are what have led the United States in the electronic world, and we need to continue to be leaders in technology innovation as a country.

And lastly, we need to share the research, the understanding on the Year 2000. We need to make sure that our businesses, our vendors, and our country, state, and local governments are all prepared to deal with this event because it is something that is extremely serious. If we can't be ready, the current research projections are that there will be $3 trillion in litigation associated with the Year 2000. I hope that won't be in the United States.

Are there any questions?

MR. DAVID KEYES: You spoke to the issue of information exchanged between the Government and the private sector on threats to and vulnerabilities of information systems in the financial world. We would be very anxious to hear from you, in any form you chose to give it to us, what would incentivize the financial industry to exchange this kind of information, realizing that the reputation of the institution can be affected by premature disclosure — or any disclosure — and we see great reluctance to put the good name of an institution in jeopardy and certainly understand that.

But if you could point us to a center of thinking on how that mechanism might work or what sort of institution might be appropriate for that sort of exchange, it would be very valuable to our exchange.

MS. MARKLE: That's a very good question, and I would like to give you my off-the-cuff thoughts. There are already a lot of activities underway, I think. In talking with some of the Council members yesterday, we talked about what's going on in New York, some of the collaboration between financial institutions in New York. That's also happening in Chicago. The financial institutions recognize such a very serious situation that some of them are collaborating.

There is also the American Bankers Association — excuse me, American Bankers Roundtable — that collaborates on a number of serious issues; some of them being security, payment systems, and so forth. So there were a number of forums available for doing this, and the financial services industry realizes that this is very serious. The issue that you bring up about the sharing of information, that's something that really is important. The confidentiality associated with this would be a key to having this be a collaborative effort.

But given confidentiality, I think you will find that financial services companies would be very anxious to cooperate.

MR. DAVID V. KEYES: Is the issue of antitrust a problem for collaboration on information sharing?

MS. MARKLE: That's an excellent question. That is really an interesting situation. We have found in some cases when we are, as a group, putting the financial institutions together and working collaboratively with a vendor, they may feel a little threatened by the fact that they have a number of big banks asking them questions. Antitrust is thrown up very often. We are super, super conscious as an industry about antitrust.

So it is a very important question, and it's something that we normally include attorneys in, to make sure that antitrust isn't an issue in each of our meetings. So this is one of those examples of a law that can be used positively and also used negatively.

MR. DAVID V. KEYES: Thank you very much.

MR. BRENTON C. GREENE: Thank you very much for the opportunity to meet with you and your staff yesterday as well.

MS. MARKLE: We enjoyed it, too.

THE MODERATOR: Thank you very much. That was our last speaker, and this is your last chance. If there is anyone left in the audience that hasn't spoken that would like to address the Commission, speak now.

Do you have any final remarks you would like to make?

MR. ROBERT T. MARSH: Well, we simply want to thank you all for your fine inputs. It's been enlightening, and we'll take your comments and remarks seriously, and in those cases where you have offered to provide us further information, we appreciate that, and we will follow through with you to obtain that.

Thank you all for coming.

*(The Public Meeting was concluded at 12:34 p.m.)*