



THE PRESIDENT'S COMMISSION
ON CRITICAL INFRASTRUCTURE PROTECTION

TRANSCRIPT OF A PUBLIC MEETING

HOUSTON CITY COUNCIL CHAMBERS
HOUSTON, TEXAS

MAY 13, 1997

LIST OF SPEAKERS

Ms. Janet Abrams, Moderator 1
The Honorable Bob Lanier, Mayor of Houston 1
Dr. John Powers, PCCIP 5
Ms. Gaynelle Jones, United States Attorney 7
Dr. Richard Winerdi, Texas Medical Center 10
Mr. Jimmy Schindewolf, City of Houston 13
Judge Robert Eckels, Harris County 14
Mr. Eddie Corral, Houston Fire Department 16
Mr. Sam Goodhope, Office of the Attorney General, State of Texas 18
Mr. Mike Green, TU Electric 21
Dr. Kenneth Mattox, Baylor College of Medicine 25
Mr. Mike Turner, Southwestern Bell 27
Mr. Robert MacLennan, Metropolitan Transit Authority, Houston 31
Dr. Naomi Ledé, Texas Southern University 34
Ms. Shelley Leavitt Nadel, National Association of Corrosion Engineers 36
Ms. Laverne Hogan, Greater Harris County 911 Emergency Network 40
Mr. Jim Shepard, Conoco 42
Mr. Chase Untermeyer, Commissioner, Port of Houston 46
Dr. Mitchell Morris, M.D. Anderson Cancer Center 49
Dr. Hugh Stephens, University of Houston 53
Dr. Joshua Hill, Texas Southern University 56
Mr. Bill Bostic, Oklahoma Association of Contingency Planners 57
Dr. Larry Leibrock, University of Texas 60
Dr. Joe Moore, Southwestern Texas State University 62
Dr. Richard DeMouy, Southwest Texas State University 64
Dr. Tom Talley, University of North Texas 68
Dr. Michael Carroll, Rice University 69
Mr. Richard Baker, City of Houston 71

| | |
|---|----|
| Dr. Robert Hiromoto, University of Texas at San Antonio | 73 |
| Dr. Wayne Sorenson, Southwest Texas State University | 75 |
| Dr. Ben Zon, Southwest Texas State University | 76 |
| Dr. Pedro Lecca, Texas Southern University | 77 |
| Mr. Mike Wisby, Texas Engineering Extension Service | 79 |
| Dr. Swaroop Reddy, University of North Texas | 81 |

JANET ABRAMS: Good morning and welcome to the Houston public meeting of the President's Commission on Critical Infrastructure Protection. My name is Janet Abrams, and I am the White House liaison and director of external affairs for the Commission, and I'll be moderating this morning's proceedings. This is the third in the series of regional discussions being convened by the Commission across the country. Our first was held in Los Angeles in March. We were in Atlanta in April, and today we are very honored to be here in Houston.

I'd like to begin by thanking our generous host for the meeting here today, Mayor Bob Lanier. Mayor Lanier brings to the discussion of critical infrastructure protection a broad and distinguished background in business and government, and specifically a significant record of leadership in the field of transportation, one of the core infrastructures that the Commission is studying. And now Mayor Lanier will officially open the proceedings.

MAYOR BOB LANIER: Good morning, and welcome to all of you to this conference. I both welcome the expertise that's here and look forward to learning from the conference, in terms of protecting our critical infrastructure, both physically and I think the material speaks of cyber protection.

I see Dr. Harris is here from the Texas Transportation Institute at Texas A&M, and I've worked with him over the years on transportation systems. And I'd like to take a moment to say that, while we do face terrorist risks and we ought to protect ourselves against them, and while we do face risks from destructive elements in our society, and we ought to do what we can to protect ourselves against them, probably the biggest enemy of our critical infrastructure is simply neglect; we don't spend enough money on it to keep it up and keep it from being dangerous.

If you look at highways in recent years, the interstate in Los Angeles probably fell down right after the earthquake as a consequence of inadequate maintenance. And if you look at a major bridge in New York City, it fell into disuse because over the years it had not been maintained and it got to where you could just take and push your hand into it. And the idea occurred that it was unsafe.

And let me digress a moment to say that this point of view is one that we really try to follow in this city. I'm not just saying something that we at least are not trying to follow. If you look at our general fund budget, we spend a little over half of it purely on the two safety departments, on the police and fire. And that's a little over a billion-dollar general fund budget. In addition, we spend about 500 million dollars a year of capital expenditures on bond funds and another proba-

bly hundred million, maybe six, seven hundred million dollars a year on bringing our infrastructure up to standard.

We completely redo fourteen neighborhoods a year. We completely redo fourteen parks a year. We will have completed at the end of this next year a replacement of our water and sewer system along with security features into water and sewer system. That costs two million dollars. You may recall seeing in a Washington paper that oftentimes the water in a nation's capital is simply unsafe to drink. And that doesn't come about through a terrorist. That just comes about through not keeping it up. And not keeping it up isn't complicated, it isn't technical, it isn't even modern. It's just old-fashioned. It's the idea if you've got a piece of property and you don't keep it up, it runs down, and that's probably the most sinister enemy we have.

I chair a group called Rebuild America, and I won't go over the numbers with you, but our history shows a steady decline of the percent of our government's money that we spend on keeping our infrastructure. And it's a kind of "pay me now or pay me later" point of view. The Hearst publication recently ran a national series in which they talked about our nation's water supply as a danger from within. They talked about worn-out pipes where you had pollutants coming into them, they talked about a nation still dependent in the main on an underground water supply where they need to shift to surface in many areas, and where that underground supply in some cases is running out, and in some cases is just no longer safe.

But if you look at the number of people whose health is jeopardized by a faulty water system and compare that to the bombing in Oklahoma City, although one is enormously dramatic and the other is not, I would submit to you the danger in the former is more certain and more life-threatening and will terminate more lives. Not that we don't need to do it all, but if we're not going to keep it up, if we're not going to keep up what we're protecting, it won't do us near as much good to protect it.

And let me just take something going on in our state now. Across this nation, we have about a hundred billion dollars of deferred maintenance in our nation's public schools, where we send children to school, and our future is no more secure than their ability to learn. And the *New York Times* recently had a series on the horrible conditions in New York City, where they had children learning in rest rooms and the fire escapes were inoperative.

We recently had a roof fall in one of our lower schools. And we had a bond election. HISD did that in our city, which I supported, but it lost, lost a bond election just to rehabilitate the schools to make them decent, make them safe where our children go to school. We're just in the process of curing the most flagrant of the fire code violations in our schools. And I would suggest to you those violations exist in every city in this land. What I'm talking about is not a specific item, really, but it's an attitudinal thing. You find in public service—by that I mean in jobs like I have—that it doesn't show if you cut the maintenance budget. The problems arising from that kind of slide on to the successor or even the guy after that. And yet I think it's something that we badly need to consider a moment.

If you look at this state, what's going on now, we're having a monumental political struggle in this state to shift—the state has about a billion dollars of the funds that they won't spend in the budget, and they're moving it back to the area schools. We do see ad valorem taxes by that amount, and then put some new taxes on, so it's kind of a shift of taxation, but with no additional monies coming to the schools.

So that billion dollars out of the state budget moving to the schools to shift the tax load from one group to another, which is probably a pretty good thing, probably a pretty sound objective. But it doesn't touch—it doesn't touch the ten billion dollars, the deferred maintenance we have in the state schools. For that reduction simply to go to there rather than being shifted, we'd have something to protect. That is to say we'd have the state schools in A-plus shape.

I guess two last things I'd mention on this. One is that these neighborhoods we're doing in the main are in the inner city, although our program would extend to the entire city. Housing, streets, water, sewer, drainage. Drainage, you know, if you don't let the drainage go out, you end up flooding people's homes. You can have one flood in many of our cities that will do more damage than some of the spectacular terrorist events and which simply aren't being tended to because really mundane things like cleaning out storm sewers and making new storm sewers is not being tended to.

But I think that allowing our inner city neighborhoods to deteriorate in terms of the structure, in terms of the physical structure the government pays for, brings enormous damage. Societally, I think it's a breeding ground for crime. We have cut crime here. We still have 130,000 major crimes a year. I think you help yourself if you have decent places for people to live. Now, having said all of that, I really admire the program, the federal program of helping with the number of

police officers. It probably ought to be augmented. I like the idea of starting at least to think about helping some with the schools, but it needs to be more than symbolism. You can't create a hundred billion dollar program with a hundred dollars a year. You can't even keep up with how fast it's going down.

I welcome you all here. I look forward to learning.

But I would say to you that, as important as it is—and it really is—that we send people to the terrorist schools and we're trying to learn and we have a special program about protecting our water and we've added 1,300 police officers in the last five years, so we believe in security, and we believe in safety. But our safety of the larger rest of the country is we're not doing the basics to attend to the infrastructure so we'll have something really worthwhile to protect. Now, thank you, and welcome to the city.

JANET ABRAMS: Thank you, Mr. Mayor, and thank you very much for your hospitality, the work of your staff who has been very helpful, and for your active interest in the work of the commission.

I'd like now to introduce the members of the commission who are here with us today. By executive order, this group is a mix of individuals representing both private business and government. Beginning with Mr. Brenton Green. He is the commissioner from the U.S. Department of Defense. Then Mr. Paul Rodgers, former executive director of the National Association of Regulatory Utility Commissioners. Dr. John Powers, the commissioner from the Federal Emergency Management Agency. Ms. Nancy Wong, an executive with Pacific Gas & Electric Company in San Francisco. Dr. Bill Harris comes to the commission from the transportation industry. He brings professional experiences from the Association of the American Railroads, and, as the Mayor mentioned, the Texas Transportation Institute of Texas A&M University. Then we have Mr. David Jones. Dave is the commissioner from the Department of Energy. Then Professor Mary Culnan on faculty of the Georgetown University school of business. And then Mr. Peter Daly, the commissioner from the U.S. Department of Treasury.

Chairing this morning's proceedings will be Commissioner John Powers, and I'd like now to invite Dr. Powers to give a brief overview of the President's Commission on Critical Infrastructure Protection and our work. And following Dr. Powers' presentation, the public testimony will begin. Dr. Powers?

JOHN POWERS: Thank you, Janet. Thank you, Mayor Lanier. And we are delighted to be here in Houston this morning. He certainly gave an eloquent statement on why it is important for us to keep our infrastructures in good shape. I can provide at another time terrible examples of what happens to cities when they fail to do so.

Our purpose here today is to build public awareness about the threat to America's life support systems, its critical infrastructures, and to hear your views on what we should and what we should not do to protect these vital systems.

The commission was created last July 15th when President Clinton signed an executive order that begins: "Certain national infrastructures are so vital that their incapacity would have a debilitating impact on the defense or economic security of the United States." In recognition of that possibility, the commission has been tasked to recommend to the President a national policy and an implementation strategy for protecting the nation's critical infrastructures and for assuring their continued operation.

So what are the critical infrastructures? They fall into five basic groups. First, systems we call vital human services. These include water supply systems, fire, police, medical, and rescue services. The next is the federal, state, and local government services that protect our freedom and help to provide for our quality of life. The second group is the financial services industry, where trillions of dollars flow through electronic and other systems daily. The impact of a disruption here would be severe. Another group is energy. This includes electric power, natural gas, petroleum. These are critical systems that provide the light, heat, and cooling and make us the most mobile people on the planet, the systems that fuel the American industrial engine.

The newest and fastest-growing infrastructure is the electronic distribution of information. America has pioneered tremendous advances in communications and information technology. We have reaped extraordinary benefits from these developments. But our new reliance on these systems exposes infrastructures in new ways and creates new vulnerabilities.

The final infrastructure category is what we call physical distribution. This group includes most of the means by which we transport ourselves and deliver our products and services.

And what exactly makes these infrastructures critical? Let me pose the answer in the form of a question. Do we have some points of failure that could prevent us from effectively mobilizing our military forces for an eventuality such as Desert Shield? We think so. We certainly know that somebody could delay us and hinder us significantly.

Do we have some points of failure that could create losses on the order of the savings and loan debacle? Probably not today. But in the future, it's a good possibility.

Do we have points of failure that could introduce widespread destruction, cause loss of lives, damage to public and personal property? Absolutely. Just how great the effects might be are a matter of debate. But we all agree that the potential effects are sufficient that it merits the attention of the nation.

The question we are often asked is why now, why this commission now. The answer is that we want to address this issue before a more serious problem develops. Today we are confronted with an entirely new set of hazards that are man-made. Technology has created an interconnected world. Each connection creates new exposure, new risk. Companies are becoming increasingly vulnerable to theft, unscrupulous competitors, malicious hackers, insider cyber attacks, criminals. The tools to exploit these vulnerabilities are readily available. All it takes to penetrate some automated systems is a PC, a phone, and skills that many 14-year-olds have already mastered. Within this context, the commission's mission is to assess vulnerabilities and threats to critical infrastructures, identify relevant legal and policy issues, and assess how they should be addressed, recommend to the President a national policy and an implementation strategy for protecting these critical infrastructures, and to propose any necessary statutory and regulatory changes.

Most important, we recognize that most of the critical infrastructures are owned and operated by private sector. Hence, the cooperation and collaboration between the public and private sectors is absolutely essential to the commission's success. We are vitally interested in what you have to say because it is you that owns and operates most of these critical infrastructures. Together, the public and private sectors can develop common solutions to common problems and secure America's future.

But, we need your help; we need your ideas; we need your participation. We need everyone's best thinking up front, so we encourage and welcome your input. That's why we are here today, to listen. That is the only way we will find solutions that will work for everyone.

So, again, we appreciate your being here today. We appreciate Mayor Lanier taking his time to be here, and we are looking forward to hearing what you have to say. Finally, should you wish to talk to us at any time after this morning—and we hope you will—please write or visit us on our World-Wide Web site at the address shown on the screen [<http://www.pccip.gov/> —*Ed.*]. Thank you very much. Janet?

JANET ABRAMS: Thank you, Dr. Powers. Before we move on to the public testimony, I need to offer a note about time. We have a very full program this morning. We've gotten terrific response from the region for this morning's meeting, and my job is to encourage us all to keep to the schedule and to give everyone who has come a chance to speak. Each presenter has been asked to limit his or her remarks to ten minutes, and I'll be watching my watch, and when you hit the nine minute mark, you will see this sign. The "one minute" orange sign is a subtle reminder that it's time to wrap up.

Please know that after you have used your ten minutes, you'll have the opportunity to have your full testimony in writing submitted for the official record of the commission, and as Dr. Powers mentioned, we encourage continued dialogue with the commissioners beyond this morning's meeting.

Also, I need to add that because the interest has been so great in this discussion today, we've asked commissioners to limit their questions this morning. We're here to hear from you and eager to hear your input, and you won't be hearing that many questions from us today in the interest of giving everyone a chance to speak. If anyone has an interest in speaking and has not yet filled out a card at the sign-in table, please do so now or in the next few minutes so we can get you on the agenda.

We're ready to begin, and I'd like to invite our first presenter, Ms. Gaynelle Jones, U.S. Attorney. Thank you.

MS. JONES: Mr. Chairman for the day, Mr. Powers, and Commissioners, I'm Gaynelle Gingrich Jones, United States Attorney for the Southern District of Texas headquartered here in Houston with branch offices in Corpus Christi, Brownsville, McAllen, and Laredo. I want to thank you for this opportunity to appear before you and provide comments on behalf of law enforcement throughout the 43-county district on one of the most important issues our government and society face today—responding to the threat to our critical infrastructure from terrorists and other forms of attack.

As the chief federal law enforcement officer in the 43-county district which makes up the southern district, I can tell you that the federal, state, and local law enforcement is doing all it can to prepare for the threat to our infrastructure industries, from domestic and foreign terrorists.

Although we have not experienced a catastrophe of this nature, under the leadership of Attorney General Janet Reno and the former Deputy Attorney General Jamie Gorelick, U.S.

attorneys throughout the nation have begun to work with the FBI and other federal, state, and local law enforcement agencies to plan for crisis management in the event of a terrorist attack within our districts. I have participated in joint programs and practice exercises with the FBI, the Houston Police Department, and the Houston Fire Department in exercises that are aimed at preparedness.

The focus has been on efforts to protect, prevent, halt, and confine attack, along with education and training on attack response. We believe it is essential for there to be coordination of law enforcement in responding to this problem. The southern district includes the fourth-largest city in the United States and is the center for major petrochemical production, space exploration, and medical research, including the Port of Houston, one of the busiest sea ports in the world.

We fear it is only a matter of time before we face a terrorist attack. Last year, the FBI found two fake explosives at the Texas City oil refinery after a bomb threat was phoned in by a terrorist. The refinery was one of the world's major petrochemical complexes located on the heavily traveled Houston Ship Channel. The threat resulted in the shutdown of an entire complex, including the channel, for several hours, while law enforcement and the Texas City fire department conducted a search and investigation. We had a real demonstration of the potential harm which can be brought on an industrial complex. Fortunately, there was no bomb, but we were all concerned and are concerned about what will happen next time.

My office is working with the FBI in this investigation, and all crimes where federal criminal law can most advantageously be used to the fullest extent possible to prosecute the culprits of these crimes. Threats of violence against federal facilities has become a reoccurring problem throughout the district since Oklahoma City. Last year the building which houses the FBI office in Laredo was burned in an arson attack. Security at all the federal buildings has been beefed up significantly as a result of these threats. With a major international airport in our city, we fear the devastation should the occasional reports of explosives on airplanes destined for this city become a reality.

Our role in law enforcement is to aggressively investigate the threats and crimes and, to the extent appropriate, maximize the punishment of any perpetrator found. We realize that we must send a message through the criminal justice system that anyone engaged in conduct of this nature will be prosecuted and punished. In addressing computer crime affecting the industry infrastructure in the district, law enforcement sees as its role to coordinate its effort. Today we have the

Houston Area Technical Support group, or HATS, an interagency group of law enforcement officers and incorporates involved in the investigation of computer-related crimes. HATS was created to coordinate the district's limited technical investigative resources, which are facing increasing demands from the criminal use of computers and sophisticated electronic devices. The HATS group meets quarterly and provides training at the Houston police academy for local, state, and federal enforcement agents and incorporates. The HATS members' primary goal is to network and share potentially significant intelligence leads. It a good start, but we know it's not enough. Law enforcement at the local and state level is ill equipped to handle the potential threat from a knowledgeable computer hacker.

Experts tell us that no computer system is completely invulnerable to the skilled hacker. We found this out last year at the Department of Justice, when its web site was penetrated by hackers and caused disruption of our computer web system for several months. We have not had prosecutions in the southern district involving computer hackers as yet, but we continue to work with the FBI, the Secret Service, and local law enforcement in our efforts to try and stay on top of this rapidly developing area. We are proud of the law enforcement efforts to address these problems, but we know they are simply not enough. Much more is needed if we are going to head off the frightening prospect of the dangers from the threat of information warfare and other infrastructure industrial vulnerabilities.

We applaud this commission's efforts towards development of protective strategies and its recognition that government and private industry must be involved in addressing our vulnerabilities. On behalf of the federal law enforcement community, we offered our continued support in any way needed towards accomplishment of our shared goals of protecting our community and our nation from the potential disrupting and devastating threat from infestation of our infrastructure.

DR. BILL HARRIS: Can you help us know the extent to which you are coordinating your efforts also with the people who may be penetrated—with the banking community, for example? Do you share information with them on the nature of the threats that you begin to perceive, or is this coordination primarily within governmental institutions at the present time?

MS. JONES: We are doing both, Dr. Harris. With respect to the banking institutions, working with law enforcement, particularly the FBI, which has had chief responsibility going back in investigating financial fraud that we had, there are working groups and other opportunities to

meet and share with the private industry. It's an ongoing process, and where we find that we have problems, we have been working with those groups. Thank you.

JANET ABRAMS: Thank you very much. Our next speaker is Dr. Richard Winerdi, President and CEO, Texas Medical Center.

DR. WINERDI: Thank you very much, Mayor Lanier, chairman, ladies. It's a pleasure to be with you today. The Texas Medical Center is the largest of the 126 academic health science centers in the United States. As a matter of fact, it's the largest medical center in the world by a factor of three. It is composed of 42 institutions, sixteen of which are hospitals, and it has 6,200 active hospital beds and 600 bassinets, most of which are full every day. The Medical Center consists of institutions of federal government, state government, county government, city government, private, not-for-profit, 501(c)(3) institutions chartered by the state of Texas, a fraternal organization, a shrine, and other agencies. All of these organizations operate not for profit and all do only three things: patient care, research, and education.

We are very much interested in the topic that you are discussing today for a number of reasons, and we have confronted threats in the past, and I'll be discussing briefly how we have responded in the past and how we plan to respond in the future to some of these threats.

Texas Medical Center is responsible for providing the health care of last resort for indigent persons and for very wealthy persons, and for everybody between. We provide health care, as do the other 126 academic health science health centers, within a broad range of responsibilities, which include trauma services, cancer and cardiovascular services, pediatric services, and just about any kind of medical care services you can imagine.

One great difference in medical care in 1997 and medical care in 1947 is today the people who come for health care to health care institutions are much sicker and can be helped much more. The reason for that is that in the last 50 years of medical research in this country, we have now learned to keep people alive who have five or six diseases that would have killed them in 1947. That's the good news.

But the thing we must keep in mind is that they are very, very dependent on the health care system to sustain life. We have people who cannot miss a single day of medication without having severe adverse reactions. And so the entire medical infrastructure, which now includes home health care and intensive care and everything in between, is a fragile and very useful resource, but something that a lot of people don't think about until they need to use it. We have

experienced in the past some very severe weather-related infrastructure threats. And while a number of the speakers today are going to talk about non-weather-related threats, I'd like to stay on the weather-related threats for just a moment, because in Houston, we're drawing day by day closer to our hurricane season, and that is a time for all of us to pay serious attention to one of nature's most dramatic assaults.

We have had, in the past, a number of near-misses, but we've had one hurricane that came straight through the Texas Medical Center with winds of 105 miles an hour. We survived that, but we learned a lot from it. One of the things we learned from it was that the more notice we could get and the more preparatory time we could have, the better. And so we are now embarked on a major program to provide us with additional time to know more about flooding, and to know more about the behavior of winds connected with hurricanes and with other severe weather disturbances.

For those of you who are not from the Gulf Coast, the Gulf Coast weather is different than the continental weather. We have rainfall that comes with different-sized drops and different kinds of intensities. The highest intensity rainfall in history in the United States was at Alvin, Texas, where 42 inches fell in 24 hours. Those kinds of numbers simply do not happen anywhere other than on the Gulf Coast.

But we have had on a fairly frequent basis in Houston numbers of ten, twelve, and fifteen inches, and those kinds of rainfall amounts, in a flat terrain, result in very serious flooding. However, we've been fortunate to date in that in all of our flooding scenarios, they have never been combined with a storm surge. We have never had a ten- or twelve-foot storm surge in the gulf where the bayous would refuse to take water. In such a scenario, in the Texas Medical Center, we would have depths of water greater than three feet for periods greater than three or four days.

Now, all of our electric interconnects are underground, and we are the largest non-industrial user of electricity in the United States. We are also the largest customer of Southwestern Bell and the largest non-travel and entertainment customer of AT&T. So you have with all of our utilities buried, and with not being able to do submarine kind of construction, you have the possibilities of taking down the major part of our electrical and communication infrastructure for a long period of time. This becomes extraordinarily difficult because of the severity of illness of the people who are in the hospitals, but it also becomes a great endangerment to the research projects

that are going on, and to the other important worldwide activities that come from the Texas Medical Center.

Today, in telemedicine, we treat people all over the world in real-time. And if we go down, projects of care go down all over the world as part of that system.

Our response has been to work on a new system that has become possible through the development of NEXRAD radar system. Because of the NEXRAD radar system, it has become possible to direct rainfall into each of our water sheds, each of our systems, Braes Bayou or Sims Bayou or whatever and then to predict how long it will take for that water to reach the Texas medical system. In our case it has to be Braes Bayou. Working with Phil Beatty there and with the University of Oklahoma, Dr. Vu up there, and they have at the University of Oklahoma developed this system for continental storms that we're adopting into the—into the gulf coast storms. We expect to be able to get up to three hours of extra notice about flooding in the Texas Medical Center.

To give you some sense of scale, less than three weeks ago we had a storm in Houston which averaged only three and a half inches. The Braes Bayou rose 24 feet in less than two and a half hours at the Texas Medical Center and was within one foot of flooding the Texas Medical Center. Three and a half inches of average rain is a trivial event in Houston, so it has gotten our attention and has us very concerned. Interestingly enough in a later event, ten days later, there was a three-foot-high tide in the gulf which, fortunately, didn't coordinate with the rainfall. Had it coordinated, we again would have had flooding. What has happened to make this so severe is that we have had substantial subsidence and we've also had substantial developments in the upstream of each of these water sheds in Houston.

So while we are anxious to have the advanced warning, we are also anxious to do something about getting upstream of these kinds of problems, and we expect to try to come up with ideas to make us safer from these eventualities than we are now, such things as improved drainage and other kinds of detention and diversions and other sorts of plans.

I want to briefly mention to you the astonishingly good cooperation we have here in Houston among our agencies. City government, county government, Metro, the federal agencies all work very closely with the weather bureau, Secret Service, everybody that we work with has an astonishing kind of collaboration with different things, and one of the best examples of that is our new TranStar center, which is on the Web, updated regularly, and tells us what roads are open in

Houston and what the speed is on those roads so people can tell whether the Medical Center can be reached and how to get there, and now we're adding this flooding information to that page, and we're working with the city with Texstar and Metro to make information available in this way to the public.

Again, I thank you for coming. I think your work is extraordinarily important, and if we can do anything to be of assistance, please let us know. Thank you.

JANET ABRAMS: Thank you, Dr. Winerdi. Our next person will be Mr. Jimmy Schindewolf of the City of Houston.

MR. SCHINDEWOLFF: Thank you Mr. Chairman and members of the commission. Welcome to Houston. Thank you for the opportunity to appear before you. I think Mayor Lanier pretty well highlighted what the city of Houston is doing as it relates to infrastructure and what he's doing as chairman of the Rebuild America coalition. And I can't emphasize how important the Mayor's comments are regarding proper funding for continued maintenance and upkeep of our infrastructures. I know that's not what—the point of your thrust here has to do with protection of the infrastructure, but in my mind, that's part of the key as far as our infrastructure, is properly funding both at a federal, state, and local level to keep our infrastructure up to a proper operating level. I'm here primarily to talk about water. That's one of the items that you have listed as a critical infrastructure. Needless to say, most of—and I'm up here probably with mixed emotions about whether I should be here or not, because needless to say, when you start talking about the vulnerability of our water systems to terrorism, then we start talking about this publicly, and then obviously that brings to the surface what are our vulnerabilities. So I know as a professional involved in that aspect of it, we talk a lot about it privately. We do a number of things, but when you start talking about it publicly, it raises some real issues.

You know, everyone has seen the movie, the sabotage at the electrical power plant, what happens when the power plant is sabotaged. Thank goodness we haven't seen that movie about what happens when a water connect has been sabotaged, and hopefully we never will see that. I think that's one of the things we need to talk about just to give you a little bit of an idea.

As indicated, I'm the director of public works and engineering here in the city of Houston, so water, wastewater, streets, drainage all fall within the purview of that department.

Water, as I mentioned here, is probably the key issue as far as vulnerability is concerned and a life line to our citizens. Just to give you an idea, our city encompasses about 600 square miles.

A very large city, about 5,500 miles of water lines. Think about that: 5,500 miles of water lines. About two-thirds of our water comes from surface treatment. About one-third from water wells. So when we start talking about surface water, we start talking about getting our water from lakes, in the case of Lake Livingston is about a hundred miles from the city of Houston. Lake Conroe is about 60 miles from the city of Houston. So we have lakes way out there, and we have conveyance systems, open canals that come from those lakes to our water treatment plans. We have two major water treatment plans. And when I talk about major, we're talking about huge facilities. So when we start talking about how vulnerable are our water systems, you start talking about the size of our water system, the security that we currently have in place, and the fact that it's impossible to properly secure all of that system.

So I will tell you that we think about it a lot, we talk about it a lot, we do the things that we think are important as far as securing our major facilities, our major water distribution facilities. Obviously we spend a considerable amount of money on those security systems, but as you all well know, it's impossible to totally safeguard our water system. So I will tell you on one hand I share with you my concerns. On the other hand, I don't know what that answer is.

But I will mention the city of Milwaukee. Most of you are familiar—or if you're not, you should be—with the case where Milwaukee in 1993 had the introduction of cryptosporidium, which is a protozoa. 400,000 people ended up being affected over that particular situation. Over a hundred people died. So that was something made by nature. That was something the city of Milwaukee was not treating for at that time. Obviously they are now.

We do in fact have a superior water system here in Houston. We've worked very diligently to maintain that superior water system, but when you start talking about water systems and all the possibilities, I will tell you there is room for improvement. As I say, I don't know what the answer is as far as making our systems totally fail-safe, but I will tell you, it's of serious concern. That pretty well ends my conversation. It's not meant to be scary, and as I say we hesitate to even talk about these things publicly, but you've asked us to talk about them; here I am. Thank you very much.

JANET ABRAMS: Thank you very much. Our next speaker will be Judge Robert Eckels, County Judge of Harris County.

JUDGE ECKELS: Mayor and commissioners, I appreciate the opportunity to come here. I apologize because I received the invitation only yesterday, as I had been out of town, trying to

work with the Mayor and city folks on getting some legislation passed in Austin in our mutual interests.

And I do appreciate your coming here today and worrying about the critical infrastructure needs of the nation and of this community. Mayor Lanier, who is graciously hosting the meeting here today, has led the fight for the city in a reemphasis on the infrastructure needs, and I would say the critical infrastructure needs for our community, particularly against the more insidious enemies of neglect and the failure to maintain that as it has in the past. And the city has had a great new emphasis on the roads and bridges and neighborhoods to standards, water systems. I'm sure you heard that in his earlier testimony.

We at the county are working towards those same ends from our side. We have completed major infrastructure projects and look forward to continuing to work with the city. And again, I don't want to get into all of that today. I know you have a lot of testimony. But it does seem as I was reviewing the committee's works in Atlanta and Los Angeles and the testimony that was focusing largely on the technological infrastructure of the country, that those traditional infrastructures of roads and bridges and flood control projects the county does are more and more related to the technological infrastructure of the country as well. That when the intelligent transportation system goes down, our road system does not function as it should, and we have to be determined about how all of these issues work together.

At the same time this commission bears a tough task in balancing the kinds of things that our government does in the county more so than any others, in the open governments and the public records. Traditionally these records have all been available, but they've been difficult to get and everyone could have access, but it wasn't as big of an issue, and now you're balancing privacy concerns and the public's right to know. Open government which traditionally has been more honest government with some of the civil liberties issues and the stories of people who are suddenly finding their property records and all of their personal lives open to the Internet and to access to the entire country.

It's a difficult decision, difficult questions. I commend you for them, and I will have our county departments, in lieu of the large number of people here today, submit to you some written testimony, particularly our ITC office, our information office is putting together information on how we are addressing those needs. Our emergency management office works closely with the city, the state, Metro, at the TranStar center, and you'll be taking a tour of that, I understand. So

my main purpose here is to welcome you. Thank you for your efforts and your addressing these issues. We do that every day through our emergency management office and the planning and mitigation, and I commend you for your work here today. Thank you, and thank you, Mayor, for opening the chambers.

JANET ABRAMS: Thank you very much, Judge Eckels. Our next presenter will be Mr. Eddie Corral with the Houston Fire Department. Thank you.

CHIEF CORRAL: Mayor, commissioners, thank you very much for this opportunity. Kind of like the Judge, I got this letter kind of late, but I couldn't pass this opportunity as I was invited to talk to you and express some of the concerns that we have in the fire service. We appreciate emergency services being listed as one of the critical infrastructures that needs to be examined for the sake of the nation's security. I agree with that, as we worry about physical threats and cyber threats. It's hard for us to think of someone who needs to be protected. And our mind-set has always been we're the protectors. So I'm here to listen and offer our full cooperation and answer any questions that you may have that relates to the Houston Fire Department.

In addition to being the first responder at events, it seems we offer the EMS service for the city, hazardous materials, arson investigation, code enforcement, rescue services, and we provide these both for our three airports and for the Port of Houston. Although I don't understand the objectives of this commission completely, it sounds to me like it's a very worthwhile project that we're doing here, and for us it's very hard to think about infrastructure as such where water and banking and all—and all these other things come in. I think it's a super idea.

And I guess our first great concern is as first responders, thinking again of infrastructure sounds more global. Yet, you know, we can see the importance of talking about other things into consideration. And as first responders, we need to think—you know, we tend to think of the big explosions, you know, the wall collapses, the spills of many kinds. But since Oklahoma City, I think all the fire services across the United States have come to realize that things can get even bigger than what we're used to. And it brings a question to us all: How ready are we to undertake some of these events that look like they are on the horizon at this particular point?

So the concerns that we would have at this time and that we would ask of the commission is, as you go throughout and learn what some of the problems are, and if you could share those things with us pretty quickly, that would be a great thing for us. Things are always changing and you have to learn. I know that the federal government has more information than we have on a

lot of things, and they have training, they have equipment and things that we would possibly need. And if there was some structured way that we could be made aware of what the federal government knows. Here in the city we've already made some efforts to coordinate the services that would be involved in a major, major disaster, and we did have the fire chief from Oklahoma City come down and tell us about lessons learned, and that episode, and it was very, very helpful and brought to our mind the fact that the need for quick information and for equipment that might be needed. And that's kind of what I would ask of this commission, as you learn how quickly we can get information and training programs and things that we would need. Because whether the event is going to be small or large, we're still going to be the first responders. We're still going to be the first there to try to help folks, and that's very vital to us.

The other thing is that, in our communications, which is so important. Without having that working, we're very crippled, so that any help that the federal government could give us in securing frequency that we might need for that endeavor. And also, secondary systems should that primary system be knocked out. So that's kind of what I would ask of this commission, and thank you very much for inviting me. If you need additional information, we'd be glad to put some things in writing for you.

JOHN POWERS: Chief, specifically we would like for you to identify what your greatest needs are as first responders, particularly your training needs and your equipment needs. If you can provide that to us separately.

CHIEF CORRAL: Yes, we'd be happy to do that.

JOHN POWERS: Thank you very much.

CHIEF CORRAL: I happen to be on the national board for the operation to respond. I don't know if you're familiar with that, but it's a software program where a person out on the scene of a spill or a hazardous chemicals can press a few buttons and get all the information from the shipper as to what's in that. And that's some of the things that I think the technology will provide with us. And we will get that for you.

JOHN POWERS: Thank you.

BRENTON GREENE: And, Chief, one point and I guess a question with it. Concerning your emergency services, I know there are cases down in Florida a few months ago where 911 systems were broken into by a malicious hacker leading to nonavailability of systems. And I would ask

the question and point to the issue of information security and the prevention of potential intrusion into the coordination of those emergency services.

CHIEF CORRAL: Yes. You know, that's precisely what I was talking about. If you have information on how we protect that, if you would share it with us, we would certainly look at it. We'll look at it from our side also. Thank you.

NANCY WONG: I was struck by a comment—I was particularly struck and interested in your comment and request about securing frequencies to respond to emergency services?

CHIEF CORRAL: Yes. The frequencies that are needed. You know, the FCC controls which we can use and which numbers we have. And we could put that in the request also and be a little more specific about the frequencies that we need and we need the government to okay those for us.

NANCY WONG: We would appreciate that information. Thank you.

CHIEF CORRAL: Thank you.

JANET ABRAMS: Thank you very much. Our next presenter will be Mr. Sam Goodhope, representing the Office of the Attorney General, State of Texas.

MR. GOODHOPE: Thank you. My name is Sam Goodhope. I'm here on behalf of Attorney General Dan Morales. We have been working for the last five years or so on a very—what might be a very small part of the overall issues that you're looking at. We're looking at border trucking issues. I would like to read Dan Morales's statement. The North American Free Trade Agreement presents the state of Texas and the United States with an historic opportunity for expanded trade and economic growth. Because the river of North American trade flows through Texas, Texas is pivotal in ensuring that the promises of NAFTA are realized. The attorney general remains absolutely in favor of free trade between Mexico and the United States.

However, in our rush to achieve such free trade, we must not engage in a race to regulatory laxity that will needlessly place our citizens in danger. Concern for the health and safety of our citizens must remain paramount.

The term "expanded trade" is an abstract term that does not fully convey the critical issues of physically moving billions of dollars' worth of goods across the 1200-mile international border between Texas and Mexico. The reality imbedded in that term is millions of trucks each year bottlenecked through seventeen United States Customs Service Ports of Entry along the Rio Grande. These millions of trucks carry or will carry hundreds of billions of dollars' worth of

produce, televisions, stereos, computers, and other consumer, wholesale, and industrial goods. However, they also carry corrosives, chemicals, explosives, jet fuel, poisons, toxic substances, and waste, pesticides, and illegal drugs.

Thus the reality of expanded trade becomes a very real, tangible presence of foreign trucks that have been subjected to lower scrutiny and, quite frankly, lower safety standards near the homes, streets, highways, and communities of nearly twenty million Texans. It is projected by the year 2000, the U.S./Mexico border could see transborder truck traffic increase to eight to twelve million trucks per year. We cannot sacrifice the health and safety of our Texas citizens. The multibillion-dollar investment that we have in our roads or our responsibility to control hazardous materials and illegal drugs at the altar of free trade.

On December 18th, 1995, the Clinton administration imposed a moratorium which stopped the processing of registration of foreign trucks. If and when the moratorium is lifted, the projected massive increase in transborder trucking transportation, coupled with the new ability of Mexican trucks to travel throughout Texas, raises or increases three significant risks.

First, as I've mentioned, the health and safety of our citizens will be endangered by overweight, unsafe, unregistered, uninsured Mexican trucks driven by Mexican nationals who may not meet certain requirements that all of our truck drivers now have to meet in the United States.

Secondly, Texas roadway infrastructure will be accessibly consumed by increased truck traffic, as well as by greater numbers of overweight trucks from Mexico. Third, due to the projected massive increase in transborder transportation, state enforcement efforts to control and check the importation of harmful products—such as hazardous materials and substances, adulterated food, strawberries, perhaps, medical waste, and perhaps most importantly, illegal drugs—will be hampered, if not made ineffectual.

With respect to issue one, as I've stated, Mexican trucks will pose an escalated threat to the health and safety of Texas citizens once a moratorium is lifted, especially when they pass through major cities such as Houston, in most of our congested highways. I invite you to go to San Antonio and take a look at I-35. It is incumbent upon public officials to fulfill the responsibility for worst-case scenarios. Just one significant accident between Dallas and Houston between an unregistered, unsafe, uninspected Mexican truck and a Texas school bus and a car containing a family could escalate a tragedy into an international incident. It could increase hostility toward Mexican nationals, increase hostility towards trade with Mexico in general and NAFTA specifi-

cally. We believe also that it would cause a lot of unhappiness on the part of citizens trying to find out who was accountable for allowing it to happen. Mexican truck compliance with state and federal laws is problematic at best. State and federal enforcement officials must be able to—without interference from federal, foreign relations, or officials with foreign trade relation or trade responsibilities—we must be able to enforce our country’s health and safety laws.

In order to do this, we need more resources so we can have more officers in the border area, more stations, co-located stations between state and federal officials to check trucks coming in, to check registration, to check insurance, to check for hazardous materials documentation. With respect to issue two: overweight Mexican trucks must be prevented from damaging or destroying our highways in which Texas taxpayers have invested billions of dollars. Over the past decade, Texas has invested about 30 billion dollars in our infrastructure. Overweight, large trucks from Mexico could wear out this system designed to last for 40 years in twelve years. At a minimum of \$350,000 a mile for repairs, overweight trucks are an expensive proposition for taxpayers of this state. We simply cannot allow large, heavy Mexican trucks to excessively consume our multibillion-dollar investment.

The Texas Department of Transportation has testified earlier that we would need twelve billion dollars for road rehabilitation, maintenance repair, and construction. That’s what we already need in the border area. By the way the statement has been provided to you all.

With respect to issue three: The growing trucking trade with Mexico must not be allowed to increase the importation of illegal drugs, hazardous or dangerous materials, or foods tainted with illegal pesticides.

We have essentially a flood of drugs coming across now in trucks across the border, through Laredo. We need help. And in order to inspect more trucks, we need more cooperation between federal agencies and state agencies that would allow us to place some of our DPS offers. I’ve got one minute, and I will be very quick here.

Hazardous materials are another issue. Documentation is lacking, if it’s there at all. We’ve got plenty of examples of trucks carrying materials that, you know, we don’t know what it is. If it’s a spill, we don’t know what the white powder is, we don’t know what the appropriate response is going to be. Again, we need to have enforcement at the border. Again there are some recommendations in the comments.

I would end by saying that the attorney general believes that it's time to look at whether or not our present infrastructure for preparing these trucks is enough. The attorney general believes that not only do we need one NAFTA superhighway, we do need two, and that includes I-35 as well as Highway 59, in order to carry these trucks, and we also need to start looking at whether or not it makes sense to divide up commercial traffic from noncommercial traffic, maybe put the trucks on their own freeway. Anyway, thank you for allowing me to speak on behalf of the attorney general. I appreciate it. If there are any questions, we would be happy to answer them. I have left off a number of studies outside that we have used in the past, and if there are any questions, I'd be happy to respond.

PAUL RODGERS: Why are these Mexican trucks being permitted to cross the border without any kind of regulation? What's the justification or rationale for that?

MR. GOODHOPE: It's not so much that there is no regulation. It's that right now we are not enforcing the laws. And when I say "we," I will say both state and federal officials. There is a problem in inspecting enough trucks to dampen the flow of non-complying trucks. I mean every time that we try to enforce our laws, there are complaints that we're getting in the way of free trade, that we don't understand what NAFTA is about, and issues like that. They ask us if we don't know that we are getting into international problems or issues. So it's really more a matter of enforcement on the border. And U.S. Customs has done—they have done the best job I believe that they can. They don't have the resources. If you all have time, if you went down to Laredo and saw a seven-mile-long line of trucks, I think you would see what the problem is. And it's going to get worse. And so even right now where we only have a two percent inspection ratio, that still causes a backlog. If we were to go to ten percent inspection, there would be no trucks getting through Laredo and trade would stop. We need more resources for inspection; we need to co-locate state and federal officials. Thank you.

JANET ABRAMS: Thank you very much. Our next speaker will be Mr. Mike Green, President of the Transmission Division of TU Electric.

MR. GREEN: Chairman Powers, commissioners, thank you for the opportunity to provide input to this very important discussion today. I will begin by briefly describing TU Electric and then will comment on five areas of our operations.

TU Electric is an investor-owned electric utility and the principal subsidiary of Texas Utilities Company. TU Electric provides electric service to about 5.9 million people or about one-third of

the population of Texas. TU Electric service area covers more than 53,000 square miles, stretching 600 miles from west Texas to near Louisiana, and from the Oklahoma border south about 250 miles into central Texas. Electric service is provided in 372 cities and 91 counties. Dallas is company headquarters and the largest company served. TU Electric operates generating units at 24 power plant locations, including nineteen fueled by natural gas, four by lignite coal, and one with nuclear energy. Total generating capacity exceeds 22,000 megawatts. TU Electric's transmission system includes about 13,000 circuit miles of transmission lines. As far as economic impact, TU Electric's plant is valued at \$15.8 billion. Its operating revenues in '96 were six billion. Total electric energy sales were 94.6 million megawatt-hours for the year. Texas Utilities has over 11,000 employees throughout its operation. The company's information technology area uses both public and private networking to provide voice and data transmission through the areas serviced. This includes microwave, 900 megahertz radio, and fiber optics as well as third-party, local exchange, and interstate exchange carrier services. These services provide connectivity between users and distributive and mainframe information platforms. The network is also used for command-and-control processes such as transmission grid and local power distribution operations. In addition to the corporate information systems and database, various functional systems exist as operational and management systems. Examples include extensive customer information system, a storage and inventory system, a distribution information system, and an energy management system. Distribution information and energy management systems provide real-time tools for operational security of the bulk power and local distribution systems.

The greatest threats and vulnerabilities to the information technology area, in order of probability are, human error, computer viruses, disgruntled employees, computer and telecommunications hackers, natural disasters, and civil unrest. Critical applications, programs and data are backed up daily and are stored at a secured off-site location. All access to the information network is protected by security passwords and any outside network interface is protected by an electronic firewall. In addition, antivirus software resides on every desktop computer system for protection against any virus transmittal attempt.

Both internal and external audit groups, as well as the company physical data and security groups, have performed extensive reviews and provided reports to company management on the steps needed to strengthen system readiness. Transmission grid security and reliability are

managed in accordance with the North American Electric Reliability Council policies and requirements for planning and operating the electric grid. These are further emphasized in the Electric Reliability Council of Texas policies and guidelines.

TU Electric maintains emergency planning and operating procedures, incorporating both Merck and ERCOT requirements for transmission, generation, and distribution. Reliability and security protocols are based on maintaining operating reserves to withstand the worst case contingencies. No loss of a single power plant or major transmission line would jeopardize system integrity. Should widespread loss of the transmission grid occur, black star capabilities are maintained in numerous strategic points and black star plans are exercised periodically.

In coordination with ERCOT, TU Electric has developed an emergency electric curtailment plan that is reviewed, updated, and exercised annually for training. This plan identifies the procedures, actions, and specific personnel and functions to address periods of adverse weather, extreme electric loads, or shortages in ERCOT generating capacity. All generating facilities have site plans for medical emergencies, oil spill containment, and cleanup procedures and site support in the event of fire. Site security for gas and lignite fuel generating facilities includes a combination of perimeter fences, gate guards, and surveillance cameras monitored by control room personnel.

TU Electric's nuclear plant is operated in accordance with Nuclear Regulatory Commission regulations which dictate explicit requirements to detect against natural and man-made threats. These threats include earthquake floods, high wind, tornado, aircraft crash, train derailment, explosion, missile impact, equipment failure, operator error, and security threat. The Comanche Peak Emergency Plant provides specific procedural direction designed to assess and mitigate physical threats to the facility. The Comanche Peak Security Plan provides specific procedural direction to assess and mitigate security threats to the facility. Both of these plans are required by federal regulations and reviewed, approved, and overseen by the NRC.

System-wide emergency planning and operating procedures including provisions for activating management and support teams which may also include activating support agreements with other utilities or contractors and suppliers. Ground and aerial surveillance of transmission distribution may also be developed to help quickly assess the extent of damages typically caused by storms or ice.

TU Electric occasionally finds it necessary to relocate company personnel or to call upon local authorities such as fire departments and area and state law enforcement personnel during periods of unusual weather and during natural disasters such as range fires to help provide support and access control for crews and contract personnel. With warnings from local governments, TU has increased security personnel at generating facilities and other critical company facilities.

The Comanche Peak Nuclear Plant's security is stipulated by the security plan and plant procedures. These include guidance to plant personnel regarding heightened levels of securities. Employees who work at Comanche Peak undergo extensive background examinations before employment. This program is prescribed in a security plan and meets federal regulations. The Federal Bureau of Investigation and the Department of Energy assessed potential physical threats to key facilities and provides so-called threat advisories to NERC which in turn notifies our organization through ERCOT. Additionally, a secondary notification system is active through the local FBI offices in Dallas. Both the primary and secondary notification systems have been tested and proved effective.

The industry has a procedure for notification of appropriate federal law enforcement agency and other industry organizations through NERC. The public sector, local, state, and federal currently provides and should continue to provide crisis assistance when needed. Local governments provide fire fighting services, access control, and security augmentation during periods of abnormality. The cooperation with these local agencies has been superb, and we appreciate that very much.

This concludes my comments to the commission. We appreciate the opportunity to make these comments during this very important work. Thank you very much.

PAUL RODGERS: Are the reliability standards for ERCOT, are those being made mandatory by NERC seeking to safeguard its members?

MR. GREEN: Yes, sir, both NERC, which is the parent organization of ERCOT, the electric reliability council are going through the process of revising our policies and procedures in making them mandatory to all participants in the electric system operation.

PAUL RODGERS: And you think that will be successful?

MR. GREEN: Yes, sir, I do. I think, number one, it has to be sufficiently reliable if the electric industry moves into a more competitive environment. Reliability has always been, I think,

the main concern of all of us in the business for quite some time, and to continue that success, we're going to have to have mandatory participation by all participants.

PAUL RODGERS: If some company doesn't do that, could there be some kind of federal backup authority to force compliance or to resolve disputes, or not?

MR. GREEN: I think that is an issue currently in front of the NERC. I think that's a process that we need to go through to find out the most efficient way to handle the requirements to adhere to these policies. I don't think we have an answer for it right now, but it's obviously critical.

PAUL RODGERS: Thank you.

MR. GREEN: Yes, sir?

DAVE JONES: Yes. You talked about security passwords, electronic fire walls, and antivirus mechanisms to protect your computer system. Do you have any type of assessment program within your organization to see how well that's been implemented?

MR. GREEN: Yes, I think I mentioned that we continually monitor ourselves, both internally and externally. We have contractors who will come in and make sure that we essentially are doing or accomplishing what we're attempting to do, and that is to protect this critical data that's so important to us.

DAVE JONES: That also extends into the operational area, other than the business information area?

Mr. GREEN: Yes, sir.

DAVE JONES: Thank you.

JANET ABRAMS: Thank you very much, Mr. Green.

MR. GREEN: Thank you.

JANET ABRAMS: Our next speaker will be Dr. Kenneth Mattox representing Baylor College of Medicine.

DR. MATTOX: Dr. Powers, ladies and gentlemen, I am Dr. Kenneth Mattox a trauma surgeon at Baylor College of Medicine and chief of the medical staff at the Ben Taub Medical Hospital, a local county hospital. I'm a member of numerous national organizations, and I'm involved in emergency health services. My academic interests have focused on emergency health issues for the last 35 years, and much of my research has been in that area. I am one of those classified by Dr. Winerdi who has cared for the sickest of the sick. And our hospital, during Desert Storm, received more casualties, more injuries on any given day than occurred in the

entire coalition forces in the Middle East. Thank you for including emergency medical conditions in the listing of the nation's critical infrastructure.

Houston has had a long history in addressing the issues of the local solutions to complex emergency problems. The first trauma center was established by Dr. DeBakey in 1949. The second was in Chicago in 1960. EMS was developed in the late 1960s and early 1970s. The Harris County Medical Society has a very sophisticated program in prevention both for general health problems and in emergency conditions as well. The innumerable physiologic, environmental, chemical, biologic, terrorist, and social factors which create conditions which require highly specialized and critical emergency medical service personnel and facilities have already been listed for you. I will not reiterate those here.

It is our job that when all of the impacts of all of the previous speakers bring us patients, it's our job to patch them up, to take care of the infection, to get out the poisons, whatever they are, return that person as a functioning member of society, both to be a voter and a taxpayer.

Access to quality emergency medical personnel and facilities is an important and element of the nation's critical infrastructure. This must be both mature and integrated.

Nationwide, numerous barriers and restrictions to access for critical emergency medical services currently exist. There are confusions in definitions, both in facilities and in personnel. There is a dilution of physician expertise for a whole variety of reasons. There are changes in medical education. There is lack of support for critical research in emergency medical conditions. And there are increasing reductions on performing this research, partly because of confusion in several federal agencies related to permission for biomedical research under emergency conditions. There are inconsistent and sometimes restrictive payment schemes, and the regulatory industrial complex creates innumerable problems. And lastly, trauma centers across the United States, particularly in California and Los Angeles, are closing. Many of the trauma centers, including several of those—at least one or two in this city, are currently in jeopardy.

Continuing graduate medical education in biomedical research components is essential for current and future delivery of critical emergency medical services, especially in the areas of trauma, burns, critical care, infectious disease, chemicals, and the like. Consistent Medicare GME pass-throughs are threatening the development of critical specialists that are required for this condition. My point for this paragraph is, a pipeline of personnel, techniques, medications, and devices for the future are required.

Ironically, in most of our cities, comprehensive critical emergency health services are in the inner-city public hospitals, a very ironic form of perhaps reverse access to quality care. At least half of these safety-net hospitals in America are in jeopardy of closing. Innovative, integrative local solutions are already being developed and are in place which condition access to medical personnel facilities. These can be done extremely cost effectively at a reduction of cost—at a reduction of cost—and can produce high quality, specialized critical emergency medical services.

Through innovative cooperation with the Harris County Medical Society, the community physicians of the city, the academic health science centers, and the public health hospitals, we are already doing such. We are doing, providing comprehensive, total health care, including home health care, emergency services, heart surgery, physician services and the like at \$35 per enrollee per month, compared to \$117 for the nation's Medicaid, and \$333 for Medicare on the average. So at ten percent of the national Medicare rate, we are providing that in this local community. Is it enough? No, of course not. Is it being done? Yes.

My point here is that community cooperation incentives can help provide solutions. Integrations of the emergency care elements into your plan for preservation of all elements of the nation's critical infrastructure is possible and essential. To include elements of both EMS, trauma care, specialized care, most of this at the specialist, not the generalist level.

For emergency health access, like health issues in general, careful analysis of the pros and cons of changes in health care delivery, and preservations of these critical elements of quality patient-physician relationship is so sacred to the health of each of our citizenry, and in our country. Managed health care and critical emergency health services are often in conflict.

Mr. Chairman, ladies and gentlemen, critical health emergency health issue is essential. It is part of the delicate ecosystem that our country is facing. And I look forward to a future opportunity to elaborate on the many components of this critical health infrastructure.

JANET ABRAMS: Thank you, Dr. Mattox. Next presenting will be Mr. Mike Turner, regional president, Southwestern Bell.

MR. TURNER: Good morning. Thank you for including Southwestern Bell in this very important activity. My name is Mike Turner. As you've heard, I'm regional president for Southwestern Bell's Houston area operations. As you may know, Southwestern Bell is a member of SBC Corporation's family of companies. SBC Communications is an international leader in the telecommunications industry with more than 41 million access lines and four million wireless

customers across the United States, as well as investments in the telecom business and in eight foreign countries.

The company completed a merger with the Pacific Telesis Group in April of this year, and Southwestern Bell, Nevada Bell, and Cellular One brands—through their subsidiaries—offer local and long-distance service, wireless page, Internet access, cable TV, and messaging, as well as telecommunications equipment and directory advertising and publishing. The corporation has about 110,000 employees.

Southwestern Bell Telephone, which is a subsidiary of SBC, provides local telephone service to nearly 15 million residential and business customers in Arkansas, Kansas, Missouri, Oklahoma, and Texas. In our market area of Houston and southeast Texas, we have about 2.6 million lines, with a work force of 8,000 Southwestern Bell employees who live and work in the greater Houston area. During 1996 we added more than 140,000 telephone lines in the area, which is more than we had in the whole decade of the 1980s. So growth is here again in Houston, and our employees are vital to helping us secure and maintain that growth.

As Houston continues to grow, so does Southwestern Bell. And the growth is more than just telephone lines as you know. While we're adding lines, we're also adding jobs and planning for the second straight year to invest more than 375 million dollars' worth of capital in the infrastructure of Houston and southeast Texas. And this will boost our service communications network both for service and also for security.

The local network is massive. More than 29 million local telephone calls are switched over our network each day. The network features 2500 miles of fiber optic cables, new switching systems at high speed technology. As you can tell we're proud of our network and the services we offer our customers.

In addition to this very brief company and network overview, and out of respect for the many speakers that are here, I think I'll move on and tell you a little bit about three critically important areas to us. First, let me address our commitment enhancing our sophisticated network and what we have invested more than twelve billion dollars in the last five years for improvement in Arkansas, Kansas, Missouri, Oklahoma, and Texas, is the area I'm most familiar with. It's for these network upgrades that we're able to maintain the strength and reliability of 99.9 percent on our network 24 hours a day. Moreover, we monitor our network remotely 24 hours a day, and we're constantly testing critical infrastructure elements of our network and systems, and

redundancies to ensure the integrity of our communications systems, to be able to swiftly and effectively make changes to the network to offset network demands or faults. All of these things are done to ensure we continue that 99.9 percent reliability that we talked about earlier. Secondly, the networks sometimes find us restoring our networks for creating communications during times of need, and of course here in Houston, we're constantly preparing for and testing our abilities to handle emergency situations. The one we think about most in Houston is hurricanes; we prepare for that.

Southwestern Bell takes emergency preparedness very seriously. Our employees have demonstrated under the worst of conditions they can restore the telephone network in the shortest possible time. Emergency preparedness is a function that is vital to preserving and restoring telecommunications throughout the entire community. Whether it be here in Houston or over in Beaumont or throughout our territory, people depend on communications for everything, including 911 and communicating with hospitals, police, and fire protection. In our world of data transfer, large businesses and Internet users today are also brought to their knees when our local network would fail. We have specific plans in place and employees who are well trained in how to respond to times of natural or man-made disasters. This intense preparation has paid off in our rapid response. Some examples of this is severe flooding in southeast Texas in the fall of 1994. Another example you're familiar with is the tragic bombing in Oklahoma City to which we responded to maintain the network. Emergency operations center in each of our market areas serve as a hub for local teams. Southwestern Bell employees marshal resources to restore telecommunications service very quickly. For example, our southeast Texas Houston team consists of employees of more than twenty work groups, representing all faces of our business. They're worried about everything from backup power splices to diesel and emergency engines, to how we communicate, to what's going on in the team, whether to assess to bring in property and equipment to other Southwestern Bell employees and further restore or enhance communication services. Also we regularly test ourselves through simulated, real-life disasters. This helped us and our team further refine our abilities to work under pressure so that we can respond quickly during disasters. Also, Southwestern Bell always stands ready to assist when communications networks need to be created, such as during the Oklahoma City tragedy, referring to our teams rebuilding land line services in the temporary time or providing wireless service for use during an emergency.

Our emergency restoration team also turns to very sophisticated telephone reading systems to enable us to manage and route calls between our telephone switching centers that we have for our man-made disasters. These calls would normally go through our damage unit and then rerouted tolling through an alternate switching route.

Network traffic, as we call it, is constantly monitored, so we know at all times the status of calls across the situation. We have a service we can redirect calls for that. In addition our electronic switching systems are equipped to automatically designate a central service to police, fire, and hospitals, and Red Cross. It's a high priority; the lines are open ahead of other lines during an emergency. As I mentioned earlier, the Southwestern Bell network is equipped with a ring. It's a secretive network technology ring, especially in the metropolitan area. The network externally has one location; you can get to it another way, duplicated. This ensures redundant routing, giving ourselves a survivable network.

To conclude this morning, let me share with you some software to protect the privacy of data that relates to our customers and employees. For our customers we have a long-standing commitment to customer privacy. No one has access to databases which contain the names and numbers of nonpublic or unlisted numbers except those groups necessary to maintain the customer service. And this includes our employees who are not necessary for that purpose. We also have rededicated ourselves to our commitment about privacy by promising publicly that we will not sell any customers name or numbers to any mailing house regardless of the policy revenues, and Southwestern Bell works diligently to protect customer confidentiality.

On the internal side, Southwestern Bell takes data security very seriously. We have employed several sophisticated technologies to ensure the integrity of our internal information and our data, including we maintain state-of-the-art firewall technologies within the company and the Internet, as well as other critical access points systems. We permit authentication process using a secure IV technology, basically the constantly changing password technology, for external access to its critical internal systems. We have increased systematic surveillance of critical networks both in terms of network surveillance and also in terms of internal corporate management controls, following up on if we do what we say we're doing, bolster our corporate security policies and procedures especially in the areas of UNIX-based systems and Internet access. We're delighted you've chosen Houston as a place to get more input. SBC and Southwestern Bell are pleased to be part of the process, and we wish you well.

DR. BILL HARRIS: As a part of an international institution, have you in any way either benefited from that or been compromised in any way in your ability to achieve the kind of security of data and the security of privacy that you think is essential for your customers in your operations?

MR. TURNER: We clearly have not been compromised by it in any way. And interestingly, and this may change over time, where the countries that we operate, our operations are pretty much stand alone in that country. And I can foresee a time, as I know you can, where you would network these services globally. There's no reason we really don't. The biggest issue for us in telecommunications is standards. If we're operating in Europe or South America or the Far East, the standards issues have been very difficult for us to deal with. We operate in a manner stand alone for that environment.

JANET ABRAMS: Thank you very much Mr. Turner. Before moving on to the next speaker, I'd like to encourage anyone who would like to speak and has not filled out a green card to do so at the sign-in table. Thanks. Now we'll hear from Mr. Robert MacLennan, general manager, Metropolitan Transit Authority, Houston.

MR. MACLENNAN: Members of the commission, Bill, thank you very much for the opportunity to speak to you this morning. My comments will be brief, will focus particularly on physical distribution of transportation and telecommunications.

For reference, as was noted, I'm the general manager of the Transit Authority that serves this region, the Metropolitan Transit Authority of Harris County. We service a 1280-square-mile area. The principal city is Houston. There are fourteen other cities and then the unincorporated areas of Harris County and bits and pieces of some surrounding counties that are in our area. I am also Chairman of the Board of the Intelligent Transportation Society of America, ITS America, and my comments will focus a little bit from both sides.

For background reference, Metro is unique in the transit industry. We do run the largest and we'd like to think one of the most advanced bus-only transit systems in the country. But we're also involved in road and street construction and maintenance. We're involved in traffic management and safety on not only on the transit system, but also on the major thoroughfares and in the major activity centers. We do have a 300-member police department that focuses on that safety and accident and incident control. We'd like to think that the combination of our efforts together with the efforts of the other policing agencies in the area allow them to focus on security and

criminal investigation, with us picking up some of the other activities associated with traffic. Houston itself is also very different from other major cities in its approach to transportation. You also heard comments from earlier speakers alluding to the fact that the Transit Authority, the city, the county, and the highway department worked very closely together. I think one of the major achievements in that close relationship is Houston TranStar, our traffic and emergency management center. I know you'll be visiting that a little later today. We welcome the opportunity to host you over there and look forward to being able to talk to you in some specific detail about the security aspects of traffic control and transportation, particularly as you tour that center.

I also know that in the audience you have the director of that traffic and emergency management center, Doug Weirsig, and I expect that he'll probably be speaking to you a little later this morning. So I won't try to steal any of his thunder.

We know here in Houston that we can't build ourselves out of congestion with concrete and asphalt alone, so as of a while back we've gone back to a significant application of the advanced technology items to do so. Here in town you'll see closed-circuit TV not only on the high occupancy vehicle lanes, but also on the main lanes of the freeways, loop detectors to determine speed and density of traffic, changeable message signs which not only give information to travelers, but also issue direction. Should there be an accident or an incident, actual direction is given to the traveling public on what to do and how to get around that scene. Changeable message signs offer a significant improvement.

Automatic vehicle locators, automatic toll collection, the beginnings of the infrastructure for navigational assistance, and in fact we're even involved in the research for the automated highway of the future in town, for those of you who might take part in looking at that demonstration in August in San Diego, you'll see some Metro buses in that demonstration operating driverless.

The fact is when all of that occurs, there's a great deal of dependency on telecommunications and obviously the security of those telecommunications particularly as vehicles traveling down a roadway without a driver is extremely essential. You've heard some of the comments made by the telecommunications experts earlier today, and I'll not repeat those except to say that we're working very closely with them and are particularly concerned that those security measures and procedures be advanced as much as absolutely practical.

We have one major project here which perhaps is a good illustration of what we're doing. The Transit Authority has the responsibility through its grant agreement with the Federal Transit

Administration to replace many of the traffic signals in town with advanced traffic signals, some 1300 of them. A 124-million-dollar project to upgrade and develop a regional computerized traffic signalization system with the intelligence of the individual signals and with those signals communicating with each other and with preplanned guidance changing not only the signalization in cars, but also in the cross corridors to allow for the flow of traffic, and having evaluated that traffic themselves without human interference. In fact, this is a reality today. We have that system in place. When you're out at TranStar, you'll see some of it functioning.

Again, telecommunications security, the ability for those signals to function without interference by somebody who wants to play games with them is extremely important to the traveling public and physical safety and its end. That system will also have in its totality two levels of pre-emption, a demand level for the emergency vehicles, the vehicles of the police department, those who need to get through on demand. It's a rather sophisticated signalization system, but it's one project, and there are many here in town. We welcome the opportunity to talk about them with you in the future in more detail and also to talk to you about the security measures that we're taking.

You also heard a comment earlier about bandwidth issues for intelligent transportation systems in general, the availability of bandwidth for the many utilizations of that bandwidth for traffic control, for accidents and auto control purposes is extremely important, and we welcome your review of that particular area with the idea in mind that it will take federal involvement to determine what the appropriate application of the available bandwidth will be.

I'll stop my comments right there and thank you very much for the opportunity to speak to you and look forward to speaking to you again in the future. Thank you.

BRENTON GREENE: Just one question: A lot of the automated and intelligent traffic control systems that you're putting into place, how are you looking at security of those systems against intruders or adequate backups, et cetera?

MR. MACLENNAN: The answer to the question is in many ways, and as you go through TranStar this afternoon, you'll get some explanation of the procedures that are put in place to control them. It does relate to the types of security systems that were identified by the Southwestern Bell representative and by the Texas representative that you heard a little earlier, the electric workers representative. Thank you.

JANET ABRAMS: Thank you, Mr. MacLennan. Our next speaker will be Dr. Naomi Ledé of Texas Southern University.

DR. LEDÉ: I want to thank this commission for holding this hearing on critical infrastructure protection.

The mission of the hearing is to examine the infrastructure crucial to the nation's security and to explore the vulnerability relative to physical and cyber threats and make recommendations. And I am pleased to speak on behalf of one infrastructure pertaining to transportation, because transportation efficiency, national productivity, public safety, and national security are all key issues that are inextricably linked to more complex issues and forces that shape transportation infrastructure needs for the nation and the constraints within which such needs must be met, and I want to dwell critically on some issues.

I've already passed out for your consideration a full paper where I am opposing the issues and making recommendations.

The first issue which Mayor Bob Lanier talked about and I want to sort of reemphasize that relates to preservation and maintenance of the transportation infrastructure. In order for us to minimize our vulnerability to both internal and external threats, there is need to maintain the current transportation infrastructure and to expand its capabilities through the deployment of new technologies. If roads and bridges, subways, ports and waterways, ground, air, and other transportation facilities are not properly maintained, we will encounter maximum exposure to threats of national security and the safety of the citizens of this nation.

To respond to that I'm asking that we make infrastructure maintenance and preservation a top priority as we move toward the reauthorization of the next Intermodal Surface Transportation Sufficiency Act, which we now call NEXTEA. The transportation systems must remain high for the services as well as maintaining not only the existing roads, but open access for individuals trapped in our inner cities who must travel throughout not only urban regions, but throughout the nation as well.

My next concern is one that has not been addressed here, and that relates to improving transportation safety and national security with an emphasis on ensuring domestic tranquillity. The concern for transportation safety extends to rural highways, roads and streets and neighborhoods and communities. There's need to review existing policies, standards, and procedures to ensure safety of travel in these neighborhoods. Urban freeways tower over inner city neighbor-

hoods, the central core of our largest cities. The transport of explosives, dangerous weapons and chemicals on our highways and freeways, in the air, on railroads and boats and ships, and even more importantly, the criminal or terrorist acts and threats to ordinary citizens threatens the domestic tranquillity and weakens the moral and social fiber of our society. Our major institutions for socialization—the churches, schools, colleges and universities, various social agencies and organizations—must become concerned about competing allegiances and the lack of social cleavages among our citizens. Social institutions with support from our government must set in motion the series of activities for preserving the ties that bind us together as a nation. The individuals who go on trial for bombings are citizens of this nation. And the very fact that we have them on trial must suggest to us the lack of a cleavage and allegiance to the principles upon which this nation was built.

Now, this falls outside of your hardware infrastructure. It gets more into social-psychological factors that motivate individuals and influence human behavior. I can best sum up this by saying that we have been shaken with these acts and these threats out of our complacency, but there's need for us to reexamine the nation's pulse relative to its philosophy, vision, and extent to which the nation can claim to supreme allegiance from its citizens.

My next point and which—I'm getting to the last—relates to emerging threat of cyber warfare, and some people have already addressed that. But there's a critical need to assess the nation's capability to effectively deal with the threat of information warfare. The information superhighway has been successful as a mechanism to facilitate technology transfer. But it can also be a hazard to our health, safety, and security. There's mounting evidence to suggest that the nation is vulnerable to sabotage in cyberspace. The cyber warfare relates to everything from national security to tampering with banking records. To address that I think the commission needs to look at very critically satellite centers that would effectively deal with misinformation, particularly in our central cities. This misinformation can call riot and destruction to the transportation infrastructure. It can also enhance movement in the case where you have to evacuate, and many of our central cities they do not have access to basic information sources, so in case there is a disaster, we need to be able to tamp that source immediately so that those individuals trapped under these freeways and neighborhoods can be moved.

And the last point I would like to make is more academic but equally as important. Technological literacy and psychological warfare. Communications technologies cannot make a

revolution in itself. The flow of classified information to unfriendly allies can undermine regimes and nations. We must have technological literacy, which is central to national security. Technology not only has promise, but it also has power. It is much more than knowledge of computers and their application. It involves a vision where each citizen has a degree of knowledge about the nature, behavior, power and consequences of technology from a global perspective.

And finally, I want to say all of this must be based on a nation's will. A great nation's will makes a nation's destiny. And I congratulate the commission on its will to act at a time when there are so many currents and cross-currents that can interfere with our national interest. Thank you very much.

DR. BILL HARRIS: Naomi, in our joint work together over the years, we haven't come on this issue of security of information systems, and now since I've been with the commission, I'm much more sensitized to the process. As you look at your educational program at Texas Southern University, do you have enough access to course material and information that you can begin to sensitize your students who are about to be graduates about this problem, or is the information really not packaged in a way that you can have good access to it so that we need to do something special?

DR. LEDÉ: We have access, but never enough. Not enough. I never believe we have enough. As you recall in your work with the transportation center, that we set aside so many funds for technology center. And that's very well in terms of the information flow. Our main concern right now at the university and indeed at the southwest region of the university transportation center which consists of the three largest institutions—Texas A&M, and University of Texas, and Texas Southern—we are all working together on transportation issues.

We have placed a great deal of emphasis on the transfer of technology. My concern right now is technology literacy, where that you not only understand the computers and its application, but the relationship between the various systems, the physical systems in all. This makes for a wholeness that would be central in terms of minimizing our vulnerability and indeed our threats to national security.

JANET ABRAMS: Thank you very much, Dr. Ledé. Our next speaker will be Shelley Leavitt Nadel of the National Association of Corrosion Engineers.

MS. NADEL: Thank you. See if this technology works here. Thank you for having me here today. My name is Shelley Leavitt Nadel. I'm the director of public affairs for NACE

International. We're the National Association of Corrosion Engineers based here in Houston. We're a professional society, 501(c)(3); we have about 50,000 members in 56 countries, represent over twenty different industries including several employees of Ms. Wong's Pacific Oil & Gas Company. So we represent just about almost all the infrastructures that you're concerned with today. And I'm here today to review very briefly the importance of corrosion control to your mission of protecting the infrastructure from physical threats.

I'm going to first summarize how corrosion threatens the infrastructure and in turn our national security and well-being, then I'm going to explain briefly how corrosion control can reduce that threat, and I'm going to conclude with a brief description of how NACE works with government and industry and how we can support the commission. I'm afraid audiovisual aids are not going to help me today, so I did provide an attachment of the overheads for your review so you don't have to write everything down.

First of all, what is corrosion? Simply it's deterioration of a material. And most of us relate to the term "corrosion" in terms of our cars rusting. But most of us don't realize that everything around us is corroding, including a lot of our physical infrastructure.

I couldn't have asked for a better lead-in this morning than Mayor Lanier who spent a great deal of time talking about the importance of maintaining our physical infrastructure. And when we talk about physical threats, corrosion is not on top of your list. I looked at some of your materials, and corrosion isn't one of the hot topics, and I understand that. Yet long before we had an Internet, long before we had electronic communications, corrosion has been a threat to the life line systems of this country. Whether it's electric power, transportation, oil and gas, or water, all of these systems require attention to corrosion control to remain viable. And I'd almost like to call corrosion the invisible terrorist of infrastructure, to relate it to your more common topic of the commission. We don't always know it's there, but even if we don't know it's there, it can still destroy us. Corrosion threatens us on four levels that concern the commission today. Economics, environmental protection, public safety, and national security.

Corrosion costs money. Corrosion costs the United States alone 300 billion dollars every year. That's over four percent of the gross national product in this country. A hundred billion of that is preventable with current technology. So when we hear debates on Capitol Hill about reducing the federal budget deficit, we're always raising our hand and saying there's a big pot of

money out there we could be saving every single year in this country if we just pay attention to the technology we already have, a hundred billion dollars every year.

Besides money, we can save reduced worker downtime, reduced product loss, reduced environmental repair, environmental controls, reduced legal remedies. Corrosion costs government and industry a lot of money. The numbers speak for themselves. Corrosion is an environmental threat. Failure of hazardous materials storage and transportation facilities, storage tanks, pipelines, tank cars, rail cars, all of those corrode, and all of those, if they do corrode, run the risk of releasing toxic chemicals into our environment. Corrosion threatens the environment through waste of natural resources. When a bridge deteriorates, you know, 50 years before it should, we have to manufacture the steel, we have to replace the bridge, make the concrete to replace the structure, and that wastes energy and it wastes natural resources. Finally, corrosion is a very big threat to the water supply. As corrosion engineers we like to think of ourselves as the first environmentalists—I say ourselves—I am not a corrosion engineer; our members are. For example, corrosion control is one of the top causes of pipeline failures in this country. The pipeline industry has a very strong record of preventing leaks, but when they do leak, more often than not it's going to be corrosion that's the cause either indirectly or directly, and that obviously has a direct impact on the transportation systems that you're looking at.

Corrosion is a public safety issue. Pipeline explosions, bridges collapsing, leaking tanks, airplane failures, parking garages collapsing, all those are corrosion related. Your rusty car might be an eyesore, but these things are major public safety issues, and fortunately we do have people that work on these issues, such as NACE members. Corrosion is a national defense issue. Weapons systems, aircraft, ships and cargo tankers, dams, we pay for the repairs, we pay for the weapon systems downtime, we pay for the waste of personnel. And I am encouraged to tell you that all of the branches of the armed services are very active in corrosion control, and NACE works with quite a number of them to help make sure that both the physical structure and the safety of the personnel are protected. So this is not a new issue for the government, but it's certainly a very large one.

Corrosion directly affects four of the critical infrastructure systems you're looking at: electrical power, gas and oil, transportation, and the water supply. Every component of those infrastructure facilities is impacted by corrosion in some way, shape, or form. And I really urge you to keep focused on that when you're talking about protecting the physical infrastructure.

What are some of things we do to control corrosion? I've given a kind of gloom and doom picture about the cost and public safety and environmental issues and the national security issues.

We do have systems in place in this country and around the world that help deal with this issue. We have public and private partnerships. For example, NACE develops technical standards, provides input on legislation regulation. We serve on advisory panels such as commissions like this, help life cycle budgeting for infrastructure. If you plan up front an infrastructure project to deal with the maintenance, deal with corrosion, as one of the maintenance issues, then you're much less likely to spend money down the road. It's your typical classic "pay now or pay later" scenario.

I won't get into the technology of corrosion control. I'm sure you're pleased to hear that. But we do have information on that. There are some major ways to protect corrosion, some of which you're not familiar with, coating—when people paint your car, that's a method of corrosion control. Obviously a bit more complicated, but that's an example.

A little bit about NACE. We're a professional society to provide educational training. We have conferences, technical standards, books and journals, and we also have certification programs so government and industry can have a level of quality assurance so when they're hiring someone, say, to make sure a tank doesn't leak at a military base, they can ask for someone who is certified by NACE and they have a quality assurance level. Finally, NACE works with a number of government agencies right now. Work with Department of Transportation, federal highway, federal aviation, federal railroad, the Coast Guard, Office of Pipeline Safety. We work with the Defense Department, Army Corps of Engineers, Navy, Air Force, and Commerce, the Environmental Protection Agency. We're very active with government to help support government efforts to improve maintenance. Finally, how can we help the commission? We can provide experts to serve on the commission. We can communicate what you're doing via our journals, via our Web site. We love to promote some of the activities you're doing because they directly impact our members. We can provide input on your investment, strategies for protecting structures, and we can help you develop your national policy for protecting infrastructure.

I urge you again to put corrosion control on your list of issues along with all the other issues, and if we can be of any assistance to you, either today or in the future. We're here in Houston, we're on the Web, and we'd love to help in any way we can. Thank you very much for your time.

JANET ABRAMS: Thank you very much. Our next speaker is Laverne Hogan, representing Greater Harris County 911 Emergency Network.

MS. HOGAN: Good morning, Mr. Chairman, commissioners. I appreciate the opportunity to appear before you today. My name is Laverne Hogan. I am executive director for the Greater Harris County 911 Emergency Network. The agency which provides 911 emergency telephone service for citizens in Harris County and Fort Bend County, Texas. I also serve as a commissioner on the Advisory Commission on State Emergency Communications, a state agency which oversees and has rule-making authority to set standards for 911 service administered in the 24 councils of governments across Texas. In addition, the state advisory commission has oversight of the telecommunications network for the Texas poison centers across Texas, the six centers that are networked together to provide poison information for citizens.

With the cut-over of 911 service and the last of the 254 counties in Texas within the year, 100 percent, all 16-plus million Texas citizens will have access to 911 emergency telephone service. The Greater Harris County 911 Emergency Network which serves this area is one of the largest in the nation, providing emergency telephone service to approximately three million citizens. The system, serving citizens in Harris and Fort Bend counties, is fully enhanced. That is, the system provides call-back number and exact location of the caller, as well as the names of the responding agencies responsible for serving that customer, or caller.

The network is currently upgrading its system to enable it to receive call-back number and location information on cellular or wireless 911 calls. This upgrade includes mapping programs to translate X-Y coordinates to physical locations, to determining the location of cellular callers to 911. Government programs such as the U.S. Geodetic Survey and agencies such as the National Highway Traffic Safety Administration could and we think should provide greater interaction and access to digital mapping resources. This sharing of technology and resources could benefit all public agencies which are attempting to upgrade their 911 systems to be capable of receiving location information from wireless companies on 911 calls placed from wireless devices.

Locally, equipment for provision of 911 service is owned and maintained by our network and is located in 50-plus locations in public safety agencies across Harris and Fort Bend counties, including Houston's major airports. The network has been diligent in providing protection and backup for that equipment in order to achieve as close to 100 percent up time as possible for the 911 system serving our citizens. Local telephone companies and wireless companies provide the

telecommunications network required for this essential service. The stability of that telecommunications network and the integrity of the databases required for delivery of caller information to public safety agencies is critical to citizens in need of emergency assistance.

In the majority of 911 systems today, the dominant telephone company utilizes one of its central offices for the routing of all 911 calls to the appropriate public safety agencies. That is currently the case with the Harris County system. Unfortunately, having all records residing at one central office presents a single point of failure. That is, if the central office were to go down from sabotage, equipment failure, or acts of God, three million citizens would be without 911 service until calls could be rerouted to predetermined seven-digit numbers. Today, the nation's 911 infrastructure is predominantly analog. Migrating 911 systems from the analog environment to digital trunking and switching will assist greatly in removing that possibility. Digital systems which can talk to each other can provide the reliability which 911 systems need. The Harris County network is in the process of migrating to a total digital network, taking advantage of its inherent diversity, but 911 entities across the country must depend upon their local telephone companies to provide or upgrade to digital infrastructures. Digital central office equipment is not universally available and is subject to telephone company long-term plans and upgrades.

Construction crews or contractors digging in close proximity to telephone company lines presents a serious area of exposure to 911 systems. One backhoe can bring down an entire 911 system. A few months back, a major cable cut just blocks away from this building disrupted the system here in Houston for 1.8 million people for a short period of time. A simple requirement that these contractors must call before they dig to determine where telephone company lines are located would help to reduce such take-downs of 911 systems. Some states have passed legislation requiring contractors to make these calls, and reports indicate that problems have been reduced significantly. One-call legislation is currently being considered by the Texas legislature. In addition, the migration of 911 to the digital environment, as cited above, would provide greater opportunities for redundancy in the event a cable cut does occur.

The new competitive environment in local telephone service and the proliferation and tremendous growth of wireless presents heavy challenges for agencies providing 911 service. Database integrity is crucial to the proper routing of 911 calls and to providing the vital information about the caller to the call taker in order to better and more quickly respond to the emergency.

Redundancy is obviously critical. Protection of the database from degradation in the new, competitive local telephone service environment will make it more difficult.

With more companies vying for local telephone customers, and those customers potentially moving from company to company, and able very soon to be able to keep their old telephone numbers no matter where they move, database integrity must be ensured. Movement of 911 database management to companies specializing in databases or to a single well established local telephone company has occurred, is underway, or is being considered in many parts of the country, including in Texas today. As the telecommunications environment continues its dramatic changes both in technology and in competitive service, it will be incumbent upon 911 providers to use whatever tools are necessary, whatever agencies or programs are available to ensure the stability and integrity of 911 emergency service for the citizens of all our communities.

Thank you for the opportunity to present these comments.

BRENTON GREENE: Thank you very much. Just one question. I had thought that the call utility kind of thing was required

MS. HOGAN: The what utility?

BRENTON GREENE: The call utility.

MS. HOGAN: No. It's required in some states. Currently in Texas it's not required. It was presented in the last State of the Texas legislature and failed to pass. It has been filed again during this session, and it's moving along, but it has not yet passed the House.

BRENTON GREENE: I think another example that points to that is the Edison New Jersey natural gas pipeline that turned into a major problem just for that same reason.

PAUL RODGERS: I thought that was federal legislation on that subject. That didn't pass, and you do not anticipate it's going to pass?

MS. HOGAN: I'm not aware that it has a chance of passing right now on the federal level. We're hopeful that it will pass in Texas this session.

JANET ABRAMS: Thank you, Miss Hogan. Our next presenter will be Jim Shepard, information technology advisor at Conoco.

MR. SHEPARD: Good morning Commissioners. I'm Jim Shepard. As you've already heard, I am an employee of Conoco Inc. Conoco is an integrated, international petroleum company employing 16,000 people and operating in 30 countries around the world. Headquarterd in Houston,

Conoco is the energy subsidiary of DuPont. Conoco is actively involved in finding, producing, refining, distributing, and marketing oil and gas products world-wide.

Although the industry I'm employed in is one of the eight critical infrastructures the Commission is studying, my remarks today will focus on information technology issues and not issues directly related to oil and gas production, storage, and transportation. This is a natural separation: as Conoco's Information Technology Security Advisor, I share in the responsibility of ensuring the safekeeping of the Company's electronic information resources.

First, I'd like to applaud the Clinton Administration for establishing this Commission. In my opinion, business and society have become incident driven. We react to events after they've happened. For instance, we shut the barn door after the horse has escaped or, to update an old adage, we change our passwords after there is evidence someone has sent a "flaming E-mail" to our boss. This Commission has a unique opportunity, and I believe that opportunity is getting shorter with each passing day, to initiate action that will lead to improved protection of our country's vital infrastructure industries. It's time to get in front of the eight-ball, not behind it.

Computers and electronic information processing are everywhere in Conoco's business. From an electronic credit card transaction authorizing payment at the gas pump to sophisticated super computers that are used to analyze seismic data in the search for new oil, we rely on information technology to run our business. When our information systems are unavailable, business slows. If an outage were substantial or sustained, the ramifications would be significant.

Fortunately this has not happened to us yet. I'd like to think we've prevented problems because we've taken precautions: We have established an electronic information security organization that oversees information security policy and procedures. We have deployed technology solutions intended to keep unauthorized users out of our private network (demo SecurID Card). We have an elaborate, world-wide private network that employs diverse routing and redundant circuitry to minimize the impact of network outages. We have implemented firewalls to ensure our network is safe from the dangers lurking on the Internet and the networks of our business partners that interconnect to ours. We have implemented computer virus prevention strategies, placing virus prevention software on 50,000 desktops within the DuPont Company. We have developed, and test on a regular basis, disaster recovery plans to ensure continuity of information processing services in the event of a sustained outage. And, we train users on the importance of safeguarding the Company's information assets.

All of this and much more is done to prevent a significant incident from paralyzing the Company's ability to manage and process information. Still, we are vulnerable. We are reliant on a host of service providers to make our information systems function. We buy telecommunications and data networking services from major and local exchange carriers. We buy power from electrical utilities. The banking and finance industry provides us with a variety of financial services. In short, we rely on all 8 critical infrastructure industries to operate as a viable business. If these entities are down, the domino affect will take over and Conoco's business will suffer as well. Thus, we to can see the importance and significance of the mission confronting this Commission.

At this point, I'd like to re-direct my comments to focus on three specific topics of interest. I hope the Commission will address these subjects in their recommendations.

First up is training. Until recently my office was co-located with the personnel who manage and operate a regional computer help center for Conoco and DuPont operations in the Gulf Coast and southwest region. This center logs over 250 calls per day from users of the Company's information systems. Most callers are seeking help and assistance with computing and networking problems. The help desk call records can provide great insight into problems of information technology. Analyzing some of this call data, with respect to information security issues, suggests users of information systems need more training, in particular refresher training. User work habits are often the difference between success and failure of information security controls. IT personnel can implement technology solutions all day long and make systems as secure as they possibly can be. However, the uninformed user who simply gives his/her logon account code and password to a Social Engineer can undo all the technology solutions designed to keep the unwanted out.

My second issue deals with encryption. Encryption technology is still evolving, but it is apparent encryption solutions will play a key role in protecting the confidentiality and integrity of electronic information. Encryption can be applied in a variety of ways—at the file level, at the media level, at the network interface point, and via a number of commercial “off-the-shelf” products from a great number of vendors. Choices and solutions abound—truly a buyers market—except that American businesses cannot export strong encryption solutions without approval from the U.S. Government. Therein lies the rub. The choices and “immaturity” of commercial encryption products make it rather difficult to select the ideal business solution and

obtain government export approval in time to meet business need. I am appreciative of the Administration's recent efforts to relax encryption export controls, but these changes fall short of giving businesses the flexibility we are accustomed to when operating domestically. This Commission could play a pivotal role in achieving the right balance between the public and private sectors needs regarding encryption technology.

My last topic is spending. It is my belief that spending on information security has not increased at a rate commensurate with the growth in risk. I believe this to be true in my company and in industry as well. We've not seen dramatic problems because America is a trusting society. However, now is the time to correct this deficiency and I think the Commission can help. The fact that this Commission exists illustrates that there is reason to be concerned. By engaging senior business management in your fact finding efforts, you are planting seeds that might be more readily harvested in the near future. As the Commission looks into regulatory practices, taxation policies and the like, there may be opportunities to provide regulatory and financial incentives that encourage higher spending levels in order to "shore up defenses."

This concludes my comments. Thank you for allowing me to speak today.

PROF. MARY CULNAN: Could I ask you one quick question, please?

MR. SHEPARD: Sure.

PROF. MARY CULNAN: Could you define what a sustained outage would be for your company that would effectively bring it to its knees? How long would that be, if your company were to go down?

MR. SHEPARD: It depends where the system outage occurred. If it were in a process industry, it would be in a matter of minutes, we wouldn't be able to manufacture product. More traditional systems, we can operate for a longer period of time. I hesitate to get very specific because of the public nature of the commission. If you want to talk off line, we can do that.

PROF. MARY CULNAN: Thank you.

DAVE JONES: You mentioned a possible shortfall in the spending area. Is there a need for more awareness on the part of those people that control the funding?

MR. SHEPARD: Within our corporation, we are attempting to do that today. Earlier we had some discussion about how do we ensure compliance with policies and whatnot. We have an audit function that audits regularly with our policies. Through that audit function, we're hoping to raise awareness levels within our management and get the spending if it is needed.

DR. BILL HARRIS: Have you yet found an insurance package that allows you to share the risk about the use of cyber attacks and cyber losses, and that also establishes certain insurability criteria, or is that yet for the future?

MR. SHEPARD: I think that is still for the future. And in fact, our company is what we describe as a self-insured company. We don't look at outside businesses to provide that coverage.

JANET ABRAMS: Thank you very much, Mr. Shepard. Before we move to our next speaker, I wanted to let everyone in the audience know that because of tremendous interest in today's program, we really have many more presenters than we expected, and we're working to see if we can go over the 12 o'clock deadline, and we'll let you know about that, and we hope that those who are called to speak over the next several minutes will work to limit the length of their remarks. Next we'll have Mr. Chase Untermeyer, commissioner, Port of Houston.

MR. UNTERMYER: Good morning. Members of the Commission, my name is Chase Untermeyer. I am a commissioner of the Port of Houston, one of seven members of the board appointed to run the public wharves and facilities of the Port of Houston, which is the nation's second largest port in terms of tonnage. In my civilian capacity I'm director of public affairs at Compaq Computer Corporation, and in prior administrations I served in Washington as, among other things, Assistant Secretary of the Navy and director of the Voice of America as well as assistant to President Bush. But it is in my part-time capacity as a port commissioner that I'm appearing before you today.

We'd like to stress in these remarks the importance of water transportation as critical to the nation's infrastructure. It's important to understand the economic impact of the Port of Houston in this national economy. Port of Houston is one of the nation's busiest ports with more than 5,600 vessels carrying in excess of 140 million tons of cargo through the Houston Ship Channel every year. The Port of Houston generates over five and a half billion dollars' worth of economic activity to the nation's economy, and an estimated 196,000 people depend upon the port for their livelihood. It's no exaggeration to see that the Port of Houston is one of the most important economic life lines that our nation has with the world.

Houston's favorable geographic location and its more than 150 shipping lines give us an easy access to more than 250 world ports. Two major railroads provide cargo distribution throughout the United States with an intermodal length of more than 160 trucking lines. The Port of Houston forms the core of the Houston international community, which includes more than 350 U.S.

companies with global operations, and Houston offices for more than 45 of the world's largest non-U.S. companies. In addition, we're home to one of the largest consular corps in the nation.

In addition to this economic and global impact, the Port of Houston plays a vital role in our national defense. During the Desert Shield/Desert Storm operation, U.S. government deployed 106 vessels carrying 458,000 tons of cargo, U.S. government cargo and military supplies, from our Barber's Cut terminal at the Port of Houston. In fact, between August of 1990 and October of 1991, the Port of Houston was the second busiest port in the nation in support of our troops. We're proud that the strategic location of the Port of Houston allows us to play this role in our national defense.

Keeping this vital link to international commerce open to continue trade is essential. Of the utmost priority to the Port of Houston, indeed, to each of our nation's ports, is keeping our federal waterways competitive in the world marketplace. The project that Houston port commissioners and staff have worked with determination for over 30 years to accomplish is improving the Houston Ship Channel by widening it from 400 feet to 530 feet and deepening it from 40 to 45 feet. The Houston Ship Channel is a narrow, winding waterway, built out of a stream called Buffalo Bayou, which flows a very short distance from where we sit. This progress—I am glad to say—was authorized by Congress and the administration last year, and it will improve safety on the channel, assist the competitive position of the port in the world marketplace and, in an unprecedented approach, provide unique environmental improvements by economic utilization of dredged material. As we meet Congress is working on the FY98 budget which includes a funding request to begin construction on the Houston Ship Channel project. Regular maintenance is also essential for any waterway. To remain functional federal waterways must be maintained at proper dredge depths, with an important impact on safety as well. For waterways that begin to shoal and thus are not operational at recommended depths, they become hazardous to the vessels that must navigate. The ability to operate intermodally, that is through rail and highway means, is an essential ingredient to the movement of commerce and defense material. Continued federal funding with the priority on intermodalism and, for example, the reauthorization of the Intermodal Surface Transportation Efficiency Act, known as ISTEA, is very important to our nation's ports. The recognition of the role ports play in the national economy should be a major consideration in the development of our national highway system as well.

As we discuss the concerns relative to security at the Port of Houston, we must maintain focus on the important economic life line of one of this nation's busiest ports. The port authority employs its own police department with responsibilities that include controlling physical access to public port facilities. The department is an active member of the newly formed joint terrorism committee referred to as the Houston Area Antiterrorism Council. This interagency working group is charged to identify and address through the development of appropriate plans the structure and coordinated effort that will be utilized to respond to major events which may affect the Port of Houston, Houston, and the surrounding area. In addition, the port police department is continuing its community policing initiative, to encourage involvement in crime prevention and cargo security by businesses in the port area.

One of the objectives of the port police department security policies is to establish an environment in which trade may be conducted with a reasonably high assurance of being free of criminal activity and without becoming a conduit for such activity. The port has an excellent relationship with local law enforcement in constricting criminal activity at the port. The department participates in the Houston antiterrorism council as I mentioned, composed of federal and state law enforcement officials from the FBI, the U.S. Secret Service, Drug Enforcement Agency, Houston police and fire departments. While we feel we've established credible procedures in-house, the Houston Ship Channel, as all federal waterways, must be alert to a possible terrorist attack. The many chemical plants and terminals along the ship channel are inseparably intertwined and could be crippled at a blow by one—an action at any of these facilities. A chain reaction of destruction could result from such a terrorist strike. We know that maritime criminals are inclined to operate in waters where government and law enforcement personnel are weak, often lacking in technical and manpower resources. We feel it is the responsibility of the federal government to assist in the protection of this valuable infrastructure and urge you to support sufficient resources to the U.S. Coast Guard to ensure safety at the port, not just in Houston, but around the country.

The increasing complex nature and international scope of maritime security issues which threaten the industry require a wide range of participation and response from all levels of government. The U.S. government has to help create a safe trade corridor. It must obtain multilevel cooperation to address safety measures to assure the stability of our infrastructure. Diplomatic and law enforcement networks are necessary in order to stem the rise in criminal terrorist activity

internationally. The federal government has to take the financial lead in building a secure trade corridor. The federal government must become a partner in enacting at ports security measures. A viable port security program is vital.

Strategic location support to the national defense, the Houston Ship Channel must remain open to navigation, and we are working to see that this is done, but together we must work to assure the safe, efficient movement of cargo and continue the effectiveness of the Houston Ship Channel as a vital source of world commerce.

Thank you very much.

JANET ABRAMS: Thank you, Mr. Untermyer. Our next speaker will be Dr. Mitchell Morris, M.D., Anderson Cancer Center.

DR. MORRIS: Good morning. I would like to thank the commission for the opportunity to present this information. On the risks that are faced by the health care infrastructure in the United States, I am the chief information officer at the University of Texas/M.D. Anderson Cancer Center, and in that role, I serve as both an information technology professional and also as a practicing physician.

M.D. Anderson is the largest cancer center in the United States and is actively involved in patient care, research, teaching, and the prevention of cancer. We also have a very active program involving large computerized network databases that drive medical care through the computerized patient record, telemedicine, and the Internet. We are part of the Texas Medical Center, which, as many things in Texas, claims to be the largest medical center in the country, and I think that's true. According to the engineers at Motorola, in terms of density of cellular phones and beepers, this has the highest density of any place in the world, and we have a complex and fragile information systems infrastructure which I will talk about.

I would like to raise some of your awareness about an emerging infrastructure so that we construct this in a secure fashion. There are risks in the health care infrastructure that may be associated with the information technology age. In health care there is an increasing reliance on electronic records. Advances in information technology permit health care providers, payers of health care, and patients to have greater access to their health care data. There are tremendous advantages to having health care information and a large knowledge base at hand during patient care, and I don't have time to detail all of those advantages for you today.

The technology of health care itself has gained a greater understanding of a number of diseases especially when it comes to genetic issues. Doctors now have the ability to study an individual's genetic background and predict the likelihood of disease or gain an understanding of the exposure an individual has had to a variety of environmental factors.

With the current direction of our information technology infrastructure, there is a potential for significant harm both at the individual level or to the American population in the area of medical care by description of that infrastructure. The old paradigm of health care information is the paper office record. Likewise, there is a hospital office record. Records are typically kept for a period of years and then usually discarded and destroyed. The greatest threat that these records faced was from national disasters such as fires and floods, and that is why medical record departments are never in the basement and the fire protection systems are excellent.

With a new paradigm of information technology, there are three major developments that expose Americans to risk, and these must be addressed. One is the computer-based patient record, another is telemedicine, and the third is health care networks.

Perhaps one of the most high profile advances in day-to-day medical care is the computer-based patient record. Information that was previously stored on paper is now contained within electronic databases. This allows doctors and nurses to rapidly communicate information regarding their patients. The databases concern knowledge bases that support decision-making. Textual information such as notes from doctors and nurses, x-rays such as x-rays and microscope slides, and structure data like laboratory results, medications and results of genetic testing. The implementation of this technology is actively underway across the United States and a large industry has grown up to support this transition.

There are significant potential liabilities with a computer-based patient record. The first is that confidentiality and privacy must be maintained. With a paper record, the physical possession of the document could ensure confidentiality. With electronic media and potential for access by unauthorized persons, information could be used against individuals for purposes of employment discrimination, blackmail or influence peddling. For example, a prominent individual in either government or industry who has had a history of something like sexually transmitted disease, HIV, psychiatric disorder, could be vulnerable should hackers or others access these records.

It would also be possible to alter information contained within these electronic databases resulting in inappropriate medical care and perhaps even dangerous medical care being delivered.

Access to health care can also be affected by unauthorized release of information regarding someone's medical history or genetic background that could affect their ability to obtain insurance. The security of the information must also be maintained as opposed to the privacy. Where no paper record exists, the loss or alteration of source data would adversely impact the quality of medical care. This would be true not only for individuals, but also for large populations.

Loss of functionality of these systems would also adversely impact health care, especially in emergency situations. The computer-based patient record contains not only information about patients, it drives the transactions and operations of health care organizations today. How the equipment runs, their schedules, the processes of an organization. Loss of this function will be devastating to many hospitals today, and to all hospitals in the near future. The ability to transmit lab data, radiology data, and so forth would make delivery of health care very difficult.

Telemedicine represents yet another emerging method of health care that is especially important to rural industries and the defense industry. Telemedicine is a process of providing health care without the doctor and patient actually being in the same physical location. This technology facilitates the review of medical information, consultations, and treatment planning fairly easily and quickly over long distances. It is dependent upon the telecommunications infrastructure such as satellite uplinks and the Internet. It is a technique increasingly used by the Department of Defense for health care delivery to our troops, especially those in remote areas who require specialty care. Disruption of telemedicine and underlying infrastructure would therefore result in an adverse impact on health care overall. Finally, there is a growing move within managed care to form health care networks. Information about patients may no longer be contained in a system in the doctor's office or in a hospital but instead in the network that serves many hospitals in dozens if not hundreds of physician offices. This care provided to Americans over a distributed network presents a new vulnerability since much information is transmitted electronically and may be intercepted, altered, or destroyed. The network permits a large number of practitioners to access information about the clients of that network. They are vulnerable to hackers and other criminals, especially if proper security measures are not in place. My presentation is a little shortened by the comments of the presenter from Conoco—I would second all the comments that he made.

What we need for the protection of the electronic health care infrastructure, I think one of the most important thing is standards. Standards that affect privacy, and there's federal legislation for

that. An area not completely evaluated are standards of electronics and physical characteristics of the data and the systems that use it and transmit it. What are the standards to prevent hackers from getting in? What security measures should be in place? We need to define the required redundancy of systems such as the backups that need to be established and so forth. Disaster recovery and backup plans should be mandated for health care organizations. Also important is protecting this critical information systems infrastructure—provided this critical information infrastructure to the health care sector from the point of view of advanced technology for encryption and other types of security.

I would say an important role for the government is to raise the awareness of the health care industry, the potential threats of systems through educational programs, legislation, and work with other standards organizations such as the Joint Commission on Hospital Accreditation, the Computer Based Patient Records Institute, ANSI, and others. I appreciate the committee's interest in this area and would like to thank you again for the opportunity to bring these issues forward. I'd also like to compliment you on the fine quality of your Internet site, which was a valuable resource to me personally and I'm sure to other citizens who are looking at it.

PAUL RODGERS: Sir, I have a question. You mentioned there should be mandatory security standards. Who should mandate these standards?

DR. MORRIS: Well, I think now the federal government, through legislation regarding the patient record, both paper and electronic, is mandating issues about security and confidentiality. I think through that same mechanism it would be appropriate to mandate what an appropriate security standard is. There is a tremendous range of variability in physicians and hospital administrators' awareness of these types of issues, and my concern is that large systems will be built without the appropriate safeguards in place to recover systems in a timely way.

The question was asked earlier how long would it take to bring us to our knees. Not very long at all. And as we gain increasing reliance on these electronic systems, we're talking about a half hour to an hour before it becomes very difficult to provide medical care. And we too have been the victims of a backhoe a couple of years ago at our campus and have taken steps to prevent that from happening again, but those are some of the kinds of accidental not to mention the intentional interventions that can happen in this infrastructure.

PROF. MARY CULNAN: I know we're crunched for time, but if you could address very briefly in the absence of federal status for privacy and confidentiality and security. What steps

has your organization taken to make the public confident that their information is being handled in a responsible way?

DR. MORRIS: I think to answer that you have to see where we're coming from. A few years ago you could walk into a hospital with a white coat and walk out with a patient's record if you knew the right thing to say. And that's an embarrassment to our industry, and paper records have been more safeguarded. In terms of an electronic record, most of the electronic systems that we've dealt with have audit trails so that you can see when employees are browsing and make sure that only authorized people are looking at records. Certain sensitive information, like I mentioned psychiatric notes and HIV testing, can be locked down so that only certain authorized users are permitted to see that. Our philosophy is that it is the patient who owns that information. It's their information that we are safeguarding for them, and if that philosophy is disseminated throughout the country, that will lead to the proper safeguard to be put in place.

JANET ABRAMS: Thank you, Dr. Morris. We are going to be able to extend the public meeting until one o'clock. We still have a very big stack of requests to speak here with the green cards, so I'd encourage everyone who is called upon to limit your remarks to five minutes if at all possible, and please know that anything you'd like submitted in writing will go into the official record of the commission's work.

Our next presenter will be Mr. Hugh Stephens, representing the College of Social Sciences, University of Houston.

DR. STEPHENS: May I express my thanks to the Commission, and in particular to Mr. Nelson McCouch for the opportunity to present observations on critical infrastructure protection. I would like to express my respect and gratitude to the President, the Congress, and others who conceived of and supported this effort. Although thoroughly worthwhile, it is certainly not before its time. Consider bombings of the World Trade Center, the Murrah Building, and in Atlanta as well as numerous failed attempts—these provide ample evidence not only of threats to the lives and property of citizens but of the potential for disruptive attacks upon systems which are essential to the viability of large segments of United States society. They also demonstrate that the source of such threats has recently expanded to include disaffected elements within this country as well as hostile terrorist groups elsewhere in the world.

My research and teaching specialization is in the area of emergency management and to a lesser extent, political terrorism. I also serve as chairman of Houston's Local Emergency

Planning Committee, am a member of the Coast Guard's Readiness Committee for the port of Houston, and belong to the National Defense Executive Reserve, Office of Emergency Transportation. Since I recently published a book on the Texas City Disaster of 1947—still the most costly industrial disaster in US history at least in terms of casualties—I am struck by the parallels between the goals of this commission and what I found concerning the accidental explosion of ammonium nitrate fertilizer in two ships moored at the Texas City docks on 16 and 17 April of that year. The Commission will of course recognize this as the same substance used to bomb both the World Trade Center and the Murrah Building. I mention this because I found that human ignorance, public complacency, bureaucratic lassitude on the part of responsible Federal agencies, and lack of preparation for serious industrial-type emergencies not only facilitated the onset of the ship explosions but exacerbated casualties and property damage. Further, the aftermath of the disaster clearly demonstrates that attempts were made to obscure liability by means of silence and even disinformation, the net effect being that everyone remained ignorant of the reasons for the disaster and reform was inadequate.

Given what we have learned about the causes of the Exxon Valdez crisis, I wonder if fundamental improvements have been achieved. It is true that safety and security regulations are better today, that emergency management structures are present at federal, state, and most local governments. But the adequacy of protective measures is always relative to hazards and threats embodied in systems and their infrastructures we need to protect against physical disruption. Today, not only is the social and economic viability of our country dependent upon uninterrupted information transfer by means of telephone and computer systems, but disruption of other systems conveying large amounts of toxic, explosive, and flammable materials could wreak havoc among substantial segments of the population and economy. The fact of the matter is that because these systems are complex, and extensively-interactive, adequate protection demands infinitely more sophisticated risk assessment, planning, and response capabilities than was the case even a couple of decades ago.

I assume the Commission is making a good-faith effort to ascertain risks and vulnerabilities of critical infrastructures insofar as is necessary to discharge its duties. As I understand its terms, this body will not engage in detailed vulnerability analysis and risk assessment nor draft programs for improved security and response capabilities. Under the circumstances, I abjure from any detailed description of critical infrastructure and protection in the Houston-Galveston region.

Suffice it to say that the region does share similar vulnerabilities with other large metropolitan areas and is one of the major locations of international finance and banking. The presence of extensive petroleum production, storage and transportation and a port which ranks second in the nation connected to the sea by a long, narrow ship channel provides abundant opportunities for serious disruption of vital systems. But, given what has happened following the International Maritime and Port Security Act of 1986 (Title IX of the Omnibus Diplomatic Security and Anti-Terrorism Act) and Title III of the Superfund Amendment and Reauthorization Act of 1986 (Emergency Planning and Community Right to Know Act), implementation is a legitimate concern. Insofar as critical infrastructure protection is concerned the major questions are as follows: What is in place to maintain continuity of government and provide adequate emergency services in event critical infrastructures in the Houston-Galveston region are attacked and is it at all adequate? That is, have critical facilities and their supporting systems been accurately identified? Given the ambiguities of harm inherent in such complex, tightly-coupled systems, have careful risk assessments been drawn? Are appropriate resource commitments and organizational dispositions extending across normal jurisdictional boundaries in place to cope with expected damage? I am not in a position to make a conclusive judgment on such matters, but my impression is that the situation here does not merit an affirmative answer to any of these questions. With respect to the first of these, as Chairman of the Houston Local Emergency Planning Committee, I can state that inadequate funds have prevented the committee from performing its statutory duty of drawing up a document identifying facilities and transportation routes associated with extremely hazardous chemicals. And I am not at all sure our situation is exceptional. I would add that I am aware of on-going cooperative arrangements among downtown building managers, petrochemical company security officers, and law enforcement personnel concerned with bomb threats. But to the best of my knowledge, these are not at present mutually supporting.

Let me return to my appreciation of the Commission's charge and what I understand to be underlying causes of disasters such as Texas City or Exxon Valdez. I hope that this effort is followed by meaningful steps to enhance the physical security of critical infrastructures. I strongly suggest that the Commission recommend creation of an entity charged with extensive collection of detailed information necessary for comprehensive risk assessment of associated with critical infrastructures. In order to facilitate the task and make allowances for regional variations, perhaps as many as four sub-committees should be established under its aegis, each

consisting of two representatives from the eight categories of infrastructure, including appropriate representatives from the private sector.

When this task is completed, the next step is to tackle the formidable task of formulating response programs. These should emphasize intergovernmental coordination capable of attaining levels of physical security which assure continuity of government and the integrity of operations of those systems within the Commission's scope which are essential to the country's economic, social, and political viability. As unspectacular as they are, these requirements must be met if we are to have much chance of avoiding a disaster caused by terrorism or sabotage on the order of Texas City or Exxon Valdez at some point in the future.

PAUL RODGERS: Thank you very much, Doctor, we'll certainly look forward to reading your statement. Your suggestions have helped.

JANET ABRAMS: Thank you, Dr. Stephens. Next, Doctor Joshua Hill, Dean of the School of Technology of the Center for Transportation, Texas Southern University.

DR. HILL: Thank you very much, and to the commissioners, I'm pleased to have the opportunity and invitation to appear before you this morning. My name is Joshua Hill. I'm the Interim Dean of the School of Technology and Professor and Director of the Photovoltaics Demonstration Laboratory in Texas Southern University.

An educated nation, indeed, an educated work force is our future. If what John Gardner has said about our nation is true, that is, a nation is never finished, you cannot build it and then leave it standing as the pharaohs did the pyramids. It has to be built and rebuilt, recreated by each generation by believing and caring men and women.

And so we've come face-to-face with this prophetic utterance. In some cases this behavior toward our city's infrastructures has been very much like that of the pharaohs. We've allowed our structures to deteriorate to dangerous levels. One-third of the nation's public schools need serious renovation. HISD schools, for example, show signs of serious decay. Projected growth in the number of school-aged children by the year 2005 will exacerbate the problem by requiring more space. Our nation's universities are buckling under the load of deferred maintenance. In Texas alone the estimate is in the hundreds of millions of dollars. Our sewer systems are spewing untreated waste through cracks in broken pipes. About six percent of the country's sewers were installed before 1950, and their pipes are deteriorating. These repairs won't come cheap. The city of Houston, for example, and our leader, illustrious Mayor Lanier, spent a billion dollars in the

upgrade of our sewer system. More funds will be needed to complete the job. Most cities are not as fortunate as Houston to have the leadership that we have in our mayor. This same scenario could be played out with streets and highways, with telecommunication systems. We recognize that we're not uncovering anything that has not been uncovered or voiced by others. However, there can be merit and progress born through redundancy of thought and dialogue.

Why have our infrastructures reached this degree of decline? Well, there are likely multiple reasons. Among these is a lack of money, or probably more accurately a lack of priorities for the use of money on infrastructure. Because many of these failing structures, such as sewers, were out of sight, they were also out of the minds of policymakers. We believe that a cure can be found in partnerships between the private sector, government, and our nation's universities. It is clear that many of the solutions to infrastructure problems will require new ideas, research, and perhaps new ways of looking at old solutions. Our universities are places for innovative thought and research.

Government and industry must be willing to invest the funds needed to attract students and researchers to these areas of need. I suggest that centers of excellence and revitalized America's infrastructures be established at our nation's schools. Grants be offered to promising students to pursue study in areas vital to infrastructure development. Grantees would be required to commit to declarations of promise to commit to at least three-fourths of their grant period in public works associated industries. Secondly, I suggest that we look to our nation's community development corporations who have built up years of expertise in building affordable housing and shopping centers. We look to them for partners in rebuilding our schools and other infrastructures. They have an excellent track record in empowering community residents to upgrade their skills. Those persons that lead the welfare roles can now be trained for meaningful jobs in their communities and rebuilding schools and managing maintenance operations of the same schools.

So, ladies and gentlemen, the time to create a future for our children, free of life-threatening and economic growth stifling infrastructural failings, is now. As partners we can do it. As concerned Americans. We must do it. Thank you very much.

JANET ABRAMS: Thank you, Dr. Hill. Next we'll hear from Mr. Bill Bostic, Vice-President of the Oklahoma Association of Contingency Planners.

MR. BOSTIC: Good morning, commissioners. I can still say good morning for a few more minutes. I'm privileged to come here today representing the voice of the Oklahoma Chapter of

Contingency Planners. I come to introduce you to the Oklahoma chapter of the ACP and to offer our chapter's support for your challenge to develop a strategy of protecting and assuring the continued operation of America's critical infrastructures.

I currently hold the office of vice-president and secretary in our local chapter. I have an information systems/information technology background, about ten years experience. My current responsibilities include managing the data center disaster recovery function for Conoco Incorporated, a major oil and gas company headquartered here in Houston with sites throughout the world including Oklahoma.

For the next few minutes I want to speak to you regarding who the Oklahoma Association of Contingency Planners are, what we do, the tools we use, and how we can begin a dialogue to work to accomplish our mutual goals.

We are affiliated with the Non-Profit National Association of Contingency Planners. National's mission is to provide leadership, direction, and information exchange opportunities to the contingency planning industry and its professionals. There are currently sixteen chapters located in nine states and the District of Columbia. Building on the national charter, the Oklahoma chapter was formed in May of 1993 to provide a forum for education and the exchange of mutually beneficial information and ideas for contingency planning professionals in the Oklahoma region. The Oklahoma chapter began with just nine members, and we've grown in the last four or five years here to a 50-member group.

The current membership makeup in our organization contains representation from all eight critical areas you've identified. Gas storage, nineteen percent; emergency services, fifteen percent; transportation, fifteen percent; banking and finance, ten percent; electrical power, seven percent; continuity of government services, five percent; and water supply systems, two percent. The balance of the membership serves basically in other continuity planning areas such as vendors and suppliers in contingency planning products and services.

Most of our members are charged with varying levels of responsibility with respect to computer information systems. The majority of our members—as is typical of the contingency planning professional—wear the hats of a strategist, a long-range planner, a coordinator, and an enabler.

To help sell the awareness and need for disaster recovery as you've heard today to communities and to employers, we typically use the tools and methodology such as risk analysis and busi-

ness impact analysis as well as protection/response planning development tools that Mr. Stephens referred to a moment ago in his speech to accomplish our objectives. We bring to bear some of the more simple, practical lessons learned in the use of these tools which I've included in my written statements.

These tools continue to be invaluable in creating effective protection and recovery response strategies and plans. Your challenge and ours, however, is to develop a strategy which integrates the product of these tools across the critical infrastructures and technologies which they depend upon. We here in Oklahoma are progressing down that road.

In Oklahoma, we are meeting this challenge by working to apply a concept which has become known as Disaster Recovery Business Alliance, or DRBA. This concept was born in California in 1994 through an effort sponsored by the Electrical Power Research Institute in conjunction with various public and private enterprises. The overall vision of DRBA is to become an international leader in mitigating the physical, economic, and ecological impact of natural and man-made disasters to people, property, and businesses.

In 1995 the National ACP board and EPRI proposed that the Oklahoma ACP chapter be only the second group to enact such a program under the DRBA umbrella.

The vision of the Oklahoma team is to build on the overall concept by forming regional partnerships with utility, telecommunications, food distribution, banking, insurance, volunteer, and research organizations, as well as government at all levels. We are early in the process of obtaining funding and support for the Oklahoma project.

To date we have held a series of face-to-face meetings with major businesses in the region to gain support. Some of these companies have stepped up to the plate to provide not only dollars, but in-kind services. We have additional meetings planned with the American Red Cross in Oklahoma and other major businesses. After startup support is gained—i.e., money—is gained from our efforts, a part-time administrative function will be funded and buildout of the program will begin using the EPRI model as a model to work from.

In order to establish a dialogue with which to build on our mutual goal, I have taken the liberty of providing you with some additional information about our chapter and about the ACP in general. At each of your individual wishes, we and the Oklahoma chapter can include you on our Oklahoma contingent newsletter mailing list, simply a monthly newsletter of our activities, our speakers, and the types of things that we are doing in Oklahoma. We also extend to you,

individually or as a group, an invitation to attend our meetings as a guest speaker or simply to learn more about us by attending as our guest. Our meetings are held the third Wednesday of each month. Typically they're held in Tulsa, Oklahoma, but they are held in outlying regions in Oklahoma where we have other members.

At a national level, the National ACP will be sponsoring in Utah in October the "Bridging the Gap" ACP Symposium. Additionally, I have also made arrangements for you to receive the current issue of the *ACP Sentinel*, the National ACP communication which is in the packets which has been provided.

In conclusion, those of us in the field of contingency planning recognize and understand the importance of your charged mission. We applaud the administration for having the foresight to create Executive Order 13010, and we especially applaud you for your efforts to implement the order. We look forward to working with you to complete your goal in the future.

JANET ABRAMS: Thank you very much, Mr. Bostic. Thanks for coming all the way to Houston. Next we'll hear from Dr. Larry Leibrock, from the University of Texas.

DR. LEIBROCK: For the sake of time, I've got handouts for each one of the members. I'd like to thank you for coming to the fine state of Texas. By way of introduction, I'm a Hewlett Packard employee on a one-year sabbatical to the University of Texas. My responsibilities there are predominantly chief technology officer for the graduate school in Austin. I'm responsible for seven-day-a-week, 24-hour operation of approximately a thousand desktop computers, on a hundred miles of Cat-5 ethernet cable. I'm also responsible for the operation of 50 operational—it's now going to come apparent that I'm not a public speaker—I'm responsible also for approximately 50 servers there at the school. I have a customer space of about 6,000 users. The goals of my talk today are really to talk about information on security. I want you to know, however, that I'm a specialist in this area. I have approximately 15 years of experience.

My opinions today are simply my own. They're not the official opinions of the institutions at which I'm involved. I think all will agree that this—that critical infrastructures are clearly the—critical for our ability to function in a complex society. However, I'm concerned and I think there's a general poor understanding and notion of stewardship in terms of the ability to support these systems.

I think, unfortunately, many of us in the field of information technology focus on some sort of technology kind of solution as a means to protect this critical infrastructure. Unfortunately, I

think a lot of the conversations in terms of information technology tend to focus on technology artifacts. Is NT better than one other type of system? And consequently I think they failed to talk about the point that in any computer system there are inherent uncertainties about operations, and there are vulnerabilities that are inherent in every type of computer system. In my opinion, frequently the highest source of vulnerabilities is the failure of choices that people undertake when they operate these particular systems. I also want to assert that people sometimes don't take the responsibility of protecting these particular environments. As an example, I would like to discuss the idea of user passwords on systems.

This is the primary technology for the identification and authentication of most people when they interact with a typical computer system. There's an acknowledged failure of most people to properly select and care for passwords. And I've got some documentation. Despite clear evidence that poor passwords were clearly a factor in an incident in 1988, people still don't take the responsibility to collect and use passwords as a responsibility that they must own.

I'd like to discuss essentially and provide some data that I developed when I was asked to testify. About 30 days ago I did an analysis of a password typology on a system at the University of Texas in Austin. It disclosed that approximately 400 passwords that were used by both faculty and students were to be compromised by a simple selection of words in the English language dictionary. I used a standard tool that's available on the Internet, and I was able to crack these 80 percent of the passwords in about five minutes. So, consequently, my point is that in spite of building complex computer architectures, people don't select or take responsibilities for something simple like passwords, which is in my opinion kind of counterproductive.

I think that implications can be drawn from this, as I would like to think that we can build a community of interest. I think there's a community of interest in terms of responsible types of behavior for information systems. I'd also think we need to clarify the need to educate people about the proper stewardship of information systems.

I'm also concerned about the supporting professional learning opportunities for both generalists and specialists. Particularly in my profession, the shelf life for technology is quite short; consequently, if you are really an expert in the field, that shelf life is six to eight months without additional training. It requires, really, I think a professional support system for that. I also think we need to better articulate both collective and individually our responsibilities for

information security. It's my opinion this is a shared responsibility among professionals and end users.

Some concluding kind of thoughts. I'd like to think about moderating our expectations about what type of technology might be best or not. I'd also think that, frankly, looking for a simple technology fix is probably inappropriate. I think we need to think about sharing the idea of best practices for system security, and I think this is, frankly, a process and we will never be complete; it's an ongoing process.

I'd also like to think about establishing collaborative environments between industry, government, and academic institutions, and I'd like to focus on some common efforts. The examples I think are the National Security and Federal Information Policy and information system security. I think we need to think about additional joint partnerships for us to help solve these issues.

I'd like to thank you today for allowing me to talk. It's blindingly apparent that I'm not a public speaker, and also I'm really a geek, and also I'd like to thank you for soliciting from the public that kind of opinion, and I'd like to personally acknowledge all of your time and efforts. Thank you very much.

PROF. MARY CULNAN: Dr. Leibrock, could I ask you a question? I share a lot of your concerns. Are you aware of anything that UT is doing to help make its students more responsible citizens of the information age?

DR. LEIBROCK: For all incoming, first-year graduate students at the business school, we now have a 30-minute course—a short course on teaching people what is appropriate kind of behavior. However, we found that the shelf life is also fairly clearly short and it looks like we're probably going to have to do this every semester.

We also teach a information security course for systems professionals, and, frankly, from looking at the site, it's on the Web, a lot of other academics are also interested in that area.

BRENTON GREENE: Do you have that web site?

DR. LEIBROCK: It's <<http://praetor.bus.utexas.edu/>>.

JANET ABRAMS: Thank you very much. Our next presenter will be Mr. Joe Moore from Southwest Texas State University.

MR. MOORE: Members of the commission, I'm Joe Moore, a professor in the department of geography and planning at Southwest Texas State University where I teach resources and environmental policy. I am also a director of the Freshwater Research and Policy Center.

In the past, I have directed the staff of the Texas Water Development Board in the preparation of the first 50-year water plan for Texas and served as the chair of the state's Water Pollution Control Agency. At the federal level, I ran the National Water Pollution Control Program in the latter days of President Johnson's administration, served as program director in the National Commission on Water Quality chaired by vice-president Rockefeller, and was briefly deputy to the assistant secretary for management in the treasury department in 1993.

Texans rely on their water supply on some 190 surface water reservoirs larger than 5,000 acre feet. These reservoirs impound roughly 30 million acre feet of water and can produce a firm annual yield of some 11 million acre feet. There's only one man-made—one non-man-made reservoir in Texas, and that's Caddo Lake on the Texas-Louisiana border. All cities in Texas are required to treat their municipal wastewater to considerably higher standards than those required by the federal Clean Water Act because our wastewater discharges serve as a downstream water supply for cities and users in the river systems and for preservation of our fish and wildlife resources in the Gulf Coast.

The wastewater treatment plants are essential for the water system because in our longest rivers, water must be used at least five times before it reaches the gulf. Destruction of these wastewater treatment plants would endanger the quality of the water supplies for downstream users as well as for coastal waters.

I do not know how all these water facilities could be fully protected without substantial manpower and high-tech communications. Reservoirs are often in rural areas with limited access. Water treatment plants, pipelines, and canals, and wastewater treatment plants may be in less populated areas. Without the kind of security and manpower that might be available in time of a national emergency, protection of every reservoir and treatment plant appears impossible.

We have some of the longest surface water distribution systems you can find outside the state of California. For example, water is transferred from Lake Meredith in the Canadian River in the Texas panhandle to Lubbock by pipeline. For Houston, the coastal industrial water authority operates a canal from Lake Livingston to this city, a pipeline from Lake Texano on the Lavaca River to Corpus Christi is planned, and in the future we may need conveyance facilities from Toledo Bend Reservoir on the Sabine to the west of Houston to get water to this city. There's also the possibility of a diversion from the Guadalupe Blanco River system to San Antonio. Some 90

percent of this state's population live in these urban areas. And destruction or damage to the reservoirs or the distribution systems would be critical to this state's contingent operation.

Also, Texas has the last leg of the gulf intercoastal waterway from Port Arthur to Brownsville. Bridges across the waterway are either constructed to navigation heights or capable of being opened for traffic. This was to provide distribution of freshwater to Texas coastal estuaries as well as a means of transportation. Its protection requires a different approach. One area in which the federal government has reduced financial support is in the collection of water quality and quantity data. Texas has historically been second only to California in the joint federal-state-local partnership of data collecting operated by the U.S. Geological Survey and the Department of the Interior. While the state, too, has reduced its support, the size and the extent of the program is largely dependent upon the level of federal funding. We now collect data in Texas at one-third fewer stations than were in existence 30 years ago. Without adequate water data, emergencies, whether natural or man-made, cannot be adequately addressed or managed. The amounts involved are minuscule when compared with the total national budget, but the need for data is critical when an emergency occurs. I urge you to consult with the U.S. Geological Survey to determine adequate funding for water data collection so that agents at all levels can plan adequately. Thank you very much.

JANET ABRAMS: Thank you, sir. Our next presenter will be Dr. Richard DeMouy from Southwest Texas State University.

DR. DEMOUY: Good morning. My area of interest is in modeling and analysis of emergency health care systems and the delivery of those systems. It's of interest to note that in the United States, that accidents are the leading cause of death in the United States for those people 45 years and younger, and they represent the fourth largest reason for death in the United States, following heart disease, cancer, and cerebrovascular disease. We know that we have approximately 90 million emergency room visits per year, and that 40 percent of all hospital admissions are through the emergency department, and this is significant when we consider that hospital emergency—rather, hospital admissions are decreasing at the rate of about ten or thirteen percent over that same period of time.

Now, whether we're talking about the small emergency that deals with the individual or the large emergency that relates to such an event as the Oklahoma bombing, we have to worry about

what kind of infrastructures do we have in place in order to provide the emergency care that our citizenry has come to expect.

What got me interested in this particular area is in San Antonio in the early 1990s, I was driving down the road listening to the news, and they came on and were talking about the fact that all of our level one trauma facilities were closed to the admission of trauma patients on a regular basis because they had exceeded the capacity of the emergency room. And so I began to look into the problem. As a researcher, I was concerned with how we got in this condition and, given that the city was continuing an upward slope in its growth, what was the future going to look like if we weren't doing the necessary strategic planning and building of the infrastructure in order to take care of that? Well, that began a process of looking into how do we model emergency health care delivering systems, and I looked at several different areas.

The first area was the structural change and how do we fund care in this country. And as you know, we switched from a fee-for-service system to a prospective payment system in the early 1980s, and we've noticed that there have been certain structural changes to the way health care is delivered. In particular, we've seen that over about the last ten years we've seen approximately 90-plus trauma centers closed in the United States.

A second thing that was of interest to me was comparatively at the production sector of our economy. And at that point in time back in the mid-1990s, we saw institutions such as the Chrysler corporation and our automobile manufacturing base begin to get into significant trouble vis-à-vis the Japanese in terms of their competitiveness. One of the things that we noticed about the automobile industry was that they recognized that one of the problems that they had was that they were not producing a product at the same level of quality and at the same cost and competitive nature as those cars that were coming in from the Japanese economy. And they began to adopt what's become known as total quality management. And so we began to look at how does total quality management differ in the production sector as opposed to the service sector.

And one of the things one notes right away is that in the production sector when a customer comes into the showroom, they can say, "I want that blue car, I want it to have 230 horsepower, I want it to be able to get 40 miles to the gallon." But when a patient arrives at the emergency room, it may be a patient that's unconscious, it may be a patient that's impaired as a result of drugs, or it may be a young child who has no way of telling the people there in the emergency room exactly what it is they need or where it is that they hurt.

Secondly, in addition to not being able to specify in very clear terms what the issue is that represents a problem for them, we also, when we are in the emergency room environment, have to create the product or the service in this case on demand. We can't store out good outcomes. I can't store out a patient that survives a car accident, or I can't develop a patient that survives a gunshot or a stabbing. And so, unlike the production sector, we have to plan in order to be able to produce that outcome when the patient presents in the emergency, which again is quite different from the industrial sector.

What that leads to is that in the emergency environment we have to provide excess capacity. And where that affects the process is that in this time of managed care when they're attempting to reduce down everything to its lowest level so we're providing just essential services and care, then that comes in direct conflict with what's going on in the emergency room and it creates a problem.

Well, in San Antonio, I began the research. And what I wanted to do was rather than looking at emergency rooms and trauma centers as places where activities go on, which has been classically modeled where people worry about how fast are X-rays returned or how fast are blood samples tested and that information got back to the physician, I was interested in looking at how the system itself operates.

And in San Antonio, as you may know, we have three level 1 trauma facilities. We have one civilian facility, the University of Texas Health Science Center. We have Wilford Hall Air Force Hospital and Brooke Army Medical Center, which is a new 450-million-dollar facility that the Army constructed. The Air Force hospital and the Army hospital share a joint residency program, and they train all of the physicians that are going to be provided to both the Army and the Air Force.

What was of interest to me in this process was, what would occur if the dynamic of that equation were changed? For example, what would happen if we had a war in Central or South America, and those physicians were no longer available? How would that impact the delivery of services to San Antonio? And that was the systemic look that we were taking, how the health services, the provision of health services changed in the system, as opposed to how do things change within the hospital structure itself. So we now have built several computer models, one for each of the major trauma centers and one for the transportation linkage, which ties all of those facilities together. Our plan is to extend that model to a 22-county area to the south and to the

west of San Antonio, called Region P, and hopefully be able to model the entire state of Texas, which consists of 22 other regional centers.

Again, what I'm concerned about in this process is not how does a hospital operate internally, even though that's very important to the way that the hospital produces the product that it's supposed to be producing, but how does the system produce and deliver care at a local, at a regional, at a national level. And I think one of the things that we need to move forward with, specifically given that we now have the computer capability and the software capability to tackle these kinds of problems, is we need to begin to do this type of thing so that, just like in war gaming exercises, we can model the process without building the hospitals, without installing the transportation infrastructure, do the cost-benefit analysis to determine where we need to place our medical assets and develop a national policy based on modeling just like we do in terms of the defense department when we do our wargaming or analysis in that fashion. I provided written comments that expand on and summarize the things that I've spoken about today, and if you have any questions, I'd be glad to answer them.

BRENTON GREENE: Excuse me. Has any of your modeling pointed and turned into positive results in investment directions, or pointing towards shortfalls to change how you plug in resources to improve university health care, et cetera?

DR. DEMOY: As a matter of fact, when we looked at a couple of the hospitals, we actually ran what are called scenarios in which we reduced the number of physicians or changed the mix of physicians or nurses or reduced the number of rooms that we had, and we could demonstrate that we did not have a diminution in terms of the time that people spent in the system or of the throughput of the system, and it suggested ways that we could reconfigure the delivery.

So the answer is, yes, I believe that once we get the models finalized, once we get them standardized, that the possibility certainly exists that we could apply these to looking at resourcing or structuring the delivery of care within New York.

JANET ABRAMS: Thank you, Dr. DeMouy. Thank you very much. I now have an announcement. Is there a Dr. Ronald Bailey present? If you would, please see the staff outside. There's a message for you right outside the room.

Ladies and gentlemen, for those of you who remain, we have nine requests to speak left and less than 45 minutes. So I encourage you to limit your remarks to five minutes. Next I invite Dr. Tom Talley of the Department of Engineering Technology, University of North Texas to present.

DR. TALLEY: Thank you. I thank the commissioners for coming to Houston, and I thank the Mayor for the hospitality and the opportunity to talk. I'll keep my remarks very brief.

In another life before professor, I was the engineer responsible for designing the internal telecommunications networks for the electric utility that was represented by Mr. Green here earlier, and I think you heard the extensive measures that are taken to ensure the reliability of the electric utility and its services.

But I would like to point out a few things. For example, there are a range of threats which can't be overcome by procedures and policies. I watched the television this morning, there was a tornado which went through downtown in Miami. Unless our legislative process is more effective than it has been in the past, I don't think there's any policy change or legislation that could be enacted that would prevent that sort of thing. So without dwelling on that much, I think really the key to electric reliability is the ability of a utility to communicate and marshal its forces in a restoration manner. I don't think a single individual or a small group of people short of a well armed and determined and capable adversary are capable of doing as much damage to the reliability of the electric utility industry as natural disasters are.

What we can do is damage our ability to recover from these by inappropriate activity on the part of the federal government.

One of the difficulties presented by deregulation of the telecommunications industry and now deregulation of the electric utility industry is the actual ownership of the customer and ownership of the responsibility for restoring services. Electric utilities used to be completely vertically integrated. They generated power, they distributed it, sent it to the customer, the customer called them when the lights went out and so forth. Now, with deregulation, this may not be the case, and, quite frankly, I think it's up to government to see that the responsibility for service restoration is placed firmly in someone's hands in this deregulated environment.

The other thing you have control over more than anything is the access to communication frequencies for use and the restoration and management of crews. I think it's very important that the commission recommend a couple things. Since it's not possible to prevent large-scale outages from occurring, the best thing that we can do is ensure that these outages are mitigated as rapidly as possible by allowing the utilities to maintain their primary assignments in radio and microwave frequencies, remain available to utilities. Recently in our deregulation efforts, several of these microwave frequencies were removed from the utilities and given to PCS services.

While these are very important, I think we should note that that diminishes the capability of the utility to communicate internally. Also, I think under certain circumstances, the telecommunications restoration plans have not been followed. For example, Oklahoma City, I understand there was some difficulties in telecommunications restorations based on interagency discussions about priorities, and, quite frankly, I think that's on the ground. It is not the place to make those decisions, so I urge you to urge FEMA and others to take leadership roles in coordinating the planning of restoration of services when these kind of things occur and aid decision-making on the scene.

Thirdly, I would like to point out that people who always show up on emergencies we don't talk about much. There's the Red Cross, Salvation Army, and also the amateur radio operators. We provide recreational land for people—amateur radio operators enjoy and recreate in the radio frequency spectrum, and, quite frankly, they then bring all of their equipment and expertise to bear when asked to in emergencies, and I would urge you to encourage the Federal Communications Commission to support the retention of radio spectrum for allocation to the amateur radio service. They're a valuable part of our process. Be glad to answer any questions.

JOHN POWERS: Dr. Talley, I would welcome any examples of situations where response decision-making has been left to the ad hoc, on the ground, where the ultimates were less than optimal.

DR. TALLEY: I'd be happy to provide that.

JOHN POWERS: Thank you.

JANET ABRAMS: Thank you very much. Next we will hear from Dr. Michael Carroll of Rice University.

DR. CARROLL: Good afternoon. I appreciate the opportunity to address the commission, and I'm very pleased to be here to represent the best university in Texas.

You heard earlier the professor had a tough time with the 50-minute time limit and deans have a trouble with that, and I have trouble with any kind of time limitation whatsoever; however, I will do my best. Hopefully without seeming unduly self-serving, I'd like to discuss a major concern from the perspective of the dean of engineering. How to sustain and strengthen undergraduate and graduate education and research in engineering especially in the classical traditional engineering discipline, the electrical and mechanical, and particularly mechanical and civil engineering. I should emphasize that this is not just a local concern. I've been for four years

on the governing board of the engineering dean's council, so I'm well aware that this is a national concern. I believe it is also pertinent to your commission's activities, especially as it pertains to protection of our civil infrastructure system, as described by Mayor Lanier.

My concern is the same as that expressed by Judge Eckels, our vulnerability to neglect. Part of the concern is the level of federal support for the academic engineering enterprise in general and particularly with regard to search and development in civil infrastructure systems protection.

One of the questions that you posed to me was, "What services do you provide and who are your customers?" I believe that any good engineering school has two products, if you will. People and knowledge. Firstly, we educate a cadre of talented professional engineers and innovators. We help to produce a well-educated citizenry, doctors and lawyers and businessmen and women with a good understanding of technology. Secondly, we are involved in a partnership with government and with the private sector to discover and apply new knowledge and apply technology. I emphasize that engineering enhances the human condition and engineering creates wealth.

What attracts bright young people to engineering? I believe that there are three main factors. The first is intellectual challenge and excitement. The second is a sense of national urgency and the opportunity to help humankind. The third is a pragmatic consideration of job opportunities and money. While this last one is an important consideration, I do not believe that it is the dominant one. Our young people have a considerable sense of idealism. However, it is unfortunate that we have created a reward system that attracts some of our best young people to Wall Street rather than to Main Street. Within engineering, the attraction to new high-tech disciplines such as information technology and nanotechnology is clear. The intellectual challenge, the rate of discovery, the sense of importance of the enterprise are palpable. The situation with regard to bioengineering and environmental engineering are similar, with the added attraction that the opportunity to help humankind is clear. The attractions to mechanical or civil engineering are somewhat less clear. However, these disciplines are critically important to the protection of our critical civil infrastructure. We must do all that we can to heighten the sense of challenge, a sense of intellectual excitement, the opportunity to come up with new ideas, and also to emphasize the national priority and importance of this effort. When I first learned of this Presidential Commission on Critical Infrastructure Protection, I was very pleased that we are finally addressing this issue. When I saw the scope of your charge, which I believe is very appropriate, I was

nevertheless somewhat concerned that the importance of protecting and enhancing the civil infrastructure systems may once again be deemphasized. It's less exciting than the high-tech information technology aspect.

I hope that you will not allow this to happen. I do not suggest that this is the most critical area, but rather, that it is the one that tends to receive the least attention. With some time remaining, I'll tell you a little bit about Rice University and the partnerships that we're presently engaged in. I think there's not much time, so I will resist the temptation to brag too much. We have a very strong effort in nanotechnology. Our leader, Smalley, just received the Nobel prize. The leader of our information technology effort, Ken Kennedy, has just become the academic co-chair of the President's Advisory Board on High Performance Computing, Information, Technology, Telecommunication and the Next Generation Internet. Quite a mouthful. We also have very strong efforts in biomedical engineering and in environmental engineering, very strong partnerships both nationally and in the Houston area. I just wanted to mention that recently my faculty came up with the recommendation that we create a civil infrastructure, a new institute on civil infrastructure systems, and I think in light of Mayor Lanier's remarks, I really would like to see us involved in a partnership with the University of Houston and the city of Houston in this important area. Thank you.

JANET ABRAMS: Thank you very much, Dr. Carroll. Our next presenter will be Richard Baker, the chief operating officer, City of Houston, Department of Aviation.

MR. BAKER: Good afternoon. I can say it officially. I'm impressed with your ability to sit here. There is other critical infrastructure necessary to work on, my back is hurting from sitting there so long. You may give me the magic warning, four minutes. I just wanted to take an opportunity to discuss airports, and you're familiar with that as some of the, you know, infrastructure that's of concern here in the United States. I just want to comment as well, the scope of your activities here is a daunting challenge. We have been looking at airports in the last couple of years, or commission, I'll get to that in a second, and we focused on air transportation, airports, airlines, that sort of thing, and that's been a lot of work. So of the eight that you've put out here, seven of those are concern to us at airports, but getting this down into a report that makes some sense and readable and the like is going to be quite an effort.

Basically here in town we have the George Bush Intercontinental, recently renamed, about 26 million annual passengers, hometown Continental Airline, then, also Hobby, which is a serious

air carrier airport, eight million passengers a year, another home—Intercontinental has the highest level of security, and Hobby also with a high level of security. We have Ellington Field as well, which used to be an Air Force Base, the home base of NASA, pilot training, and some international guard, Coast Guard and the like.

I want to talk about the Gore Commission. That was basically another presidential commission in the works, looking at some of the same matters that you are, and it was therefore—looking at their transportation safety and security in particular. We at both of the two airports here, because of their level of testimony, did what we call vulnerability assessments followed up by the action plans, and those were submitted to the Gore Commission, Federal Aviation Administration, and I'd like to—actually you don't want to hear the specifics, we don't have the time, more than that I can't tell you because that's all security classified. That's one of the new federal aviation regulations.

We use local consortia, that's basically the people, the users to get together talk about what the vulnerabilities were, and we put together a couple of plans that the FBI have told us have been pretty good in models for some of the other airports. Certain of our key management have gotten key security clearances so that we could get some additional information and we work closely with the HPD and the FBI.

That's the Gore Commission. I want to tell you what we learned from the full process and my recommendations here.

Basically, you're not going to be able to identify every vulnerability or threat or anticipate those. That's one thing. If that was any part of your objective, that's just nonsensical. The key to success on trying to anticipate problems is getting the best intelligence. And that's something we've been trying to do, is get the FAA and the various federal agencies, the local agencies to do a much better job at getting specific threat information. If you can do that, you can do something about it. If you don't get that, unfortunately, you know, the world in general, and the United States in particular, is what the military calls a hard rich environment. You can drive yourself nuts trying to figure out how to address all these things.

Long-term planning and design of infrastructure should be one of your concerns. This stuff does not happen quickly. It should be from a deliberate process and not a reactive one. And unfortunately, a lot of transportation policy and other policies of the federal government have

been made reacting to the last event, and that last event comes in the context for action to the next event, and that is not necessarily where we need to be.

Long time—Important to recognize the priorities will change over time. As we've heard today, technologies change over time, so you have a bit of a moving target and you have to adjust the process.

Now, clearly it's been mentioned before, substantial funding is going to be required, and one of the things that's been noted from the air transportation industry, the airport improvement program and some other, operating funds from the Federal Aviation Administration and other agencies has been on the decrease as opposed to the increase, and clearly any kind of hardening of facilities or any kind of better, you know, security or the like is going to be more expensive, not less expensive, and I think the federal government maybe needs to identify some of the priorities, and maybe you can help them with that sort of thing.

We'll just leave it at that. I thank you for opportunity. I've got less than a minute for a question if you want one of those. Thanks very much.

JANET ABRAMS: Thank you very much. Our next speaker will be Robert Hiromoto from the University of Texas at San Antonio computer sciences division.

MR. HIROMOTO: Good afternoon. My background is in Los Alamos for approximately thirteen years. I've been doing research there in parallel computing. I came to San Antonio in 1993. They wanted me to put together a computer science program there that was based in high performance computing. Let me just start off by saying something pretty trivial. That is that knowledge or, parenthetically, information is power, and with that, of course, there is protection, protection for that power, and also restriction that is imposed either by legal, moral, maybe ethical considerations.

I think, in looking over the charge that you have, there really is two areas where information really dictates the direction of the industries. Those two are telecommunications and computing.

And since coming to San Antonio, I've been involved in a telecommunications project which is mobile wireless communication. We're trying to put together a system there to do mobile wireless communication. One area would be, for example, emergency systems. So, for example, an infrastructure could be built—and I think it is being built right now—where you have sensors in the highway, computers monitor that and send that to a central location. They are then trans-guides along interstates and highways. That information could then be used directly to sup-

porting emergency vehicles in terms of moving patients directly to emergency location, hospitals, for example. All of this is done through the technologies that have come across because of telecommunication and computing. And in fact, both of them sort of work hand in hand together.

I think that the major explosion in telecommunications is the fact that computing is exploding in speed. I believe it was probably in '71 when IBM came up with their PC. At that time I think the speed was like five or so, six megahertz. Today I think we're talking about 190 megahertz. I think Intel will be announcing a product of their Pentium which will be a speed of about 233 megahertz, and I think within a year after this probably about 300 megahertz. Dell has a processor that goes up to 500 megahertz.

The importance is what we have now, is we really have high performance personal computers. And that is, in some sense, is going to drive the shape of our economy, but it also has a lot of consequences. For example, it's now going to be an easy tool for anyone to have to do their hacking, and their hacking can come in lots of different forms, but clearly one is—will disrupt the infrastructure that we have.

The personal data surveillance. That's going to be a big issue. Personal communications—where the computational part comes in is to take that information and make—or try to make some sense out of it, put it into a form that's understandable, visualize. Unfortunately, or fortunately, we're at the point of doing that. We are now really in the Information Age, and it's a little frightening in a sense. There's a lot of power that goes with it.

I think another thing that has to be, I'm sure, a concern for the Department of Commerce, that is, at what levels can we be exporting PC's to other countries? And in particular, unfriendly countries. I think because of the ways everything is moving so quickly, one of the major problems you're going to have, that the countries have to face is deciding or identifying potential problems that we have to address, and that's going to change so rapidly. And we have to act quickly. It's not just a matter of identifying, but to address those problems. One technology that's emerging in computers right now is that idea of metacomputing where people use the Internet to find idle machines to do some additional computations on. This is seamless computing, and it's a potential area of real problems.

So, I thank you very much for your time.

JANET ABRAMS: Thank you, Dr. Hiromoto. Our next presenter will be Wayne Sorenson from Southwest Texas State University.

MR. SORENSON: Gentleman, good afternoon, Mr. Chairman, ladies and gentlemen of the commission. Thank you for inviting me here. I'd like to introduce myself. I'm Wayne Sorenson, the Chair of the Department of Health Administration, third in the trio of Southwest Texas professors to present to you today, and I'm pleased to be here.

My topic has to do with health care delivery in America, and I just want to remind you that we have the best health care system that money can buy in America, and we have health care, as expensive as it is, because we choose to pay for it. On the other hand, health care delivery in America is fragile; we've spent a great deal of money on that health care delivery, and yet it's quite vulnerable to disruption in its support. It is not self-sufficient. Health care delivery in America is totally dependent on the infrastructure. And it depends entirely on continuous support from sources of energy, communication services, transportation, and financial services. We'll come back to financial services at the end of my presentation. A breakdown in any of these available support systems could cause central health care services to cease, and under the delivery system as it exists today, could deny essential health care services to our general population within three days. I base this on a situation where a large-scale emergency could occur, such as breakout of war, large storms, flooding, similar effects, that could affect the infrastructure system as I mentioned.

Why? Because in the interest of efficiency over the past several generations, we have reduced the ability of our health care facilities to act independently. We are now dependent upon each other to a greater extent than ever in our history. Where once we had 30 days' supplies of expendables in our hospitals, now it's typically just in time delivery. And that's fine, as long as you have an adequate infrastructure that supplies you with the people, supplies, equipment, and energy that you need to short notice.

In other words, it works well in ordinary times. It does not work well in emergencies. We rely on evacuation of patients to extend our services throughout a region, for instance. Deny access to transportation, and evacuation is no longer a choice. Essential sophisticated health care services disappear.

We rely more on managed care today than on inpatient services than we once did. It's cheaper to provide managed care services, but there is little depth in that service for emergencies. We are downsizing, we are closing hospitals, we are expanding outpatient clinics, and preventative

services. Again, this is fine, in ordinary times, but in an emergency, an emergency would force a triage of patients.

Now triage is a common term to use in the military. It's a common technique used when there are insufficient access to people, equipment—in other words, the same things we've been talking about. However, triage turns the health care delivery system upside down. It's ineffective, an unpalatable choice to most Americans, and will only be used in an extreme emergency. It's where you treat those who need the minimum amount of help and ignore those who need the greatest amount of help. We don't do that routinely.

You heard testimony about how the sophisticated Medical Center and best health care system in the world provides for the most exotic care. People are brought there who would otherwise die. We have delivery of children who weigh less than a pound. It's routine. Those people would not be provided health services in a triage setting. That's the effect in an emergency. We give up those accesses to sophisticated services.

If you think this sounds alarmist, then let me mention one thing that has happened in the health care delivery system in the former Soviet Union. They have lost the ability to provide health services not because of their infrastructure as we discussed it disappeared, but because they lost their financial support. They lost 80 percent of their money. As a result the health care system has literally collapsed.

That to me is the greatest threat in the long term to our health care delivery system. We have an infrastructure system second to none in the world, but we're starting to question the cost of health care delivery, and we don't have enough money to go around to do everything.

I'd be glad to answer any questions you have. I wish we had a little bit more time to discuss this. Thank you.

JANET ABRAMS: Thank you very much, and I regret that we don't have more time, but anything you'd like to submit for the official record will be included.

MR. SORENSON: Thank you very much.

JANET ABRAMS: Next, Ben Zon from Southwest Texas State University.

MR. ZON: Thank you very much for the opportunity to speak here. I'm Ben Zon, and I'm working as a faculty member at the Department of Geography and Planning at Southwest Texas State University.

Because we have limited time, I'm going to make it very brief. I'd just like to mention three points from my perspective that I believe are important for the national infrastructure. That is environment, transportation, and spatial data infrastructure.

Over the years I have learned—you learned in this country that the more roads were built, the more congested those roads tend to be. We still don't really understand why. And from my perspective is we really have limited understanding of how the transportation system functions as a whole. So it's my contention that we really need more research in this aspect to consider this system as a whole system, not only a construction of more highways, but how transportation and land use with the environment and how people actually perceive the transportation infrastructure and how we live in the environment. Secondly, the impact of transportation on the human and physical environment as we can see is enormous. First of all, we have the modification of the physical environment. And secondly, when we have more highways going, we bring along constructions along those highways. So there is a modification on the human landscape as well. Then there is air pollution and noise. And how we are going to really address these environmental issues relating to transportation is to the best interests of the nation and to the very well-being of the American people.

The third question that I'd like to raise is that any research related to the transportation and environment has to do with spatial data and spatial data infrastructure. There is research in the—called the national spatial data infrastructure. I'd just like to emphasize here, for the national information infrastructure, that's a very important component, because anything always happens somewhere. To research or to practice in transportation and the environment, we always need that information, and there will be more support from the federal and the state level for developing a national spatial data infrastructure. Thank you very much.

JANET ABRAMS: Thank you very much, Dr. Zon. Next Dr. Pedro Lecca, Dean, Texas Southern Department of Pharmacy.

DR. LECCA: As dean and professor, I really would give you commissioners an extra ten points on your final grade, being so patient and courteous. I really appreciate that very much. I am, as mentioned, Dr. Pedro J. Lecca, dean and professor at the Texas Southern University College of Pharmacy and Health Sciences. I will be brief. Thank you for the opportunity to provide input into this commission's work on critical infrastructure protection. As dean of the Texas Southern University College of Pharmacy and Health Sciences, my remarks under-

standably are directed toward the emergency services infrastructure. Specifically that they are focused on health and medical emergency preparedness. Most particularly, my comments focus on the role of pharmacy professionals, who function as an equal member of a health care team on a day-to-day basis and who would serve in an expanded capacity in an emergency situation.

It is recognized that the city of Houston, Harris County, has in place a comprehensive emergency management plan with an established infrastructure, including command center for its implementation.

I appreciate that the plan includes health and medical components of that state and federal support systems which would be used and stand ready. Further, it is understood that the local health and hospital segment has an emergency plan in which pharmacy, and particularly the doctors of pharmacy, the doctors of pharmacy as members of the health care team, are an integral component of that program and is emerging as the only entry-level degree in the field of pharmacy.

Preparation of the pharmacy goes beyond that which has been for pharmacists in the past. Encompasses pathophysiology, integration of concepts related to biotechnology, more comprehensive clinical experiences, and novel drug delivery, expanded preparation in pharmacotherapeutics, applied pharmacochromatics; chemotherapeutics has also significantly expanded their function in the health care arena. My friends, this translates into significant service, potential in a disastrous situation.

Currently in addition to the pharmacist membership in the health care team, they staff drug information centers. One such center is here, Ben Taub Hospital here in Houston, and serviced by pharmacy professionals who reasonable provide health care professionals, physicians, nurses, other pharmacists, community members with information to assist them in the provision of safe and efficacious use of drugs for both inpatient and outpatient information. It is engaged in drug use policy designed to ensure equally efficacious cost effective therapy. Quality assurance and adverse drug reaction, reporting and monitoring.

The center houses the microdecks drug information system consisting of drug decks, poison decks, and emerge decks. Further it has the capability to perform extensive online medical searches. It is anticipated that centers of this nature would be a vital link in many major emergency situations.

External to the hospital setting, the commuting pharmacists play a vital role in disasters. For example, the Georgia floods of 1994 pointed out that, one, disaster victims usually have no supplies of medications and often little knowledge of their drug therapy. Two, in the first 72 hours after a disaster, pharmaceutical problems must be handled at the local level and pharmacists are pressed into service around the clock. And finally, three, pharmaceutical stocks run low, and it becomes necessary to wait until wholesalers can resupply necessary drugs, which can take several days.

As a consequence of that experience, it was recognized that guidelines for emergency action were needed to access patient needs and help organize and distribute drugs. A national conference involving delegates from state pharmaceutical associations throughout the country were convened through a grant from the Georgia Pharmaceutical Foundation in September of 1995. Its purpose was to develop a plan that pharmacists in all states can come to response to a disaster situation. I urge this commission to obtain a copy of that plan for incorporation into its critical infrastructure.

And finally from a national perspective, it does not appear that pharmacy as a profession has defined a disaster preparedness plan nor is it a topic pursued in the colleges of pharmacy throughout the country. Perhaps it is because health disciplines in a significant degree function as members of teams that disasters have dealt with on a more local and regional rather than national level. Thank you very much.

JANET ABRAMS: Thank you. Our penultimate speaker is Mike Wisby, Texas Engineering Extension Service.

MR. WISBY: Good afternoon. On behalf of myself and our director, Dr. Kim Bennett, I appreciate the opportunity to be here with you today. I'd like to just give you a brief overview of what the Texas Engineering Extension Service is and what we do.

Basically our clients are the folks that have gotten up here today and talked to you. We basically are a one-stop shop in the state of Texas where local government can come and get training. We train their law enforcement officers, their fire fighters, the water and wastewater people, their utility folks, their communications people, all of those folks that it takes to run your local government, that's what we do. We've been doing this since 1930. I work in the fire protection training system, and at Texas A&M we have a world-renowned fire training facility. We're currently training students from all 50 states and 34 foreign countries. As I said, our clients are

the folks that got up here and talked to you today. The medical centers, petroleum industry, local governments, the county and city emergency management personnel, all of these folks. So what we're seeing in our business is we have new challenges.

In the fire service, we just used to fight fire. Now we're doing hazardous materials in every major city. The EMS and trauma systems are working at the maximum capacity they can. So these things are challenges that we must meet.

You heard the state talk about the interstate truck traffic and their concerns, coming from Mexico and what to do with hazardous materials on our highways. Oil spill is there on the coast, including our weather incidents such as hurricanes and things like this. So our roles are changing. We must change with it. How do we do that? Well, we coordinate. We coordinate with our cities, our counties, our state, and with FEMA, and there are certain things that you're aware of, or may not be aware of, that are going on between the Department of Defense, Department of Justice, with the Nunn Louver initiative, also with the President's policy on counterterrorism; there's a lot of things coming down that we want you to continue to support.

Here in Texas we have an urban search and rescue task force which is called Texas Task Force 1 that will mobilize and assist any local government within the state or out of the state as requested to deal with building collapse or rescue type situations such as what we had in Oklahoma City. In addition, there is ongoing efforts for technology handoff, where we hand off stuff from the military. And this is critical to us. There's a lot of military technology that are first responders in fire, EMS, and law enforcement need, and there's some national efforts going on through direct whip at FEMA and people like that, that we would like you to continue to support.

We heard talk about coordination. Training and simulation are critical, evaluation. We're leading an effort on computer simulation where we can train these emergency management folks in local governments in these areas. There needs to be continued support for that. We're handing off military war gaming type technology to local government so we can do this.

In short, we're here to support you. Anything we can do, I encourage you to please contact us, and I applaud you for sitting here today, and also the hard working staff and all of the things that you all have done. Thank you.

NANCY WONG: Mr. Wisby, just to show that we are still paying attention after a very long morning, your work at the center sounds very impressive to support local governments and

agencies in training. What relationship, if any, and what type of support do you provide private industry in these areas?

MR. WISBY: Well, the gentleman that was up here from the University of Houston earlier talked about the Texas City disaster. And all of the industrial clients up and down the Houston Ship Channel corridor, the Texas City industrial complex are clients of ours, and I'll tell you they are a model response system for an industrial emergency. If you watched the news this morning, they had an industrial tank farm fire in Corpus Christi, by the way, but they are a model for that, and they work together and coordinate, they share resources between all petrochemical and oil companies. In addition in the Gulf of Mexico, there are over 10,000 people every day that work in the gulf on rigs and platforms. These all share information. We help pull that together. Our job is to help coordinate and train those folks.

JANET ABRAMS: Thank you, Mr. Wisby. Our final speaker, who has been asked to limit his remarks to two minutes, please, is Swaroop Reddy of the University of North Texas. Thank you.

DR. REDDY: Good afternoon, and thank you for this opportunity. My passion is disasters. I teach disasters management at the University of North Texas. Ours is the only institution at the country that offers a four-year Bachelor's program in disaster management.

Basically I'll keep my comments short and brief. By accommodation I think we need more universities offering a degree program in disaster management. The number and frequency of disasters, near-catastrophe disasters, nine of the ten costliest disasters in U.S. history have taken place since 1989. I can repeat that. Nine of the ten worst disasters in U.S. history have taken place since 1989. And each costing more than one billion dollars. And disasters create complex environments, and disaster managers should be aware of the complexities.

And to protect a nation's critical infrastructure, the emphasis should be on education and training and disaster managers. The University of North Texas is an example. We've been in the field for the past ten years. We have over 350 graduates, and they've been absorbed by the federal government, state government, local government, and corporate sector. And there are other programs which are about to start in other parts of the country like Florida, California, Tennessee, Pennsylvania, and Arkansas, starting their own programs in the local universities. And FEMA, emergency management institute have been very proactive in developing the disaster management field. That would help contribute—start new programs in disaster management. And also we need certification of emergency managers, say for instance, National Coordinating

Center for Emergency Management. They've been very actively involved in certification for emergency managers.

Basically the bottom line is we need more schools offering a degree program in disaster management, and we need certification, increased professionalization of disaster management. We need to build a knowledge base in disasters. Thank you. Any questions?

JANET ABRAMS: Thank you very much. This concludes the public testimony today, and thanks go to all of you who have been here for this long period for your patience and for the specific and important contributions you've made to the work of the commission.

If anyone would like to submit comments to the commission or get in touch with us for future dialogue, please stop by the table on your way out for information on how to contact us, and I'd now like to invite Dr. Powers or any of the other commissioners to offer concluding remarks.

JOHN POWERS: The thing which is disappointing about a morning in which we have so many speakers is that we would have liked to have engaged each and every one of you with extensive comments. I have a whole set of questions I would like to have raised, all the way from health care to whether or not standards are viewed as adequate, and had I done so, Janet would have been after me, so that wasn't a good idea. We are tremendously appreciative of your thoughts, and we would very much like any follow on comments or e-mail that you might want to send us. Brenton and I and James Lee of the senior staff are at FEMA on Tuesday, and if you have some messages that you would like us to consider delivering, we would be most appreciative in receiving them. But in any case, your thoughts have been extremely thoughtful, and very well received, and again, we give you thanks to all of you who have made presentations, those of you who have sat here and to the city of Houston.

(Hearing concluded.)