

PRESIDENT'S COMMISSION ON
CRITICAL INFRASTRUCTURE PROTECTION



PUBLIC MEETING TRANSCRIPT

ST LOUIS, MISSOURI — JUNE 19, 1997

APPEARANCES

MAYOR CLARENCE HARMON

MEMBERS OF THE PRESIDENT'S COMMISSION:

ROBERT MARSH

Chairman

JANET ABRAMS

Moderator

MARY CULNAN

Commissioner

RICHARD CASE

Commissioner

PAUL RODGERS

Commissioner

DAVID KEYES

Commissioner

FRED STRUBLE

Commissioner

STEVAN MITCHELL

Commissioner

JOHN DAVIS

Commissioner

NANCY WONG

Commissioner

INDEX OF SPEAKERS

OPENING REMARKS BY JANET ABRAMS	1
WELCOME BY MAYOR HARMON	1
INTRODUCTION OF COMMISSION BY JANET ABRAMS	2
OVERVIEW OF THE COMMISSION BY CHAIRMAN MARSH	2
SPEAKERS	
Richard Poehling	5
Vincent Stehlin	9
Kenneth Jones	12
Tony Thompson	15
Neil Kurlander	19
Cecil Wright	23
Mike Cannon	27
Stephen O'Brien	29
James Ferrell	34
David Snider	35
Dan Walz	38
Phillip Gould	41
Charles Heisler	42
Tom Bratkowski	44
David States	47
LeRoy Fulmer	50

PROCEEDINGS

MS. ABRAMS: Good morning once again, and welcome to the President's Commission on Critical Infrastructure Protection. My name is Janet Abrams, and I am a White House liaison for the Commission, I will be moderating this morning's events. This is the fifth in a series of regional discussions being convened by the Commission. We've held meetings this year in Los Angeles, Atlanta, Houston and Boston, and this morning we're honored to be here in St. Louis. I'd like to begin by thanking our generous host for the event today, Mayor Clarence Harmon. Mayor Harmon, we thank you for your hospitality and for your active interest in the work of the Commission, and I'd now like to invite you to officially open today's proceedings.

MAYOR HARMON: Good morning, and thank you. On behalf of the City of St. Louis, I extend a warm welcome to today's meeting. St. Louis is proud to host this meeting, the outcome of which will promote infrastructure safety not only in our region, but throughout the country. The President's Commission on Critical Infrastructure Protection has held public meetings in four other cities. This meeting in St. Louis will complete the public hearing portion of the process being conducted by the Commission. The focus of today's meeting draws attention to the importance of our infrastructure.

Too often, we take for granted the comfort provided by our infrastructure—the quality drinking water, the efficient banking and finance systems, and the transportation systems. Our infrastructure is the skeleton that supports our region, and any strike to it would be very debilitating. Because our infrastructure plays such a vital role in our everyday lives, it is important that we secure it so that it will not fail us, or in the worst case, become a point of vulnerability. None of us likes to contemplate the possibility of our safety being threatened, however, evaluating our environment strengths and weaknesses is a necessary process to ensure we continue to lead peaceful lives. So I commend this Commission for their foresight, and I thank today's participants for being here to deliver testimony that will be used to secure a better living environment for all of us. The input and expertise of our community leaders will help shape the Commission's recommendation to President Clinton on national policy that will protect our critical infrastructures. With our participation in our process, we proudly serve our communities and our nation. Thank you.

MS. ABRAMS: Thank you very much, Mr. Mayor, and again, thanks go to you and your staff for supporting today's meeting. I'd now like to introduce the members of the Commission who are here with us today. By executive order signed by President Clinton last summer, this is a group made up of a mix of individuals, representing both private business and government. All members of the Commission bring experience and expertise in specific aspects of critical infrastructure.

First, Ms. Nancy Wong coming from Pacific Gas and Electric Company in San Francisco. Next to Nancy are Mr. John Davis, commissioner from the National Security Agency, Mr. Stevan Mitchell of the Department of Justice, Dr. Fred Struble, who brings to the Commission some 30 years of experience in the Federal Reserve System, and Mr. David Keyes, commissioner from the Federal Bureau of Investigation. Next to the Mayor is our chairman, Mr. Tom Marsh, who comes to the Commission from the aerospace industry where he has served as chairman of the Thiokol Corporation and as a director of numerous boards of directors. He is a retired four star Air Force general. And then Mr. Paul Rodgers, who's former executive director of the National Association of Regulatory Utility Commissioners. Next, Mr. Richard Case, who comes to the Commission with over 40 years of experience with IBM Corporation, and then finally, Professor Mary Culnan of the Georgetown University School of Business. I'd now like to invite Chairman Marsh to give you a brief overview of the work of the President's Commission on Critical Infrastructure Protection.

MR. MARSH: Well, good morning all, and thank you very much, Mayor Harmon. It's a pleasure to be here in St. Louis this morning. As you heard, my name is Tom Marsh and I'm the chairman of the Commission. Our purpose here today is to build public awareness about America's life support systems, its critical infrastructures, and to hear your views on what we should or should not do to protect these vital systems.

The Commission was created last July the 15th when President Clinton signed an executive order that begins with this sentence: "Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States." The central purpose of the Commission is to recommend to the President a national policy and an implementation strategy for protecting the nation's critical infrastructures, and assuring their continued operation.

So what are the critical infrastructures that we're looking at? They fall into five basic groups. First, our systems we call vital human services. These include water supply systems, fire, police, medical and rescue services, and federal, state and local government services that protect our freedom and help 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 the destruction there would be severe. Another group is the energy infrastructure, which includes the production, distribution and storage of electrical power, natural gas and petroleum. These are critical systems that provide light, heat and cooling, make us the most mobile people on the planet, and fuel the American industrial machine.

The newest and fastest growing infrastructure segment involves the electronic distribution of information. America has pioneered tremendous advances in communications and information technology and reaped extraordinary benefits, but our reliance on these systems exposes infrastructures in new ways and creates new vulnerabilities. And the final infrastructure category is what we call physical distribution. This group includes all the means by which we transport and deliver our products and services. And what exactly makes these infrastructures critical? As I mentioned earlier, their loss or incapacitation would have a debilitating impact on the defense or economic security of the United States.

A question I'm 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. Many companies, such as utilities, are very familiar with natural hazards. Those of you living here in St. Louis are very familiar with such hazards, including floods and tornadoes. Now this Commission will obviously not stop acts of God. Our intent, however, is to stop certain acts of man. That's because today we're confronted with an entirely new set of hazards that are man made. Technology has created an interconnective world, but each connection creates new exposures and risks. Companies are becoming increasingly vulnerable to theft, unscrupulous competitors, malicious hackers, insider cyber attacks and out and out 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 seem able to master. 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, and recommend to the President a national policy and an

implementation strategy for protecting the critical infrastructures, and in the process to propose any necessary statutory or regulatory changes.

I want to emphasize that cooperation and collaboration between the public and private sectors are absolutely essential to our success. We are vitally interested in what the private sector has to say, because it owns and operates most of the critical infrastructures. Furthermore, government relies on the private sector infrastructures for services required for national defense and well-being. Together, the public and private sectors can develop common solutions to common problems and secure America's future. But, we need everyone's help. We need your ideas, and we need your participation. We need everyone's best thinking up front. So I encourage and welcome your input, we mean that sincerely. That's why we're here today, to listen. That's the only way that we'll find solutions that work for everyone. So again, we appreciate your being here today, we appreciate Mayor Harmon taking time to be here, and we look forward to hearing what you have to say.

Now furthermore, should you wish to talk to us at any time after this morning, please write or visit us on the World Wide Web at the address shown on the screen, <<http://www.pccip.gov/>>, and I thank you very much, and we'll move ahead.

MS. ABRAMS: Thank you, Chairman Marsh. Before we move on to public testimony, I need to offer a little note about time. We have a very full program this morning, we've gotten terrific response from the St. Louis region for this morning's events, and my job is to encourage us all to keep to the schedule and to give everyone who has come and signed up a chance to speak. Each presenter has been asked to limit his or her remarks to ten minutes this morning, and I'll be looking carefully at my watch, and when you hit the nine minute mark, you will see this subtle sign, and it's my hope this one minute notice will encourage you to wrap up and complete by the ten minute dead line.

Please know that any testimony you'd like to submit in writing will be included in its entirety in the official record of the hearing, and as Chairman Marsh just mentioned, we encourage dialogue with you, between you and members of the Commission beyond this morning, and you can contact us at this address and over the World Wide Web. Let me also add that anyone who's planning to speak this morning needs to have filled out a blue card. Some of you may have come in by chance and not filled out this card, but I need to have this card so that I can call you. As I introduce each presenter, I will also call the name of the individual who will follow that presenter.

We're ready to begin and I'd like to invite our first speaker, Mr. Richard Poehling, Assistant United States Attorney, following Mr. Poehling we'll have Vincent Stehlin, Sergeant, St. Louis Police Department.

MR. RICHARD POEHLING: Good morning, ladies and gentlemen of the Commission, my name is Dick Poehling, as I was introduced, I am an Assistant United States Attorney for the Eastern District of Missouri, and I appear before you today as a representative of that office to share some thoughts with you with respect to the topic that you're concerned with, how it impacts on the operation of our office.

I graduated from St. Louis University Law School more than a few years ago, the actual year is unimportant, except I take some comfort in the fact that the Missouri law of statute of limitations has run on those time periods, but I have a very vivid recollection in my law school years, during my freshman year I took what was a required course called Legal Research and Writing, and as a result of that course, during the course of the operation, of course, there was topics given for law students to research, but the topic was given to many law students, and there was a treasure that ensued trying to find the law book to read it so that you could probably complete your assignment, and if you were lucky, you got the law book early, if you were unlucky, you had to go to other libraries trying to track it down.

That course is still taught today in the law school, but the face of that course is dramatically changed with the advent of computer technology. Now the law students have the law books available to them on the computers. Innumerable amounts of students can simultaneously access the material they require, and they don't even have to be at the law school to do it. They can be at other locations, such as their residence. This is just one example of how it impacts on the daily operations of the lawyers now that we are being sometimes dragged kicking and screaming into the 20th century and forced to become computer literate.

With the advent of technology in the areas of computers, although we've also had some difficulties, we have paid the price that comes along with that, and one of the prices we have paid is we have become dramatically dependent on the use of computers, and in doing so, we have increased our vulnerability for our day to day lives with respect to the area of computer operations. Several years ago a colleague of mine was in a private civil law firm which was on the cutting edge of computerization, and they were highly automated in their office, and one day the inevitable happened, and the system crashed, and there was a flurry of concern obviously,

they begin to appreciate the civil lawyer not being able to type a lawsuit out of something like that, you can gauge the magnitude of their concern, and they discovered that in becoming computerized, they had discarded all of their previous equipment, such as electric typewriters, they had none in the office. Well, at the end of that day, they immediately went out and bought some electric typewriters. They realized how dependent they had become and how vulnerable they had become on a day-to-day basis with the use of computers.

In addition to the general public using the computers to increase their skills, unfortunately we have seen criminals also turn their activities to the use of computers. The United States Attorney's office has gone through a learning curve I guess, so to speak, with respect to computer crimes. Initially we entered into the area of criminal prosecutions through computers in the area of child pornography where the computer was being used as a means of transmission. We have adopted a zero tolerance policy, which means we do every single case in the area of child pornography, and that policy remains in place today.

Then we saw a difference in some of the referrals that we were receiving from the FBI, we began to get referrals from the hackers, as they are known, people who illegally enter computer systems basically for a nonprofit motive, either just for the thrill of being able to say they did it and did it successfully, or perhaps disgruntled employees who are not seeking any economic return, but are seeking to wreak havoc on their employer for some grievance that they feel they have suffered as a result of the employer's action, and the actions that they may take to get retribution might be the injection of a virus, perhaps trying to and successfully crashing the entire system.

So we began to see those cases. Now we have progressed beyond that, and now we are seeing people using computers for profit. We are seeing computers being used in the area of criminal frauds where individuals are utilizing it as a tool, and it goes across the board in terms of economic crimes, we see drug dealers using computers to launder money, things like that. So that is the learning curve, so to speak, that we have seen in the United States Attorney's office with respect to computer crimes.

Perhaps the strongest point I could submit to you today is computer crime from our experience is definitely on the rise. It is not decreasing at all. All of the areas I have mentioned, the child pornography, the hackers, the fraud area, we continue to get record number of referrals from the investigative agencies, which is primarily the FBI, in terms of using computers to

commit these crimes. So our work load continues. When we receive those referrals, our office is placed basically in a reactive mode. We are entering these cases after the crime has been completed. As a result, we face generally a faceless perpetrator, all we can figure out probably is a keyboard somewhere was used. Often it's an unknown location, because as you're aware, when you sign on you're coming from St. Louis, that doesn't necessarily mean you're coming from St. Louis, there are multi-district situations in which the computer trafficking has been routed from various parts of the country or perhaps even overseas to ultimately reach their destination to commit their crime, and our historically means of investigative techniques do not work, we don't have eye witnesses, we can't conduct lineups, we don't have fingerprint evidence in these kind of cases. In the very sophisticated cases it's extremely difficult even to locate and identify an electronic trail. A paper trail, of course, is not there; sometimes if we're lucky we have an electronic trail. But it greatly increases the difficulty of being able to successfully investigate and prosecute these cases.

In order to mitigate the scope of the problem, it is essential that we develop a period of intense cooperation between the governmental agencies, law enforce community, and the potential victims of these crimes, whether they be private industry, educational institutions, government entities. Nowhere is this necessity for cooperation probably more critical than the area of your focus, which is our country's critical infrastructure. We need to encourage victims to come forward early if they even think that there's a possibility that their systems have been compromised, and certainly for sure if they know the system has been compromised. We need to know as a law enforcement community when they smell the smoke, and not have them call us after the building has burned down. We can be much more effective in our reaction if we get into the case early before the people that are responsible have had time to cover their tracks additionally. Delay is a factor that really hurts our ability to successfully prosecute. I indicated that our cases come to us in a reactive mode and the difficulties that go with that, we need to realign and get involved in a proactive mode, and this can be done by sharing information among computer system operators, as well as protections that will allow them to safeguard their systems so that we can hopefully decrease the number of referrals that we are receiving. We need to advance educational initiative to—such as the Commission is doing here today—to educate the public to the scope and the nature of the problem. We spend a considerable amount of time in our country educating people

with respect to the drug situation and the DARE program. Perhaps we ought to consider a CARE program for computer abuse.

The earlier we can get to the citizens in our country, the better off we are. We have computers now that are literally in preschools and children are taught to use these, and those computer skills will hopefully be enhanced for lawful purposes for the rest of their life, but it's important that we understand, that we get them to understand that it is, there is improper conduct that can also be abused with computers and to establish a sense of values in those young citizens that this is not proper conduct, and hopefully we might deter some people from crossing over the line later on in their lives.

We are fortunate in my district here to have a highly skilled Assistant United States Attorney and skilled FBI agents that are assigned to investigate these cases. Additionally, we are blessed with a very good spirit of cooperation among various people in the private industry, an example comes to mind of Southwestern Bell on a recent case. They were extremely cooperative with us; the expertise they provided was a significant factor in allowing us to successfully prosecute the case in which they were assisting us.

Finally, I would suggest we must maintain constant vigilance for this problem. The potential abuse for computers is limited only by one's imagination, as we are seeing new developments and new schemes coming forward every day. The work of the Commission increasing public awareness of this problem is an invaluable contribution to letting the general public know the threat that we are facing as a country. As history has often shown us, a recognition of a problem, from that recognition springs hope that a solution will follow. I thank you very much.

MR. KEYES: Mr. Poehling, a question that I would intend to ask Sergeant Stehlin, as well: What is your sense of the federal government's role in providing specialized training in computer crimes? How might that process be working in your federal district, and what areas of assistance do you believe state and local law enforcement officers could best receive either through your office or through some other federal training entity? In fifteen seconds or less.

MR. POEHLING: Okay, there is not to my knowledge a permanent working group in existence that addresses that problem. We have on a case by case basis provided educational information to various individuals with respect to responding to a particular problem that they have faced. Obviously if we have an investigation under progress where we realize—be it in a critical

infrastructure or anybody—that their system is going to be attacked or anything, we certainly share that information with them and try to educate them so that it doesn't occur.

I think the state officers could benefit from that effort, however, I think that generally our experience has been that the computer system does not limit itself to a particular geographical area, which the state officers are usually confined to. I think it predominantly remains a federal problem that we have to address, but in no way does that take away from the fact that we need the cooperation of the local law enforcement officers. In the vast majority of our cases that we prosecute that we call federal, it's the local law enforcement officers that provide significant assistance to us and enable us to have a successful result.

MS. ABRAMS: Thank you very much. Next I'd like to introduce Sergeant Vincent Stehlin, sergeant with the St. Louis Police Department. Following Sergeant Stehlin we'll be calling Mr. Kenneth Jones.

SERGEANT STEHLIN: Commissioner, members of the Commission and Mayor Harmon, I want to thank you for giving me this opportunity to talk with you. Each one of the infrastructures mentioned on your portfolio you sent out are very important to the law enforcement community, however, I'd rather use your Web site to do all my opinions, I would like to address three of them quickly. One is the telecommunications infrastructure, the second one is continuity of government, and the third one is the emergency services.

I have a little unusual job in law enforcement, because I spend the bulk of my time working in the emergency management field as a coordinator for local, state and federal agencies. In looking at the telecommunications infrastructure on a local level and law enforcement, the 911 system, and the communications systems are very important to us. Are we prepared for everything that could occur in a natural technological type of incident or a terrorist activity? And the answer is no. I don't know many agencies that could speak here that could say that they are totally prepared for any such incident. However, we are looking at and doing some progress in that particular field with the security and the integrity of the 911 system. We have a long way to go. Cellular communications, one of the things we find out is that there is a federal regulation on intercepting information off the cell phones, but in our opinion, it's almost unenforceable, because anybody can go to Radio Shack and buy a scanner and listen to every call that's coming out. We would like to see something done on that. That was, there was problems down at the

Oklahoma Murrah bombing, World Trade Center bombing, and in the floods of '93 where everybody was able to intercept your conversations on cellular phones.

Telephone Service Priority systems that went out, we had meetings on them, the people that we deal with on that particular topic, it sounded like a very good system, but it was economically unreal for local agencies to participate in that particular program, the individuals we deal with. Telephone Service Priority is a very valuable asset, however, it's a little bit out of our reach for what we would need in 911.

The Emergency Alert System that went into effect in January of 1997 is a very viable system, we're still working on getting in that, but we have to meet with other people to ensure that everything is carried out the way it's directed. The entire telecommunications industry is the backbone of a lot of law enforcement activities. We're down at the bottom of the food chain here, so when something occurs, a lot of people, probably the bulk of the individuals that are victims, they don't call the FBI, and they don't call DEA, and they don't call FEMA, they call the local police agencies, so our 911 systems are probably very vulnerable, but we're trying to do the best job that we can on local levels, and I think that goes for local law enforcement agencies across the country.

Continuity of government, it's very important that we go down three and four deep in each one of our organizations and have leadership in those particular roles. We find out that a lot of times we have some strong individuals at the top, but we're not doing enough work to ensure the stabilization of the community in our government system with the continuity of government going down into the branches and cross training some of our personnel.

Lastly, Emergency Services, I feel very strongly about this topic. We do a lot of work here in the city of St. Louis and with the St. Louis Emergency Management Agency, the State Emergency Management Agency, FEMA, that we through the St. Louis Police Department spearhead. We probably train the bulk of disaster type training in the state of Missouri through our agency here; in fact, we're just finishing up one today. We average about 650 people that go through the programs. One of the problems that I see, and I have talked with people with FEMA and different federal agencies, is that we do a lot of training in disaster operations that handle terrorist activities, natural disasters, et cetera. We do a lot of training of local agencies, we do a lot of training state agencies, and the involvement of the two is excellent. We work a lot with the Federal Emergency Management Agency and James Lee Witt and John McKay with Emergency Management

Institute, they do a fantastic job, but what we perceive as a problem, and it came up in the Murrah bombing, it came up in the World Trade Center bombing, and it came up in a lot of terrorist type activities, is the merging of federal agencies with state and local agencies. We do a lot of training and there's nothing more that we would like would be to involve federal agencies in part of the training. When we go in, and I'm not asking for instructors, even, because each federal agency that we've ever dealt with have always accommodated us very good in providing instructors, but the instructors are not going to be the people who are going to be out at the scene of a terrorist attack or in a national disaster type situation involving the infrastructures that we're talking about. We would like to see a more blending of federal agencies and state and local in different types of incident management programs so that we're all on the same sheet of music. Right now we have different, we're talking about the same music, but we've put different titles on the top of it, and we have to make it so that when an incident occurs, whether it's on a local, state or a federal level, we are, the players are on the same sheet of music, we understand it, and we feel comfortable working with the individuals that we're going to deal with. So with that, that was a law enforcement perspective that I wanted to get across to you. We have some additional information for you on the Web, thank you very much.

MR. RODGERS: I have a question.

MR. STEHLIN: Yes, sir.

MR. RODGERS: Sir, on this training, you have this intensive training which, of course, is very important. Does that include training to respond to biological, chemical and radiological incidents, or have you gotten into that?

MR. STEHLIN: The training on biological and chemical incidents, we do training required by OSHA 1910.120 in regards to response to hazardous materials. To be quite frank with you, we need a lot more training. We've identified the key agencies who respond to that. When we get into the avenue of biological type incidents, I think we're still out in the forest trying to flounder our way through. We need a lot of training on that type of deal. Could we handle the response to a gas incident on a local level? I hope it never happens, but I think we would be in some problems. We do not have a lot of training in biological training.

MR. RODGERS: Thank you, sir.

MR. KEYES: Have you received or do you see a need to receive any specialized training in the area of computer intrusion or abuse?

MR. STEHLIN: Yes, sir, we do. A lot of that would go to, start on a local level, as the U.S. Attorney representative said. A lot of it is developed by police officers on a local level and goes up.

MR. KEYES: So you have received training or you would be in need of training?

MR. STEHLIN: Some of our officers have received training, and there is a need for that type of training, yes.

MR. KEYES: And is there a federal role in providing that training.

MR. STEHLIN: On a lot of it we look to the federal role for training and direction in specialized courses, such as that.

MR. KEYES: One last question. You did not mention anything about the availability of radio spectrum. Has that proved to be a problem for you in any way.

MR. STEHLIN: I'm not really an expert on that particular topic, I think another law enforcement representative is going to discuss that with you, sir.

MR. KEYES: Thank you.

MR. STEHLIN: Thank you.

MS. ABRAMS: Thank you very much, Mr. Stehlin. I'd like now to introduce Mr. Kenneth Jones of the St. Louis Board of Aldermen representing the 22nd board, and following Mr. Jones we'll be calling Tony Thompson. Thank you, Mr. Jones.

MR. JONES: Good morning, I would also extend my gratitude to you for coming to our city and sharing concerns regarding the question of infrastructure. I'm Kenneth Jones, I've served on the St. Louis City Board of Aldermen for 14 years, and I'm a construction worker. I was an iron worker for 20 years, and upon realizing that wire is lighter than steel, I transferred to be an electrical worker, because it's easier on my body. I've also spent much of my life participating in the peace movement. I recall in the '70s and '80s there was a hysteria throughout the world, because people were afraid that they might die in a nuclear holocaust, and so I saw the connection between peace and the needs of our nation, and for that reason I participated in the peace movement, and now we are no longer confronted with a nuclear holocaust thanks to the many people who participated in that movement. I recall that a period, 80 percent of the American people were supportive of peace, and those of us who participated in the peace movement believed that our nation's resources could be better spent addressing the infrastructure problems that we have. I remember at one point former mayor, the late Harold Washington said that the nation's cities

appear to be swallowed up in the ground, discussing how, like in our city, for instance, our sewers are wood. The major sewers, the main sewer systems, are made out of wood, they're just that old, and we have so many cave ins and other problems of that nature.

And I think the federalist approach that some have used shifting the burden to the states and cities won't work, because we just don't have the resources, and what has happened as a result, you find the people in the inner cities, you find hysteria and the people in the inner cities turning on one another and blaming each other for problems that are really created by nature. I think man's greatest struggle is the struggle to, with nature, the things that are caused by nature, the depreciation of buildings, these are all natural things that we are confronted with and that we must find solutions for.

And before the Congress today, we have the Martinez bill. The Martinez bill is HR 950, and you had the same legislation before the Congress last year. There are many of us throughout the country who believe that this would be a good first step in trying to address our nation's infrastructure problems. Last year the St. Louis City Board of Aldermen passed a resolution in support of the Martinez bill that we not have a resolution in the rules and resolutions committee support that bill. I'm proud to say that my congressman, Bill Clay of the first Congressional district in the state of Missouri is a co-sponsor of that bill. I would hope that you would urge President Clinton to give leadership to the government in support of passage of the Martinez bill. I just want to read this resolution that we have before the Board of Aldermen, share it with you, and entertain any of the interrogatories that you may have. But I never answer any questions unless I'm asked by a lawyer, thank you.

On the 15th of March, 1996, the St. Louis Board of Aldermen passed Resolution 256, which strongly supported HR 1591, the Martinez Job Creation and Restructure Restoration Act. Congressman Martinez's bill has been reintroduced during the 105th Congress as HR 950. Congress has found that the investments made during the '30s, '40s and '50s in the infrastructure of the United States through the Roosevelt Public Works Program, the National Highway Act under President Eisenhower, and other major efforts, led to the greatest spirit of economic recovery and sustained level of economic growth in the first 150 years of our nation's existence.

The nation's infrastructure has suffered greatly over the past three decades, because of the failure of the federal government to ensure renewal and restoration of roads, bridges, public buildings, public lands, and other public assets. Employment has reached the level of a major

national crisis with 20 million workers unemployed or under-employed, 20 million children living in poverty, and one out of five new jobs below the poverty level. Without decent jobs and the opportunity to live productive lives, young people are pushed into drugs and crime. Much of the infrastructure of St. Louis is in dire need of repair and expansion, and estimates reported by contour St. Louis show that at least 18 billion dollars could be possibly spent on improving the infrastructure of the St. Louis area highways and bridges, mass transit, waterways, water supply, waste water and storm water. The lack of resources for the maintenance of the infrastructure during this period has led to the loss of both jobs and job skills in these vital areas, with consequently increased unemployment and a reduction in the quality of life for residents of affected areas.

Policies at the federal level have demonstrated diminished concern for the infrastructure needs of the communities of the nation and a shifting of the burden for maintenance and creation of highways, bridges, mass transit, and the other infrastructures onto local government. In addition to the burden for local needs, such as public safety, education, health and public welfare, that those jurisdictions bear their by stretching already shrinking resources beyond capabilities of those governments to address these needs. The creation of living wage jobs in conjunction with a large and sustained public works infrastructure renewal program will reap significant rewards in direct tax payments at all levels of government, increased economic expansion for the country, and substantial reductions in the outlays for unemployment support, welfare, Medicaid and other government expenses. It will also lessen the burden on government expenditures, the result of lack of employment for those at risk of entering a life of crime.

So we're calling on the Congress, as well as the President, to get behind the Martinez bill, we think that just is the best direction. I would also like to add from the perspective of a construction worker, just as the human infrastructure deteriorates with time, so do our physical infrastructures, but species *Homo sapiens* being more advanced than the others, recognize that there are certain steps that we can take to prevent a deterioration. So we have been victim makers for our bodies, and I think people are recognizing that this preventive maintenance, catching it from the front end, especially with serious illnesses and diseases, if we put more resources on the front end, we will have to utilize less resources at the back end with acute care. The same holds true for buildings. If you paint steel, you prevent it from rusting. If you put a roof on a building, you prevent the rain from deteriorating the entire building, okay? With our city hall here, if there

would have been more preventive maintenance, the Mayor wouldn't be in the position he's in now trying to raise money to repair the building. So that's what we've got to do also, to commit more money for preventive maintenance for infrastructure, and I thank you all for taking a very good step forward. Thank you.

MS. ABRAMS: Thank you very much, Mr. Jones. I'd now like to introduce Mr. Tony Thompson, manager of Safety Technology for the Monsanto Corporation. Following Mr. Thompson, we'll be hearing from Neil Kurlander.

MR. THOMPSON: I can certainly agree that maintenance is an important aspect in the society today. Mr. Mayor and Commissioners, good morning, my name is Tony Thompson, and I work for a local firm here, as introduced, with the Monsanto Company. The issue I would like to discuss this morning is perhaps a little bit different from some of the others that we've heard, but I think it invokes very, very strong feelings on my part, and hopefully it will on yours. Very briefly it involves Internet communication of something called a "worst-case scenario" for locations of very toxic and very flammable chemicals. Let me begin very quickly of a history of how we got where we are today and the position we find ourselves in.

First there was passage of the Clean Air Act amendments of 1990. Within these amendments, Section 112(r) directs the EPA to develop a Risk Management Program or RMP regulation. It also requires that RMP information be made available to the public. One year ago the EPA carried out its responsibility and promulgated the RMP regulation. It requires the users of 77 toxic and 63 flammable chemicals develop a Risk Management Program and communicate that information prior to June 21st, 1999, almost two years from today. Further regulations of these plans are required for sites of processes using more than a threshold quantities of these 140 regulated chemicals, the plan will have a number of parts, including a prevention program that would summarize how the site manages the risks that are involved in handling those materials, summarize the emergency response plan, a five year accident history, which is the actual releases that have occurred at that site over the past five years, and perhaps most importantly, a hazard assessment which summarizes the potential off-site consequences of a chemical release, including an event called a worst case scenario. Completed RMP will be registered with the EPA administrator, be submitted to the Local Emergency Planning Commission, the LEPC, and also, as stated in the Clean Air Act, be made available to the public.

This is kind of where we are today. The regulatory details have been developed, chemical lists defined, and the recipients of the information have been identified. Some points in the way of background. Many companies in the United States, including Monsanto, utilize significant quantities of toxic and flammable chemicals. The EPA estimates that over 60,000 locations will file risk management plans. In most cases these materials are stored in large vessels, single tank, which receives significant attention to ensure that their contents are not released into the environment, and at Monsanto these are very, very important vessels.

Under the worst case definition contained in the RMP regulation, the effects of releasing these large quantities of material in a ten minute period, a very brief period is simulated using a computer model, we've been using computer models for a number of years to predict the impact that a chemical release could have on the surrounding community, this is a very sure science. And in many of the worst case scenarios these models predict a toxic cloud which would extend a distance of 25 miles or more from the point of release. Anyone within that cloud would either be killed or would suffer very, very serious health effects for the long term.

My concern. Currently the EPA is evaluating mechanisms to communicate RMP information to the public, as required in the Clean Air Act amendments. With the growth of the Internet, it's logical, you can use it as a tool to do this. It's inexpensive, it's relatively simple, at least my sixteen-year-old son at home and it's used by a rapidly growing population of people within the United States. Working with a number of people, the EPA has defined a proposed RMP Internet data base that includes a number of data elements which each regulated chemical user would submit to a central data base. And for a majority of the RMP information, I sincerely believe it would be an useful tool in how Monsanto and other companies manage both risks. However, information would also be submitted which pertains to the worst case scenario events. The current proposed data elements include name and location of the company, longitude and latitude, the chemical used, the quantity stored, and the worst case scenario release rate, and again, remember, it's the total quantity divided by ten minutes, the distance to a chemical specific concentration end point of a simulated release as defined in the regulation, the residential population within that distance, and the public and environmental receptors impact, including schools, hospitals, parks and other buildings.

This information used improperly in an act of sabotage would have catastrophic consequences for the people surrounding the location. The Internet data base could be used, for

instance, to list all chemical inventories which would impact the Gateway Arch, Busch Stadium, or for that matter, the White House. Individuals wishing to express their personal grievances with an act of destruction would have a road map showing them which is the worst of the worst case scenarios. I personally have great concerns with placing this type of information on the Internet. I believe it will increase the probability of an act of sabotage, marking the spot for a local audience 24 hours a day of a disaster which could result in the deaths of thousands of people just does not seem to make sense to me today in these times.

I would like to conclude by requesting the Commission to investigate this issue, to join in the discussion with EPA and others. I continue to maintain my opinion that worst case scenario details must be withheld from the community Internet data base. While the probability of improper use of information like this may be low, the consequences are of such devastating proportions that widespread Internet dissemination of worst case scenario data must not be done. In my opinion as a single voice, and there are many others who see positive signs, the signs of public disclosure of all of this data, and their conclusion is different than mine.

I should also add in conclusion that I believe the EPA has done an excellent job in developing this regulation. They have been willing participants seeking input from anyone who wanted to talk to them about it. While it may seem I'm being critical of their work on this issue, nothing could be further from the truth. They're working very hard to make this the best regulation they can for the United States and for all of the people that are involved. So I would like to thank the Commission for your time this morning, and again, I very sincerely urge your involvement in this matter.

MR. RODGERS: Mr. Thompson, the Commission is very much aware of this EPA proceeding, and we certainly are watching closely, but we appreciate you bringing it to our attention.

MR. THOMPSON: Thank you.

MR. KEYES: If I understand correctly, sir, you do not object to the concept of coordinating the emergency response plans with the appropriate local and state officials.

MR. THOMPSON: No, we've been doing that for a number of years. If we did not go by the Internet, I could see positive benefits.

MR. KEYES: And so the problem would be, for example, someone with malevolent intent using a computer in Bangor, Maine, or Baghdad, Iraq, seeking out the specific information that would allow them to target a facility with the full knowledge of which facility to target.

MR. THOMPSON: *(Nods affirmatively.)*

MR. KEYES: With the full knowledge of the emergency response plan being able to put in place countermeasures to interdict emergency responders or perhaps, as is the case with the IRA in the United Kingdom, attack the emergency responders, and thereby compound the extent of the problem. Have I properly understood your presentation?

MR. THOMPSON: Yes. See, one of the things Monsanto believes and that we believe in being open, we like to tell people how we run our plant, so we will share as much information as we can. We do that with local citizens who have the risk of living in the cloud, if you will. My concern is once it goes outside the local community, you're opening up a different kind of risk, I believe. I think Internet access can be used very successfully and has been used very successfully to share best practices, communicate how things are done in other parts of the country, and it's very, very positive, and I will encourage and have encouraged the EPA to continue on doing those kind of things.

MR. KEYES: Well, do you have a mechanism in mind whereby the company would coordinate with city emergency managers and local community managers?

MR. THOMPSON: We're doing that already as far as the LEPC.

MR. KEYES: But not provide that to a larger audience, is there a model in mind that works to current standards of privacy and disclosure and so forth? Do you have a different model in mind than the EPA standard? Can you suggest to us an alternative?

MR. THOMPSON: Well, there have been a number of proposals that have been suggested, all of them as a way of communicating with the public are inferior to the Internet for a number of reasons. Speaking for Monsanto, I believe we would have very little problem with hard copy information communicated to the local people that are in that area. Certainly this is going to be an event that's going to receive considerable media attention, when all of these RMPs from the 60,000 locations are filed across the country. This will be an event that will draw considerable attention to the chemistry and the risks that we have to our citizens. So we will be open. We have invited people into our plant, saying "Come, let us show you what we're doing, talk to our people that are running this place," and I think we've tried to do that, and that is the model that is in place today. I guess what I'm saying is that's the model that needs to be in place for the future I think, because it's the only one that really works. Those are the people that have the risks, those are the people that need to understand them. The people in Washington D.C. really, the citizens,

do not need to understand the risks of a plant in St. Louis, so that would be the model that we would, that we would propose, let's make this a local issue, let's keep the communication local, and for God's sake, let's keep this off the Internet.

MR. KEYES: Thank you.

MS. ABRAMS: Thank you very much, Mr. Thompson. I'd now like to introduce Neil Kurlander, chief of police of the Maryland Heights police department, and following Mr. Kurlander we'll have Cecil Wright testifying. Thank you.

MR. KURLANDER: Good morning, Commissioners, Mayor Harmon. As I listened to our previous speakers, it occurs to me the overlap of some of our testimony, and that should be expected, and that's really a positive sign, because each of us need to coordinate our responses to these threats to our infrastructure, and so as our previous speaker talks about release of information that may cause a terrorist act that would have a spread of biological material or chemical materials that would be threatening to our population, those of us in emergency service again look at how would we evacuate large communities if we had such a release. We have the computer models to forecast where that spread would go. We have computer models that would tie into our highway systems, that would tell us peak usage of our highways at the times of those releases, and is it safe to use a certain highway, how much load can that highway have. Some of my comments will overlap the U.S. Attorney's comments and Sergeant Stehlin's, because we all work together closely in these issues, and so my perspective will be a little bit different from the U.S. Attorney, I'll talk about the local perspective as opposed to the federal perspective, and some other issues in communication.

I have three specific areas affecting law enforcement. The first of them is communication between public safety agencies. I'm the chairman of the Code 1000, which is a committee of a regional board of law enforcement. It's a coordinating board for the St. Louis region that deals with a variety of issues, emergency services being one of them, and I chair the committee on emergency services. In that capacity, I'm responsible for the plan for St. Louis County for police response for disasters and emergencies, also the training of all police officers in St. Louis County. The population of St. Louis County is just under one million people. We are 91 municipalities and 65 police agencies that provide services to these citizens. It is our experience that at scenes of large scale disasters, communications between law enforcement agencies, fire and emergency

medical services and private sector responders is frequently a barrier to effectively coordinating operations.

Let me give you an example of such a situation. Last November a tanker truck carrying 8,500 gallons of gasoline overturned on an exit ramp at I-64 and I-170 in St. Louis County. (It's interesting as an aside that there's a tanker truck that overturned very near that location today, so if you're traveling I-64 east on the inner belt, you probably ran into that this morning.) In this particular incident I'm speaking about last November, the truck was trying to make a turn on the ramp, its balance shifted and it overturned. Eventually the tanker ruptured, the gasoline flowed into the sewer system under the highway and in through a nearby residential neighborhood. The tanker exploded and ignited the gasoline in the sewer system. Seven police agencies and 25 fire services agencies responded to the scene. The neighborhood was evacuated, the highways closed for several hours, as you would expect, gas company employees responded to cut off the gas to the residential neighborhood and commercial base in the area. The Missouri State Highway Patrol responded because the accident occurred on the highway, but the state troopers were not able to communicate with the municipal officers on the primary radio frequency that we deal with emergencies in St. Louis County. This is because their radio had a different frequency and could not operate on the frequency that we all used. The fire department was interrupted by the gas company's walkie-talkie transmissions, so fire service couldn't communicate when the gas company was communicating. What occurred is a classic case of interoperability of the public safety communication system. Basically what happens is the multiple agencies must work together during times of disaster emergency, they cannot in many cases talk to each other because they have a variety of radio frequencies, and those have been assigned to them by the federal government over the years.

As a backup, many agencies have attempted to communicate via cellular telephones, and we heard some testimony this morning about the security of the cellular telephones, that they can be penetrated, and that's not the emphasis I want to make, but is certainly a concern. Our experience has shown that whenever we have a significant incident that the public is aware of, we can't use the cellular system because the system becomes flooded, and we just can't speak on the system. We can't get a line, and when we do get a line, even when we're on radio frequencies, the same radio frequency, the agencies involved working in an emergency, what we find out is because they're so limited in terms of frequency, it can congest that airway, and we can't speak. If you

could imagine carrying on a conversation on one telephone line with five people at the same time. Now multiply that to 20 people or 30 people, and you can see the difficulty we have. We're just congested, we don't have enough frequencies.

And this situation is not unique to St. Louis—we see it all over the country with every emergency. Any exercise you go to, any training in this country you go to, the first thing they say in any disaster emergency, the first failure is communication. The communication system will not support the response. Currently, as you are aware I'm sure, Congress is considering legislation that would set aside 24 megahertz of radio spectrum for the use of public safety. A spectrum is a band of frequencies. We need those frequencies for public safety for the obvious reasons I just spoke to you. Without them, we have very little ability to effectively communicate at times of disaster.

The second issue—very briefly—is the lack of a comprehensive national program designed to prevent disruption and destruction of vital services by terrorist acts. Those of us who are involved in emergency management are aware of the threats posed to our community's vital services by terrorist acts. The nation must take seriously the potential for mass destruction and loss of life as posed by terrorists who may elect to attack using either conventional means or nuclear and biological material. The federal government must prioritize its efforts to provide training and equipment to local first responders in dealing with these types of incidents. Now I'm aware that there is movement in that direction, that the FBI is putting together a national program training program. It needs to be prioritized, it is significant. Training is no good without equipment. You can train us what to do all day, but if we don't have the equipment on the local level, we cannot respond. In one of the exercises and one of the discussions between law enforcement and fire safety we are talking about is the release of hazardous material and the lack of equipment that local law enforcement has to breathe in such an environment. And my colleague from fire service told me, "Well, we always have the early warning system." I said, "What is that?" "We just look for the cop that falls over, and we know how far it's coming." Obviously that's humorous, but it's not humorous if you are the people who are falling over.

The third area of concern is the ever increasing use of technology for criminal purposes, and the U.S. Attorney spoke to that and I don't want to prolong it other than to mention a couple of things. I've attached to my written testimony two articles concerning this topic. The first article appears in the June 9th, 1997, issue of *Newsweek* magazine, the second article is the June edition

of the *Law Enforcement Bulletin*, a publication of the FBI. Both articles discuss in some detail the use of technology to commit crimes, which is no secret to anybody. Police agencies are increasingly being tasked with the difficult job of solving crimes in which the criminals use technology in some way. Not only on the federal level, but every day on a local level. My community has a population of about 25,000 people. We're not a large agency, as 90 percent of the agencies in the United States aren't large agencies, we are smaller agencies, but I can tell you that we have dealt with a variety of computer crimes from embezzlement, hacking, attacks on phone systems, child pornography cases, in my jurisdiction, and I'm sure that's replicated everywhere around the country. We don't have personnel that are trained to deal with that, we do not have equipment, and we are a fairly high tech police department, fairly high tech, and we still don't have resources to deal with that. We really need some help in that area from Congress to appropriate funds for training purposes. We need more training for our local officers, because we work these cases with the federal agents, but sometimes by the time the federal agents get involved, the evidence is destroyed, because we don't know what to do with it in many cases. Also Congress needs to appropriate sufficient funds to development technology that ensures the continued access for law enforcement agencies to communication systems being used by criminal organizations for their activities. The continued development and use of new communication and encryption technology must not be allowed to block the lawful execution of court-ordered wire taps that are used to detect and prosecute those engaged in criminal acts, and what we're seeing is that the sophistication of the criminal is outstripping our sophistication, and with encryption, strong encryption technology out there, the threat to our communications systems, our data bases, as the gentleman from Monsanto just testified, it was very, very critical, very critical.

If you have any comments I'd be, or any questions I'd be glad to answer them.

MR. KEYES: The 24 megahertz of radio spectrum being allocated or proposed to be allocated in this Congressional allocation, do you perceive that to be adequate for your needs?

MR. KURLANDER: Well, what has been I assume agreed upon by compromise—which normally takes place—is 24 megahertz. We certainly need all 24 megahertz. My understanding in Congress in the discussions that there is a movement to try to reduce it and make it up to 24. 24 is the minimum number that we foresee for the immediate future. This is going to be a long term problem, and it has to be followed carefully. Thank you.

MS. ABRAMS: Thank you very much, Chief Kurlander. Our next speaker will be Cecil Wright, executive secretary of the Missouri Public Service Commission. Following Mr. Wright, we'll have Mr. Mike Cannon.

MR. WRIGHT: Thank you, Mr. Mayor, and the Commissioners. As Ms. Abram said, my name is Cecil Wright, I'm the Missouri Secretary of the Public Service Commission, I'm here presenting comments for Carl Sobers, who is the chairman, who had a similar meeting in Jeff City today and couldn't be here. I'm just going to give you kind of a brief outline of our concerns and our position, we are providing a more fuller response in response to your questionnaire, and that will be forthcoming in the next twenty or so days. For those of you who are not aware, the Missouri Public Service Commission regulates electric, natural gas, telecommunications, water and sewer companies doing business in the state of Missouri. The Commission, as I believe everyone here, has a keen interest in protecting the state, as well as the nation's critical infrastructure as it relates to energy, telecommunications, and the water area, and I have provided a copy of our annual report so you can kind of see how many utilities we have and how the state is structured.

The three areas that I will comment on briefly are the energy area, the telecommunications area and the water area. With regard to energy, our primary concern there is safety and reliability. With the numerous restructuring proposals that are being offered in Congress, as well as in many high cost areas like California, Pennsylvania, and New England, it is essential that the safety and reliability of the existing power transportation and distribution area be maintained. Regardless of whether a state is a high cost or a low cost area, safety and reliability should be a primary concern. In an increasing competitive environment, which we are all seeing throughout the nation, consideration should be given to enactment of federal laws which embody reliability standards which have been the subject of the formal agreements and standards since the northeastern U.S. blackout of 1965. While the North American Electric Reliability Counsel has done an excellent job of overseeing reliability, its guidelines and standards are voluntary. The issue of reliability is of great significance, particularly in light of two outages experienced by western states during the summer of 1996, and there also are some fears that there will be shortfalls in generation experienced by the upper Midwest and New England this spring and summer due to several nuclear plants being offline, I think all of these concerns need to be looked at.

States, individual states should be permitted to develop their own plans or restructuring and relate choice and should not be forced to fit into a national standard that may reflect high cost areas of concerns. Missouri is a moderate to low cost electrical state, and we are exploring electricity restructuring on two phases. First of all, we have a state, the state provision has developed a task force which is going to be having its first meeting on June 25th, and also the Missouri General Assembly has a joint legislative committee which will be meeting in July to look at restructuring in the state of Missouri.

According to 1996 figures, the average cost of electricity for Missouri and electric utilities for all classes—that's residential, commercial and industrial—was 6.38 cents per kilowatt hour. According to 1995 figures for Missouri, the average cost was 6.37 cents per kilowatt hour. Now you compare these with the national figure of 7.2 cents per kilowatt hour. If you just want a quick break down, the residential of 7.5 cents per kilowatt hour versus 8.9 U.S., commercial is 6.29 cents per kilowatt hour, 7.9 U.S., and industrial 4.68 cents per kilowatt hour, versus 4.8 U.S. Missouri's municipally-owned and rural cooperative electric utilities tend to be slightly lower on average than privately owned utilities, and the sources of these.... We've got the figures for the private owned utilities that are regulated, of course, from them, and the other figures we got from the American Public Power Association.

As I said as I began, the Commission looks at safety and reliability as the primary concern when you move into an area of retail competition and retail choice, and if you're looking at reducing costs for the customers for the end user, you still have to make sure that they are receiving electricity in a safe manner and that they will receive that electricity whenever they need it and as they need it.

In the area of telecommunications that you're all aware of, we're kind of in the area now of where we're entering competition in the basic local exchanges. We are just now moving into that area, we have many companies who have applied for certificates who are wanting to buy service, we have one company who is actually providing competition for basic local services in Springfield, Missouri, but we are not sure whether this competition will effect the telecommunications infrastructure that has been put in place by the incumbent local exchange company. These companies do claim that there is a threat, but it is difficult for us to assess it at this time, because we have not seen the full-flown competition till we've had a chance to really determine whether that is really true or not.

The last area is the water area, and I think this is the one that I think the chairman wanted to emphasize, I'm glad that I already heard that several people have commented on that, and our focus is maybe a little different, but what we have found is that really the water area is the most capital intensity of all the utilities that we regulate, and on a per customer basis, the water and sewer companies have the largest amount of capital devoted to public use, yet water companies probably have the lowest rates of all utilities and, therefore, the lowest revenues in order to meet these capital improvements. An example is that American Water Works, the largest privately owned water utility in the United States, has roughly seven million customers with one billion dollars in revenues, but a combination of a merger of western resources of Tennessee Power and Light, which is a new company, will have two million electric, gas and security customers, and they'll have three million dollars of revenues.

The problem is that while the infrastructure of water companies is in need of repair and federal regulations on safety are increasing, the population base is not increasing significantly allowing the revenue to keep up with the requirements of the new regulations. The recently re-authorized Safe Drinking Water Act will require 131 billion dollars to replace or repair the aging water infrastructure according to the U.S. Environmental Protection Agency. However, Congress has allotted only nine billion dollars to fix this problem, and I think Mayor Harmon is probably very familiar with the problem, as was mentioned, I think, by the alderman of the problem of the infrastructure, of how the city of St. Louis' water and sewer and drainage system has deteriorated and the age of them. These problems occur with leaking mains which caused by the old systems, some of which are as old as 100 years in certain areas, and causing many cities to lose as much as 30 percent of their fresh water supply each day, which I think, if you think about that is a very serious problem. While usage per customer declined in the last 20 years, growth and net planning has increased. Because use has not increased, there is pressure for companies to raise rates on taxes or raise capital to finance these projects. In the case of raising taxes, money must come from local customers, yet the population growth for existing companies has only been one half of one percent. Missouri has experienced continual problems also with small water and sewer companies that lack economies of scale and have relatively few customers to raise the capital and expense costs associated with the Safe Drinking Water Act and infrastructure replacement, and I think you will see that in our annual report how many small companies we have, and hopefully

we will express in a written comment about all the problems we have with these small companies about meeting a safe water and Safe Drinking Water Act.

The solutions to this: It may take a national program to support these systems which cannot support themselves through increasing rates and taxes, and also consumer education. Water and sewer bills may need to look more like phone bills and electricity bills, and you will be paying more in the future for your water supply. Thank you, and if you have any questions—

MR. RODGERS: Mr. Wright, you mentioned the need for reliability standard as we move into this restructuring. Who do you think should mandate those standards?

MR. WRIGHT: Well, I think, as with all legislation that affects the nation, there should probably be some federal overriding, overall federal standards, but I think that there should be some flexibility to allow the states to meet their individual needs as you get down to the local level.

MR. RODGERS: Thank you.

MR. KEYES: Just to make sure I understood what you said about the funding of the capital improvements and capital maintenance. Are you saying that you think it would be more appropriate for the federal government to raise taxes to pay for these capital improvements and maintenance activities as opposed to state and local governments raising taxes or raising rates for that purpose?

MR. WRIGHT: Well, I think those are the two options, and if you have a national program that tries to address this, then, of course, it will probably come from national taxes, or, you know, if the state government felt it is appropriate, then it would come from state taxes, but I think we see that as a problem and that's where the two sources of revenue that are available, and I think if you go to all of the states and you meet with the national associates, regulatory associates, that all of them have this or similar problems with regard to small companies and that needs to be addressed at probably the national level.

MR. KEYES: So if I understand you correctly, you're saying you believe that the federal government should raise taxes to fund these repairs in capital improvements?

MR. WRIGHT: Well, I don't know that I'm going to stand here and tell you that the federal government needs to raise taxes, but I think they need to develop programs that will allow these companies to meet their infrastructure requirements as a low-cost way, and I'm not prepared to tell you that the federal government needs to raise taxes, no.

MS. ABRAMS: Thank you very much, Mr. Wright. Next I'd like to introduce Mr. Mike Cannon, vice-president of NationsBank Corporation. Following Mr. Cannon we'll be hearing from Stephen O'Brien.

MR. CANNON: Good morning, Mayor Harmon, Chairman Marsh, distinguished members of the Commission, welcome to St. Louis. My name is Michael D. Cannon, I work for NationsBank Corporation, we're the fourth largest bank in the United States. I'm the manager of the Contingency Management Group of the NationsBank Corporation; we have several people who work in contingency planning in NationsBank Corporation. My responsibility is to coordinate the whole activities for the corporation. We work with the technology group, we work with the business units throughout the organization.

Just to tell you a little bit about NationsBank overall, NationsBank is in sixteen states and the District of Columbia. In 1996 we had total revenue of more than ten billion dollars and operating profit of nearly two and a half billion dollars. We have over 2,600 banking centers in the United States, and in excess of 5,000 ATMs throughout the United States. We have key lines of business in global finance, which take care of wire transfers and corporate type of activities, cash management activities, stock trades, so forth. We have a group called General Bank, and their responsibilities are more to the banking centers and the activities that go on within the banks for normal customers like you and I. And then we have Financial Services Group also, and their activities include credit card and mortgage services throughout the United States. The NationsBank Information Services Network provides commercial and retail customer access to their accounts 24 hours a day based on strict access controls.

I do have some concern in particular about the possibility of terrorist activity which could impact the telecommunications infrastructure of banking and financing institutions. I want to tell you a little bit about the process that banking uses to develop their contingency management, contingency planning management activities. First of all, in the event of any type of emergency in a NationsBank facility, a first and foremost concern is the life safety of our associates and customers. So we spend a lot of time developing training and exercises that we perform on a regular basis to make sure that everybody knows what to do in the event of such an emergency in any of our facilities. We have a dedicated staff of emergency planners and emergency preparedness personnel who continually test and update their plans, perform exercises continuously to be certain that everyone knows who will react, what they will do, when it will be done, and where it

will be done. Our emergency exercises are based on scenarios which could occur in our locations throughout the United States. We also use actual disasters that have occurred within our corporation as scenarios. Some of our emergency scenarios include hurricanes, tornadoes, floods, earthquakes, bomb threats, power outages, water damage and fires. We include technology and business recovery strategy in all our plans. All exercises are evaluated and documentation is updated appropriately. By mandate of the Office of the Comptroller of the Currency which reports to the U.S. Treasury Department, banking institutions are required to have contingency plans. They are also required to have those tested and updated annually, and they are required to present them to the board of directors for approval, as well. One of my concerns is that other industries do not have these mandates, and I'm not aware of any of these mandates for some government agencies, as well.

Another one of my concerns is with the critical infrastructures that we have, as has been told to this Commission by other members of the St. Louis community and their agencies, the age of our utilities in large metropolitan areas are aging, or becoming very old. This is an area that banking and financial institutions, as well as other industries, have no control over. Every day I read about collapsed sewers, broken water and gas pipes, sliced electrical and telephone lines, and more. It's occurring all over the United States. I know it is very expensive to maintain and upgrade these infrastructures, however, it's only going to get worse if something isn't done.

The last area that I want to discuss for concern is that banking and finances industry should partnership with the public sector. Fire and police department, Emergency Medical Services, FEMA, SEMA, American Red Cross, and others must come together with the private sector to help each other in time of major emergencies. We are teaming up with a group called Disaster Resource Council with members from the various public sector groups, not too many of the other public groups are involved, public sector companies are involved in that group. This disappoints me. The private sector must make the effort to better understand what the public sector is doing to prepare for emergencies and to get involved in emergency exercises. In St. Louis we are trying to build stronger partnerships with each other. Banks can explain what they do or are doing to help provide continuous availability to their customers during emergencies, and so can the public sector. I wish to include information to them about what we have to offer in the event that there is an emergency and that ATMs may be down, or how we can bring our systems back up very

quickly in the event of an emergency situation. This would include various electronic funds transfer systems, as well.

I appreciate the opportunity to speak to you this morning, and I will answer any questions that you might have at this time concerning my statement.

MR. KEYES: One ongoing theme that we've heard in many areas is how hard it is for private sector, particularly banks, to maintain their public standing, the recognition of the security of operations within the bank and so forth. Is there some mechanism that you can recommend whereby financial institutions can report such things as computer intrusions, particularly external intrusions in a way that would not have an adverse impact on the reputation of the institution?

MR. CANNON: That's a hard one to answer, because nobody wants to mar their reputation if there's an incident that's internal to their organization and it was handled properly and probably got the right public sector representatives involved. Banks especially have to communicate with the public sector and the FBI and other federal and local police agencies, so these incidents that might occur, sometimes they're just the result of hackers that are trying to get in, and there is no major loss to the organization. Other times there might be, and that must be followed up on, and of course proper procedures followed.

MR. KEYES: Thank you.

MS. ABRAMS: Thank you, Mr. Cannon. If there's anyone here who would like to speak who has not yet filled out the blue card, please see Ms. Sauer at the table. Thank you.

And now I'd like to invite Mr. Stephen O'Brien, principal scientist of TASC, Incorporated, of Weston, Virginia, to present. Following Mr. O'Brien we'll have James Ferrell.

MR. O'BRIEN: Good morning, Mr. Mayor, Mr. Chairman, and members of the Commission, and thank you for inviting me to appear before you this morning. TASC provides broad support and information operations to both the public and private sectors. Its activities include threat tracking, analysis and protection, vulnerability assessment, computer emergency response, and systems engineering of solutions to the intrusion problem.

Much has been written regarding the threat to the U.S. critical infrastructures in the last couple of years. Today I will constrain my comments to a brief discussion of a new emerging threat. I would like to discuss a very different aspect of the threat, which has received little attention, the sale and transfer of control of the domestic infrastructure. The issue incorporates aspects concerning public safety, as well as the economic and national security of the United

States. Most threat information examines the subject from the perspective of a friendly system which is the target of a malicious attack from outside organizations or individuals, or is betrayed by insiders or disgruntled employees. However, a new potential threat and conveyed set of capabilities is surfacing. This new potential threat to the well being of the U.S. and its citizens is the transfer of ownership and control of our domestic telecommunications infrastructure to foreign entities with close ties to foreign governments.

Let me be clear. The issue is not the export of telecommunications systems, technology or equipment which would generate business for the U.S. and provide jobs for its citizens, nor am I referring to the smaller regional service providers. Rather the issue pertains to the sale and transfer of control of the existing U.S. domestic infrastructure to foreign entities. The control and services provided by the few national telecommunications firms in the United States play a central role in the operation, recovery, reconstitution and preservation of other critical national infrastructures. The role of the national telecommunications firms is vital to this end, and the U.S. should not allow the transfer of control and ownership of these infrastructure lynch pins to foreign entities, many of which are owned or controlled to varying degrees by foreign governments. The transfer of ownership and control of the national telecommunications infrastructure could have fatal consequences.

For example, on 17 May, 1997, *USA Today* reported that the FAA had experienced an outage that left 180 aircraft over six states with little contact with the control center. The FAA was reported as saying that the problem appeared to involve MCI communications equipment. The communications system handles the radar information from ten remote towers in six states providing controllers with communications to pilots and other controlling centers. Seven towers were knocked out while others had limited visual signals. According to Tim McDonald, a union safety officer, “We were really sweating it out watching weak images of the planes flying overhead, trying to calculate if any were on converging flight paths.” This recent event underscores the interrelationships between certain critical infrastructures. Given this example, the importance of maintaining a connectivity and control of these services and its necessity in avoiding collisions and providing critical data to air traffic control centers, we need to seriously examine the sale and transfer of control of the companies which hold these contracts and provide these types of services prior to allowing their takeover by foreign entities.

Fundamentally we must be able to answer the following questions. Is it in the best interest of the United States to turn over the control of such support systems to foreign entities? Second, how do we protect the safety of our citizens if we sell off the controlling infrastructures to overseas buyers? Third, would we have awarded contracts entailing such sensitive capabilities to these firms if they were under foreign ownership and control at the time of the award? And finally, how do we ensure that these foreign buyers won't sell the U.S. domestic critical infrastructures to more hostile states in the future?

In the area of economic security, the economic or the Electronic Communications Privacy Act, or ECPA, gives telecommunications service providers the right to intercept, use and disclose information that is passed over their systems. Given foreign ownership and control, this could easily be performed from a continent away. While the ECPA never envisioned foreign ownership of U.S. telecommunications service providers, the U.S. has legalized the interception, disclosure, and use of communications by all service providers and, therefore, may, in effect, be inviting foreign owners to use this exemption to collect economic intelligence on U.S. firms.

In Senator Patrick Leahy's testimony to the Permanent Subcommittee on Investigations approximately a year ago, the senator quoted an unidentified U.S.-based manufacturer who said, "We just lost a major procurement in a Middle Eastern country by a very small margin to a state-subsidized European competitor. We were clearly breached; our unique approach and financial structure appeared verbatim in their competitor's proposal. This was a 350 million dollar contract worth over 3000 jobs."

While the Congress has taken recent action to combat economic espionage, the sale and transfer of control of major U.S. telecommunications service providers to our economic competitors could undo much of the progress that has been made to date. The ECPA's provision for service providers could result in an economic intelligence windfall for our competitors across a spectrum of U.S. businesses.

As the former director of French intelligence, Pierre Marion, once said, "Economic espionage is a fact of life." This opinion is held by more than one of our economic competitors, each of whom derive a great economic advantage over American businesses provided with the capability and opportunities to legally intercept, use, and disclose any or all information transmitted over one of the largest telecommunications systems in the U.S. and the world. While Messier Marion

is correct in his assessment, I do not believe we should make it any easier for our economic competitors than it already is.

Finally, in the area of national security, a serious concern presents itself. As was described in *Jane's Defense Weekly*, "About 90 percent of the Army's information is owned and operated by non-DOD public agencies. This presents the greatest challenge to information availability and reliability, because the deployed force commander no longer controls circuit availability, integrity, reconfiguration or reconstitution." In order to provide necessary connectivity for the Department of Defense, the Defense Information Systems Agency, or DISA, has initiated a series of contracts with the largest national telecommunications service providers. The program is known as the Defense Information Systems Network or DISN, and will have transmission services, network management, and classified portions of the network provided by AT&T, MCI and Sprint, respectively.

Given the long dependence of the DOD on these national telecommunications service providers, the United States needs to ensure that we do not sell off or transfer the control of these systems to foreign entities which might compromise the availability, integrity, reconfiguration or reconstitution of the DOD's telecommunications. It would be ill-advised to provide any foreign power with the capability of denying, disrupting or monitoring our defense telecommunications in the United States.

In summary, the United States needs to act in the interest of all the citizens rather than providing a means to accumulation of wealth by a relative few. We are approaching a critical juncture in telecommunications. While the U.S. has never permitted the transfer of control of an entity such as AT&T, MCI or Sprint, the first takeover bid has been made, and the FCC and, hopefully, the Committee on Foreign Investment in the United States are currently investigating the implications associated with the proposed sale and transfer of control of one of these firms. This is a very dangerous precedent that is being examined. Caution is required and a deliberate approach is necessary to ensure that the issues that I have outlined above are adequately addressed.

Again, let me be clear, the issue is not the export of telecommunications technology, equipment or services, which would generate business for the U.S. and provide jobs for its citizens. Nor are my concerns related to the sale of telecommunications assets in foreign countries. Rather, the issue pertains to transfer and control of the U.S. domestic infrastructure to foreign entities.

Allowing foreign companies access to the U.S. telecommunications market is one thing. Transferring the control of the U.S. domestic infrastructure is something else.

Finally, we must weigh what might be gained by what we stand to lose. The American people need to understand the potential impacts associated with this topic as it cuts across the rights of U.S. citizens, public safety, and the economic and national security of the United States.

Thank you once again, Mr. Chairman and Commissioners, for this opportunity to speak to you today, and may I convey my best wishes. And if I have about 10 more seconds before the end, I'm also an instructor or a guest instructor at the Federal Law Enforcement Training Center, and I would put in a plug that we come up with some means by which those types of materials and courses could be given in terms of a mixed audience which would cut across the federal, state and local level and perhaps find a means to convey at least some of those materials to the commercial section.

MR. RODGERS: Sir, I have a question. I take it your alarms encompass the MCI-British Telecom merger that's proposed. Do you feel that the FCC does not have a direct mandate to protect the U.S. interest, the public interest in this kind of merger, that the only way we can protect it is to prohibit those kinds of acquisitions of U.S. infrastructure by foreign powers, by foreign companies?

MR. O'BRIEN: There may be a variety of what mergers that can be prohibited. There may be a means by which such a sale could be allowed given certain provisions, but I don't know how you try and protect the domestic infrastructure and those things which those contracts also support, such as the FAA, for example, when you are indeed transferring the control of those entities and the physical infrastructure over to a foreign entity, over to a foreign government.

MR. KEYES: You indicate you are an instructor of FLETC?

MR. O'BRIEN: I'm a guest instructor.

MR. KEYES: Does FLETC have a capability for instruction in computer intrusions that could be made available at the state and local offices?

MR. O'BRIEN: To that extent, the only thing I can say is that we have put together a course in the Weston, Virginia, area with cooperation from down in Winfield, Georgia, where I'm also a guest instructor, to try and give a broader distribution.

MR. KEYES: Is it a distance learning project, or does it require on-site participation?

MR. O'BRIEN: It's on-site participation.

MR. KEYES: Are you aware of any distance learning?

MR. O'BRIEN: No, sir, I am not.

MR. KEYES: Okay.

MS. ABRAMS: Thank you very much. Our next presenter will be Mr. James Ferrell of the St. Louis Regional Commerce and Growth Association. Following Mr. Ferrell, we'll be hearing from David Snider.

MR. FERRELL: Thank you, and welcome to St. Louis, it's a pleasure to be here today. My name is Jim Ferrell, I'm Vice-President of Infrastructure for the St. Louis Regional Commerce and Growth Association. We are the regional economic development agency for a two state and twelve county region in this metropolitan region. We represent over 4,000 businesses that equal up to and over 40 percent of the employees throughout the St. Louis metropolitan region. We also represent the full spectrum and range of business and employers in the area. These range from the major employers of McDonnell Douglas, Boeing, Monsanto, and Anheuser-Busch to many of the small high tech firms that are emerging and growing very rapidly in the St. Louis market place. We have over 1,200 high tech firms in the area, and we would represent thousands of small businesses, ranging from one- to five-person shops, whether those are printing companies or small individual professional firms, as well as the major trades that are available here in the St. Louis area. So we represent all types of interests and businesses throughout the region, and RCGA has been working very diligently with the cooperation of our public sector partners—the City of St. Louis, the St. Louis County, the other counties in our metropolitan region, as well as the two states—in dealing with the critical infrastructure issues that face in this region and face the country, and we recognize the critical need that is out there for funding and adequate funding for all of these infrastructure initiatives. We feel very strongly, and in our development of our strategies for economic development in this region, infrastructure has been identified as a crucial component of economic development, as it is across the country.

It's never more evident than in the St. Louis area, which is a national and international transportation hub with the second busiest airport in the country. A new major airport just developed on the Illinois side, a joint public/private use airport, four major interstates that dissect the metropolitan region, the second largest inland port in the country, and the second and third largest hub for a rail hub, not to mention the three rivers that run through our community that

provide tremendous water supply to our area. But infrastructure has been identified as a key to the economic future of this region, and we are continuing to develop our strategies to improve that infrastructure system and working with the federal, state and local communities to do that.

One of the issues that has been brought up here by many of the people that have spoken already is telecommunications. Telecommunications is an area of infrastructure that we have recently really focused on as crucial to the future economic development of our region. We have selected some of the key telecommunication companies and executives in our region to help us develop a strategy that will make sure that the businesses and industry within our region have the advantage of having a quality telecommunications infrastructure that will enable them to compete in the international global market place that every business is really dealing with these days, not only in this St. Louis region, but across the country. Telecommunications and the strategies that we look to develop today and in the future will absolutely be crucial to each and every business that we represent with RCGA and that are throughout the metropolitan region and this country, because we can no longer just look at the borders in which we reside or our country resides, but the market place is international, and telecommunications and the ability to have safe secure systems is crucial to each and every business, no matter if they are a one person shop or the thousands of employers and employees of a major corporation.

So we encourage your efforts to identify these critical security needs for our telecommunications and information technology that is so crucial to the future economic development of our country and the St. Louis region. So we commend you for your efforts and are willing to offer our assistance in whatever we can do to further your work and the efforts of the country in that effort.

MS. ABRAMS: Thank you very much, Mr. Ferrell. Our next presenter will be David Snider, Assistant Chief Engineer with the Missouri Department of Transportation. Following Mr. Snider, we'll hear from Mr. Dan Walz.

MR. SNIDER: Good morning, Mayor Harmon, Mr. Marsh, and members of the Commission, I'm going to digress from all this, I'm going to talk to you about steel and concrete rather than fiber optics. The Missouri Department of Transportation is the largest state transportation department in the state of Missouri—it's the only one, so we're the ones that's got all of the apples, so to speak. When Mr. Marsh wrote and invited our department to make a presentation, he listed five things, I'm going to address those five questions he did, because I think it's important,

because you know where one state DOT stands in regard to the possibility of having a loss of some of its infrastructure. What's critical to us? Well, our state is blessed and cursed by two rivers. The Mississippi is our eastern boundary; the Missouri, which splits our state in half and is half of our western boundary, provides tremendous commercial, recreational, and a source of water for many of our citizens. That's the blessing. The curse is you can't get across it unless you cross on a bridge. Now there used to be ferries, and they'd take 100 cars every hour or two or something like that, we have one little bridge over here carries 185,000 cars a day. And if you want to see the chaos that happens, somebody sneezes on that bridge, you back traffic up for a half hour or more just because of that. This morning a gentleman mentioned the fact that a tanker turned over, I happened to be coming in on I-64 this morning right about that time. Let me tell you, it's not fun.

Actually, this is fairly timely for us, because I just appointed a task force to review our earthquake preparedness plan, because the New Madrid earthquake fault has a significant possibility of moving one of these days. One of these days is whatever you want to define it, if you want to say tomorrow, fine. If you want to say 10,000 years from now, that's fine, too, but it's going to move. They tell us it's going to move. And if it does and if you measure it 7.0 on the Richter scale, our fair city of St. Louis here and its environments will become idle. Having thought about that, the Missouri, Mississippi and Meramec Rivers create an island effect on this city, except for the Route 100 that comes in on a ridge, that's the only access that you, we almost can assure that's going to be available. Thinking about that, there's a similarity in what if you lost those structures not to earthquake, but to some other reason—same effect, you become an island. And so, therefore, our bridges, our highways, and our buildings that we own and operate are very important to us, and that's our critical structures. Probably bridges is the key thing, because our whole system of highways in this state, and I tell you all the whole United States, is only as strong as the bridges that they have to link the highways that join them. So that's our number one.

Now what are we doing about some of the things? Well, let me tell you some of the problems that we have in this state. We want to retrofit the bridges in St. Louis for earthquake devastation. Right out, and I don't know which way I'm facing, but U.S. 40 is right here beside City Hall, it's I-64, there's what we call a double decker there. We want to retrofit that to withstand earthquakes, 33 million dollars. One bridge, one bridge. I think there's eleven or twelve in the

Missouri and Mississippi/Meramec basin. So we have a great challenge, what I talk as a challenge to ourselves to do that. By the way, we have a number of bridges down the Mississippi through our boot heel that would cause just as much devastation to those people as the loss of these bridges here.

What security systems we have in place. I presented the lady outside a description of what we are doing so far as far as trying to watch ourselves. We have what's called a neighborhood watch program, so to speak. Daily we ask our field personnel, as they drive our system, if they see any unusual vehicles parked near or very close to any of our structures, we ask that those be turned into our highway patrol or local police or local sheriff's office for review. What's going on, why is that there, because normally it's not there. Can we, can we stop devastation? I don't think so. But what we can do is what you've heard a lot this morning is the training. There's policemen, there's firemen, there's ambulance drivers, many emergency personnel that drive our city on a regular basis, and if they, too, were schooled in the fact of watching for things like this as they do in their normal rounds, not maybe emergency rounds, be our eyes for us to watch for potential hazardous situation. Can we stop it? I'm sorry, gentlemen, I or my staff or my peers, we don't know how you look after 32,000 miles of a highway system in our state or the 110,000 miles of highway system in Pennsylvania and West Virginia, Virginia and South Carolina, I don't know how you do that. All we can do is be prepared if something happens to know how we're going to react, and react as quickly as possible.

A couple of gentlemen talked to you about power outages. Think about it, Mr. Mayor, it's 4:00 today, and we have a total black out in St. Louis. I've calculated it takes fifteen minutes to have gridlock on 500 square miles of highways in this area. So I don't know what that says to you, but it says a lot to me, that you're not going to get any fire protection or police protection or ambulance protection if you have gridlock, if you understand what gridlock means, it's a big parking lot on the highway. So we're doing things in our own buildings, we have now keyless entries in many of our buildings, we have security measures, we have our Capitol Police review every district office in our state to look at various ways to protect our people as well as our customers for intrusion that shouldn't be there, and we're modernizing that as we have the funds available.

Are the services you receive reliable? So far we haven't lost a bridge, so I guess they are. But so far all I can say is we, we're as good as what we have seen so far, and so far no problems.

What should the government's role be in regarding safety and dependability? I'll take anything. We have, as I said, really thought about this, and I guess we have the responsibility and so we've told our people, "Watch, look, look for the unusual, look for the things that you don't normally see, that's uncommon," and provided the training, I guess if government does anything, provide the training for the people that are out there that can possibly help us do things like this.

And what are the future safety plans? Well, we're going to continue watching our bridges, we're going to continue retrofitting our bridges so that they are usable, passable under all conditions. Our buildings, we will continue to upgrade them also for security purposes, because there are large numbers of people working there, plus the fact that we have many customers that come to see us on a regular basis that need to do business with us, and they need to be in a safe property.

Gentlemen, ladies, I thank you very much for the opportunity on behalf of the Missouri Department of Transportation, and I hope I've answered your questions, Mr. Marsh, as you come forth.

MR. WALZ: Thank you, good morning, welcome to St. Louis, and welcome to our cool summer weather. My name is Dan Walz, and I am the Conference Coordinator of the *Disaster Recovery Journal*. Today I am representing Richard Arnold, who is the president and editor-in-chief of the *Disaster Recovery Journal*, and the president and CEO of Private and Public Businesses, Inc., otherwise known as PPBI, and Richard is standing off to my left next to the wall. Richard would be speaking to you himself today, but he suffered a stroke seven years ago, and his speech is quite impeded, so I will be speaking for him. We thank you for inviting us and giving us the opportunity to talk to you this morning. We thank you for the honor and the privilege.

Richard would like you to know more about PPBI. There is a packet of information passed out sitting before you explaining the formation and structure of the organization and its mission and goals. PPBI is a nonprofit corporation that was established in 1996 after Richard identified a need for all types and sizes of businesses. Richard identified one distinct problem above all other problems when disaster strikes and infrastructures fail. The main problem is exemplified by the Oklahoma City bombing disaster. Although the Oklahoma City bombing was a unique incident, it spotlighted a problem that all businesses are vulnerable to in a major disaster. The problem. In

the Oklahoma City bombing, as in the World Trade Center bombing and the flood of '93 here in St. Louis, it was limited access or no access by business owners, proprietors or their agents to their businesses, which caused businesses to fail, which led to further hardships in the community.

Richard visited the Oklahoma City area shortly after the tragedy, observed long lines of people waiting to get clearance to pass beyond the outer perimeter of a cordoned off area. Among the people waiting in these lines were owners and operators of businesses that were affected by the bombing. Some had to wait several days before being allowed to examine their property and retrieve vital records and equipment. Some were denied access altogether, even though their business was not directly affected by the destruction. The same can be said of any disaster where access is limited, whether it is due to such events as hurricanes, tornadoes, wild fires, blizzards or floods, and as in Oklahoma City and the Trade Center bombing in New York, it's man made.

The result of denied access was a loss of revenue, a loss of inventory, a loss of jobs, and a loss of tax revenues to the community. The devastation goes far beyond the disaster setting, it extends beyond the infrastructure, it extends to the viability of the entire community. Because access was denied to business people, Richard saw a problem that could be remedied. The solution to the problem is something tentatively called PACA, Preferred Authorized Customer Access. This is just one of the elements of PPBI's goals and objectives.

As part of the, as part of President Clinton's Public and Private Sector Partnership Initiative and FEMA's Disaster Resistant Communities Initiative, PPBI has had several meetings with FEMA officials in Washington to discuss this problem of business access during disasters. In these meetings, we discussed a credentialing system such as PACA for allowing access by business owners or their agents to the property located within a restricted area due to a disaster.

FEMA has been very receptive of the concept and understands the needs, but has been very slow to act. It is vitally important to the continued operation of any business that access be gained to their property to assess the extent of devastation, evaluate the destruction, to retrieve vital records and documents, and secure vital information and equipment, and to develop a strategy of recovery. We ask that you, as a Commission, look further into this matter and assist the concept that is proposed by PPBI.

The mission statement. The mission of PPBI is to act as a clearing house for the exchange of information between private business, public agencies, emergency management, through

communications, training, and standard setting in order to increase awareness of the economic viability of a community as an issue during the recovery from disasters. PPBI is composed of an executive board and a research and evaluation board. Members of the board include executives from three major vendors in the field of disaster recovery planning, and others, including Comdisco, SunGard and IBM. Also Northrup Grumman, Southwestern Bell, and members of the public sector, such as the director of Emergency Management for the city of Phoenix and the President of NCCEM, the National Council for Certification of Emergency Managers, as well as academia, through George Washington University, Southern Cal, North Texas State and SIU, Carbondale. PPBI will be meeting this coming Sunday and Monday in Chicago to refine the concept of credentialing and to prepare a deliverable that is based on common practices and accepted standards.

PPBI will also be presenting the credentialing process in six states on a local level. Some of the local jurisdictions have already approved some form of identifying qualified individuals in the credentialing system for business access. PPBI will offer the system to other jurisdictions and will also offer them an opportunity to give input into the process.

This March 16th, 1998, PPBI will hold a CEO conference in San Diego where 200 CEOs from around the country will discuss disaster-related issues in a round table discussion. An invitation has been extended to the vice-president, Al Gore, to address this group on the Partnership Initiative and the Disaster Resistant Communities Initiative. One of the discussion points will be access to businesses after a disaster.

To assist in the development of the private public sector partnership, you need to better understand the issues involved in disaster recovery planning through the public and private sectors. PPBI has developed a glossary of terms used by emergency management and the disaster recovery industry. This glossary combines the terms used by NEMA, National Emergency Management Association, FEMA, academia, and DRJ's own glossary of E.R. industrial terms. You can find this glossary and more about PPBI by visiting our Web site at www.ppbi.org. We thank you for your time, and we ask you for your support in this matter. Thank you.

MS. ABRAMS: Thank you very much. Following Mr. Walz, we'll now hear from Mr. Phillip Gould of Washington University, Missouri, Seismic Safety Commission, Professor and Chairman of Civil Engineering at the university, and then Mr. Charles Heisler.

MR. GOULD: Good morning, ladies and gentlemen, thank you for the opportunity to speak to you briefly. I am here in two roles, both as the chairman of the Department of Civil Engineering at Washington University where we ultimately have a big responsibility in educating the engineers of the future to be able to design the appropriate types of systems that we identify will be needed for our country, and also as the vice-chairperson of the Missouri Seismic Safety Commission. As I've noted in my written remarks, we have recently prepared a report under the mandate of the state legislature and have delivered this report to Governor Carnahan within the last month, so I won't really have to discuss this very much—this is available to you.

The Missouri Seismic Safety Commission is directly concerned with the protection and survival of critical infrastructure. From Chairman Marsh's initial remarks, it's apparent that the flood and tornado threats to this region are well known. But as Mr. Snider has also noted, we do have a significant earthquake threat. A high priority in our report is the consideration of other threats besides earthquakes, both physical and natural. We call this multi-hazard consideration in our design of structures and other infrastructure systems. For example, a prominent conclusion of the investigation of the Oklahoma City bombing was that if that structure had been designed according to the standards for earthquake-designed construction and detailing, much of the damage to the structure would have been reduced and the collapse would have been avoided, so that's a poignant example of the connection of multi-hazard protection of infrastructure.

I encourage the Commission to encourage multi-hazard considerations in the design of new infrastructure systems and also in the rehabilitation of existing systems. Rehabilitation of existing systems is a particularly significant issue, because in many cases, this is not mandated, this is not covered by building codes, but rather is dependent on volunteer compliance. The infrastructure interdependence is, in fact, remarkable and greatly complicates the consideration of individual hazards. Again, Mr. Snider has described the effect of gridlock produced by the collapse of one infrastructure system and how this makes it virtually impossible to invoke protection on another infrastructure system.

Another example which was again alluded to, if this earthquake that we do expect within the next foreseeable future had occurred during these floods of 1993, this St. Louis region would have been a virtual island, and the rescue and response operations which have been very carefully conceived and planned by Emergency Management Agency would have been very, very difficult to carry out, due to the limited access and the unavailability of some of our roads and bridges.

The Seismic Safety Commission hopes that our report will be of value to this Commission in their deliberations. Thank you.

MR. RODGERS: Sir, I have a question. You mentioned about this architecture that would better protect these buildings. You mentioned the operative ability in Oklahoma City. If that building had been constructed the way you would now recommend, would it have cost any more to construct it, or is this a much more expensive type of architecture you're talking about?

MR. GOULD: The type of construction and the engineering, additional engineering studies that would have been required to construct that building to earthquake standards would have been less than five percent additional cost of the building.

MR. ROGERS: Thank you.

MS. ABRAMS: Thank you very much, Professor Gould. Our next speaker will be Charles Heisler of the Jefferson County Commission, and following Mr. Heisler, Professor Tom Bratkowski, Maryville University.

MR. HEISLER: First of all, speaking for Jefferson County, the county is going on 200,000 people right now, when I did receive your invite, Mr. Chairman Marsh, the first thing the County Commission did was directed our Director of Emergency Management to compile some information which your secretary will have a copy of. I know this has been a long drawn out affair here, and I think most of the comments I have may have been recited, but I'd just like to read a couple of excerpts out of our executive summary on this. Jefferson County is the fifth largest county in Missouri with a population in excess of 192,000 in 1996. The county covers 168 square miles, and is surrounded on three sides by navigable waterways. In addition to the hazards addressed in the attachments, I am concerned with five other vulnerabilities which apply to the hazards addressed. Number one, warning systems, number two, the economic impact of interrupted access to St. Louis, we've heard about bridges, continuation of waterways and ground water, and number five, the lack of local public and aviation support.

I'm going to skip a paragraph, because I think we have to look at the long term survivability from a worst case scenario. It would be determined by the following three items. The ability to reestablish transportation routes with St. Louis County and city, and number two, the ability to expedite insurance claims for home owners, and number three, the ability to counteract social and emotional stresses resulting from a massive disaster, and I'd like to read just one more short paragraph here, because this all comes back to what we've heard today is the economical factors.

The most devastating economic factors facing Jefferson County is the potential for isolation from St. Louis County. Approximately 65 percent of our work force resident in Jefferson County work in St. Louis County and the city. If transportation routes across the Meramec River are blocked or lost, the long term impact would be devastating. Interstate 55 and 44, Missouri States Route 21 and 30 are the only links between Jefferson County and St. Louis. Survivability of Interstate 44 and Missouri State 30 are fairly high. Survivability of Interstate 55 and State Highway 21 are less probable. These two roadways carry the majority of our traffic.

I have our Director of Emergency Management here who developed this book for us, you will receive a copy, and he's done some very detailed work in the back, some very graphic work on Jefferson County, and I would really appreciate it if you all could take a look at this, it was a good job and again, speaking for almost 200,000 people, we hope that you're here in St. Louis today to listen to our problems and possibly send some type of procedures to help us out, and I thank you very much. If you have any questions, I'd be more than happy to answer them.

MR. KEYES: Do you have any thoughts on particular funding options for these issues? Obviously there's the Federal Highway Trust Fund, but are there other areas that you would contemplate?

MR. HEISLER: Well, we have been using some, naturally for some of our roads we have gotten federal funding, and also some state funding, so we have tried to use any and all possible ways to protect ourselves. We also have asked the citizens of Jefferson County to tax themselves for road and bridge. I feel very proud that since about 1979 or 1980 there was a bridge bottom passed, a half cent sales tax, and in Jefferson County, and certainly you can document this with the State of Missouri, our bridges, our local bridges, we are number one in the redevelopment of our own bridges, so we're very proud, and again, that's how we have tried to help ourselves, taxing ourselves. And now we have identified with our constituents and we have a fifteen year sunset on this. About the year 2001 we're going to go back to ask them to do some other things. So we're willing to go out to our people and ask them for money to do it, we have proven we can do it, but again, as I stated here, there's federal and state highways that really affect us, so again, I thank you very much, and if you have any questions, please contact us, thank you very much.

MS. ABRAMS: Thank you, Mr. Heisler. Now I'd like to introduce Tom Bratkowski, Professor of Biology and Dean at Maryville University, and then we'll be hearing from Dr. David States.

MR. BRATKOWSKI: Good morning. I'm Tom Bratkowski, and I am Professor of Biology at Maryville University and Dean of the College of Arts and Sciences there. I'd like to thank Chairman Marsh and Commissioners for the opportunity to speak before you on the topic of protecting our national critical resources and infrastructures. I'm a life-long resident of the city of St. Louis, and I play a role in this community as an educator and a private citizen. I encourage you to take a minute after these long and patient hours of hearing to stretch and to kind of look around the room and enjoy the appointments before you. This building and its ornate appointments are a legacy of many generations of St. Louisans. We've had a proud tradition of taking care of our urban infrastructure, and we hope to do so in the future.

I realize that the mandates of the Presidential Commission is to provide a strategy to bring forces together to deal with the immediate risks and to plan for the continued operation of critical infrastructures. There are some major concentrations of resources which could, unfortunately, act as vulnerable choke points in St. Louis and in many other cities. I would like to touch on a few local examples of our urban infrastructure which could become sites of either natural disasters which we've heard about or the targets of physical threats.

The oil tank field along the Mississippi River out here, which is just south of the famous Anheuser-Busch Brewery, is an area that could be the object of criminal attack. Due to the proximity of numerous oil tanks to each other, to the river and to Interstate 55, an explosion could possibly block this major north/south transportation artery, as well as cause an oil spill on the Mississippi River of great proportion.

The large natural gas storage tanks in our city are also located in vulnerable places. The gas tank at the west end of St. Louis just south of Interstate 64 or Highway 40, which is our major east/west transportation route where about 130,000 cars pass every day, is also vulnerable. This tank is very close to the BJC Hospital Complex, Washington University Medical School and the Central Institute For the Deaf. Another large natural gas tank which is located on Interstate 44 at the southwestern city limit is also a potential transportation choke point. An explosion of either tank could cause much loss of life and block highway traffic along our primary transportation corridors.

These are examples of urban components which are conspicuous because of their size, and I hope that our city planners and emergency preparedness managers have already given some thought to the oil and gas tanks and these distribution points to make them less susceptible to

damage due to natural disasters or violent acts. An initial inventory of similar major choke points in our cities across the country seems like a good starting point in identifying and protecting these sites for the distribution of petroleum products and natural gas.

My major concern this morning, however, is to address the subtle and less obvious aspects of our regional infrastructure. Our St. Louis urban infrastructure is very fragile in terms of the erosion of our core city and the decentralization of our population into the surrounding rural environment.

An example of this thinning of critical infrastructure can be seen in the demand for utilities. As the lines of service for water, sewer, electricity, natural gas and telephone become stretched due to urban sprawl, the cost of those utilities increase due to added construction and maintenance outlays. In reality, rather than supplying more people for less cost in the central core, we're subsidizing the people at the extremities of our region by dividing up this added cost among all the customers for these services. This approach is not sustainable for the future. It will become increasingly a transgenerational burden.

There should be a differential utility rate and a differential utility tax to reflect the increased cost of providing service for distant residential, commercial and industrial construction. This added expense to the distant consumer may provide an incentive for central metropolitan repopulation. Similarly, due to urban sprawl, transportation needs continue to increase. The planning, construction and maintenance of highways, roads and bridges, as we've heard about before, consume more and more of our tax base and lead only to more vehicular traffic, more cars, more roads, more bridges.

At the same time, the consumer distances between homes, places of employment, education and recreation, continue to grow. We are spending more of our time driving and increasing our per capita consumption of natural resources. This model is also not sustainable in the future. We need a strategy to reduce the current American ideal of one person, one car. At the same time, the real impact of vehicular emissions continues to frustrate efforts to improve the air quality in the St. Louis region. Some of the volatile organic emissions and ground level ozone production due to automobiles have been in part addressed by the EPA mandated vapor recovery measures instituted, and by the state motor vehicle emissions and safety inspections.

But the current pattern for the future appears to be for increased individual vehicular travel, more four lane or better highways and roads, more bridges over more waterways and consequently more shared transportation costs for future Americans.

There are some bright spots to point to as better directions for the future. Our local effort in St. Louis mass transit known as Metrolink has been in operation for a few years, and was initially predicted to carry only 17,000 passengers per day. But instead, Metrolink now carries 40,000 people each and every day. The long term outlook requires that we try to find ways to put more people into fewer vehicles to reduce traffic congestion, to reduce collective costs for fuel, to reduce air pollution, and to increase the livability of our metropolitan area.

We must build a transportation infrastructure which is durable and sustainable. The current network of roads and bridges has carried us this far, but thoughtful planning for mass transit is now essential to have a sustainable transportation infrastructure.

The short history of our Metrolink has proven that people will use mass transit when it is safe, convenient, clean, comfortable and inexpensive. The ongoing challenge for Metrolink is to maintain high standards. The few examples of breaches of security in park and ride facilities must not be allowed to grow and to spoil the positive public perception of a well run organization. The goal of transporting more people with fewer vehicles would go a long way toward developing an air pollution prevention strategy.

I would like to call your attention to the impact of flooding on the infrastructure of our region. The most recent major floods in 1973, 1993 and 1994 devastated parts of our metropolitan area. Yet during those floods most of the city of St. Louis and its surrounding suburbs remained well above the crest of the deluge. The water purification plants and the metropolitan sewer district facilities continued to operate without interruption or inundation.

What we have ignored, however, is to protect our regional watershed and its absorptive capacity. As more surfaces have been paved over, there has been a gradual increase in local flash flooding, rapid erosion, and some mud slides. This is most notable in hillside subdivisions where some foundations have shifted and cracked causing newly built homes to be virtually worthless.

Across America there are central cities like St. Louis which have provided a fine living space for many people in the past, but they are underpopulated today. These are places where people can and should live rather than on flood plains or in areas prone to flash flooding or rapid

erosion. The central urban infrastructure is now still intact and under-utilized, and it makes sense to provide a federal tax incentive to repopulate our cities.

Every time there's a major building implosion, the event is promoted as a positive step and the staging is followed by media coverage, but in reality, it is a clear loss of our infrastructure. Solid buildings can be maintained and continue to be useful to our society for hundreds of years, yet they're demolished for parking lots to continue to consume fuel and to pollute our air. There is a need for a federal historic tax credit which would be one way of supporting the maintenance and creative reuse of central urban buildings of all types.

There are many ways of defining and protecting America's critical infrastructures for the future. I ask the Commissioners to broaden the presentation mandate to include a fresh approach to reappraising the value of the living space of our central cities. Their current policy of benign neglect at the center and urban sprawl at the fringe is extremely costly and cannot continue. There must be defined limits to suburban expansion. Our nation's infrastructure without this limit will ultimately collapse.

In my mind this larger challenge is greater than the risk of criminal or cyber-terrorist threats to our nation, and it's a challenge which we must face at the local, state and federal levels. Thank you for the opportunity to address the Commission, and best wishes in your deliberations on all of our behalf.

MR. STATES: Mr. Marsh and the Committee, thank you for permitting me to speak, I will keep my remarks brief and will focus on the issue of computers in communications in the health care system, and concerns about their performance during times of crisis. We face an increasingly complex and information intensive health care industry. Americans are older; as we become older, our medical problems become more complex, the fact that we have a more elderly population is, in fact, a direct result of the health care system which is far more capable than it was only a generation ago.

The health care system depends on communications, telecommunications and computers in many ways, ranging from the diagnostic laboratory to the monitoring systems used in the hospitals, communications, and even computers as instruments of therapeutic control. The elderly population places an increasing priority on the need for timely access to medical records.

At the same time, the health care industry, as many industries, faces several drives to look at the centralized and limit diversity in services. There are economies of scale in telecommuni-

cations, as well as efficiencies of scale. Why invent a second Internet when the Internet exists and you can simply use it? There are also market forces driving centralization. For example, although we have two cellular phone systems in the St. Louis area, because of marketing considerations, the staff at Barnes Hospital almost exclusively uses one. If there were an outage in that cellular phone system, it would significantly disrupt communications within a major emergency hospital.

Similarly, we depend on the Internet for communications to the outside world, and increasingly because it is such a convenient system under normal times, it becomes a critical part of the infrastructure. Distributed computing is also evidently leading to distributed vulnerability. The economy and the power of distributed computing systems is that you can make use of, promote computers for various capabilities, but inevitably, you are depending on them, you are depending on them, and if either communications to the remote site where the remote site itself becomes disabled, you may be, in fact, disabled yourself and we see this, for example, that a problem of a malfunctioning piece of equipment in one part of the Washington University campus disabled computers at many other sites.

Rapid growth has also—I think—led to ignorance of dependencies within the systems. I think we are very acutely aware of the threats to our bridges and electric power systems, because we've had bridges and electric power systems for many decades. The communications and computing systems have grown up very recently, and we have only had a very limited number of times where these systems have been subjected to a major disaster.

Computing can also be a barrier to communication, as well as a facilitator of communication. We joke in the computing business that there's one universal standard, it's 8.5 times 11, the printed sheet of paper. The interoperability of computer systems is very difficult to achieve. If we want, for example, to transfer patient records in large scale from Barnes Hospital to another hospital to provide care at a remote site during a time of crisis, that is very difficult to achieve without advanced planning.

There are those who will raise a privacy issue in particular on patient care records, I would say that in many respects the cat is already out of the bag in the form of normal business records, that an insurance company that has been asked to reimburse expenses for cardiothoracic surgery or chemotherapy can and does reasonably infer that this individual has heart disease or cancer.

The answer to that is legislative protection, such as the Americans With Disabilities Act, rather than not fixing the problem of interoperability and communication of health care information.

The efficiency and somewhat cut-throat competition in the health care industry is also being derived to eliminate any unnecessary services and inevitably to reduce the reserve capacity of the health care system. During times of crisis, we obviously need exactly that reserve capacity.

In terms of recommendations for the Commission, I would urge you to consider the reserve capacity of the health care system in ways in which that ought to be funded. This is really a national need. Disasters can be regional as well as local. It is not a part of the ordinary business plan of the hospital or health care system to be providing out-of-the-ordinary disaster relief services, but clearly in the case of a major fire, flood, earthquake or other disaster, those services will be needed. I do think that interoperability and telecommunications of health care information is something that needs to be addressed.

Finally, I would urge the Commission to consider the possibility of major epidemics—as well as fire, earthquake, a terrorist attack—as a threat to our infrastructure. We have a population which is a unique biological niche; there were not 250 million Americans only a couple of generations ago. We have faced major epidemics in the form of, for example, the swine flu epidemic, the AIDS epidemic, and we have an increasingly centralized system of food services and preparation of various articles so that contamination of one lot of strawberries can have literally national consequences. The infrastructure needed to deal with this possibility includes monitoring of the research and investigation infrastructure to be able to identify what the cause of an epidemic is. One of the unknown or little credited benefits of the war on cancer is the fact that we knew what AIDS was when HIV struck. Without the war on cancer, we would not have known anything about retroviruses and would have been literally clueless in trying to understand what was happening when HIV struck, and health care epidemic will place a severe burden on the health care system and the reserve capacities as needed.

I'll take any questions, thank you for your time.

MS. ABRAMS: Thank you very much, Dr. States. If there's anyone else who wants to speak, please see Elizabeth for a blue card. If there's no one further, our final speaker will be Dr. LeRoy Fulmer, who's assistant superintendent of the Waynesville R-6 School District.

MR. FULMER: Good morning. I welcome the opportunity to address this Commission, and I wish to thank you for affording me the opportunity to do so. I realize you have put in a long morning, and I will keep my remarks brief and short.

I commend you for having the foresight to bring together business and the government to develop a plan to protect the critical infrastructure and information system. Within individual corporations of the private sector, there has already been extensive research into this problem. I would encourage you to utilize the existing R&D in this field and extrapolate from those programs a solution to this problem.

But within that solution, one component should be the education of our youth as to the vital importance of the safe, uninterrupted operation of our critical infrastructure and the role it plays in the daily operation of their life. In an earlier Commission meeting, U.S. Attorney for the Northern District of Georgia Kent Alexander submitted eight suggestions for your consideration. The fifth suggestion was educate our youth.

As human beings, we sometimes get to feeling a little bit superior. We make plans, we conduct business, and we go on with our life with a certain knowledge that we are firmly in control. It's just about that time, however, an unforeseen problem strikes, and we find out how easily our plans, our meetings and our businesses go by the boards as we find ourselves engulfed in chaos. It is as if we have forgotten the basics, and those basics assert themselves and refuse to be forgotten or ignored.

So, too, when dealing with the important issue of infrastructure protection, we tend to forget another basic. We read reports, we write legislation, we calculate budgets, and we tend to forget that neither reading, nor writing, nor calculating could take place if it were not for educators who taught us these skills. Somewhere along the line, we sat in classrooms, we mastered the complexities of reading, we conquered the subtleties of writing, and we learned to cope with the enigmas of math. We do not do this on our own, but we accomplish these life skills with the help and patience of educators. Now we must tackle the intricacies of the problems that the new technology has presented us.

Again, I suggest to you that one solution lies in the education of our children. They must be educated to understand the importance of not disrupting or disabling the critical infrastructure and information system. If we are to solve this problem and meet the challenges of our age, it will be through education that we succeed. Education is, indeed, the most important aspect of

life. Without it, there is nothing, with it, all things are possible. I thank you very much for your time, and I wish you success in your endeavor. Are there any questions?

MR. KEYES: Do I understand correctly that the thrust of your recommendation has two phases, one of which is sort of ethics oriented?

MR. FULMER: Yes.

MR. KEYES: In view of the ethics of the Internet and so forth, and the other is the infrastructure of the educational system itself.

MR. FULMER: Yes. I think in earlier Commission meetings they talked about the fact, or the talk was centered around that past interruptions in the system by people have resulted in comments like, "Well, you know, so I got caught," or, "You know, I got caught, what's the big deal?" And I don't think they understand just how critical this is to the lives of every citizen in the United States, and I think we need to address that aspect.

MR. KEYES: Thank you.

MS. ABRAMS: Thank you very much, Dr. Fulmer. This concludes our public testimony today, I want to thank everyone for your participation in the work of the President's Commission, and I'd like now to invite Chairman Marsh to offer any concluding remarks.

CHAIRMAN MARSH: Well, it's been a long morning for you all to sit here and listen, but we think it's a subject of vital importance to our country, and we are diligently attempting to come up with a reasonable and collaborative plan, public and private, that we can recommend to the President, and your participation and contribution to that is much, much appreciated. Thank you.

(At this point the hearing was concluded.)