

# THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION



## PUBLIC MEETING

BOSTON, MASSACHUSETTS

FRIDAY, JUNE 6, 1997

A transcript of a public meeting of the President's Commission on Critical Infrastructure Protection (PCCIP), held in the City Council Chambers of the Boston City Hall in Boston, Massachusetts. Commencing on Friday, June 6, 1997 at 10:10 a.m. Present for the PCCIP were the following persons.

Robert T. Marsh, Chairman  
Stevan Mitchell, Commissioner  
Thomas Falvey, Commissioner  
Irwin Pikus, Commissioner

William Harris, Commissioner  
Mary Culnan, Commissioner  
Paul Rodgers, Commissioner  
Nancy Wong, Commissioner

LIST OF SPEAKERS

MS. ABRAMS ..... 1  
MAYOR THOMAS MENINO ..... 1  
CHAIRMAN ROBERT T. MARSH ..... 2  
MR. STEPHEN HEYMANN ..... 5  
DEPUTY SUPERINTENDENT DONALD DEVINE ..... 7  
COMMISSIONER MARTIN PIERCE, JR. .... 10  
CHIEF KEVIN MacCURTAIN ..... 11  
MR. ARMEN DER MARDEROSIAN ..... 13  
MS. BARBARA FARRELL ..... 16  
MR. LOUIS RANA ..... 18  
MR. DAVID LUCHT ..... 21  
DR. WILLIAM MUNN ..... 23  
MR. ROBERT CURRAN ..... 25  
MR. PAUL LaSHOTA ..... 29  
DR. LAWRENCE MOTTLEY ..... 31  
MR. IANG JEON ..... 33  
DR. MOHAMMAD NOORI ..... 36  
MS. DIANE MODICA ..... 39  
MS. EILEEN RUDDEN ..... 42  
MR. DANIEL SHIMSHAK ..... 45  
MR. EDWARD McGANN ..... 48  
MAJOR GREGORY RATTRAY ..... 50  
MR. JAMES NICKERSON ..... 54  
MR. RAYMOND McCABE ..... 57  
MS. ROBERTA CROCE ..... 59  
MR. BENJAMIN TARTAGLIA ..... 62

## PROCEEDINGS

MODERATOR ABRAMS: I am Janet Abrams, and I am the White House liaison for the President's Commission on Critical Infrastructure Protection. I'd like to welcome all of you to the Boston Public Meeting of the Commission. I'll be moderating today's proceedings. This is the fourth in a series of regional discussions being convened by the President's Commission. Our first was held in Los Angeles in March. We were in Atlanta in April, Houston in May, and today, we're very honored to be here in Boston. I'd like to begin by thanking our host for this visit, Mayor Thomas Menino. Mayor Menino has provided important leadership to the City of Boston in the area of critical infrastructure. He's responsible for increasing the use of computer technology in the schools, in City Hall, throughout the libraries and community centers, and he is also praised for his leadership in updating the City's Emergency Response Planning.

We thank, Mayor Menino. Thank you for your active interest in the work of the Commission and for your hospitality here today. I'd like to invite you to officially open the proceedings.

MAYOR MENINO: Thank you very much, Ms. Abrams, and good morning to all of you. Commissioner Marsh, it's great to have you here even though you had technical difficulties in getting here. We'll investigate the airlines next.

Members of the President's Commission, it's a pleasure to have you all in Boston for this very important hearing. We are honored you have chosen Boston as one of the five cities to study the security of our critical infrastructure. It is especially fitting that we discuss these issues this week, for the nation's attention has been turned to the tragic events in Oklahoma City. Although we have not faced a crises even close to that horrible bombing, it would be not easy to think that we are immune to such terrorism or any other tragedy that other cities have faced.

I'm proud of our efforts to coordinate police, fire and EMS with a Boston Emergency Management Agency and other city departments, so that we are better prepared to handle an emergency. We have worked closely with the state and Federal officials on urban search and rescue and other situations that demand a prompt, efficiency response. In fact, just last week, we were proud to be one of the first cities to undergo an assessment by the U.S. Army Domestic Preparedness Office. The assessment team was so impressed with our approach, that will serve as a model for other cities nationwide. Most people wouldn't think of Boston as a potential earthquake site, but, in fact, we are more vulnerable than you might imagine. Fortunately, we are

prepared, as evidenced by our ranking as the No. 1 eastern city for earthquake preparedness. We are a Federal Regional Center, a state capital and the hub of the region's economy. Only a handful of cities meet that criteria. Our reputation as an international center from finance, tourism and technology make us potentially vulnerable to acts of terrorism. As we continue to make progress in these areas, we have responsibility to proceed with caution and foresight so the residents, visitors and businesses are protected for harm.

I want to thank you, Commissioner, for all that you are doing to raise the nation's awareness of these vital issues. Your efforts to bring all sectors of our society together to ensure a safe future provides us with the greatest gift of all, peace of mind. I look forward to continuing our work together so we can all live without fear.

Thank you very much for having me this morning. Thank you and good luck.

MODERATOR ABRAMS: Thank you, Mr. Mayor. I'd now like to introduce to you the members of the President's Commission who are present with us today. By executive order, the group is a mix of individuals representing both private industry and government.

After the introduction, Chairman Tom Marsh will give a brief overview of the work of the Commission and then public testimony will begin. First Chairman Marsh is at the center. Tom Marsh is an executive in the aerospace industry. He has served on the boards of numerous technology companies and was the chief executive officer of the Thiokol Corporation. Mr. Marsh is a retired Four-Star Air Force General.

Now, moving along, beginning with Mr. Stevan Mitchell, our Commissioner from the Department of Justice; Mr. Tom Falvey from the Department of Transportation; Dr. Irv Pikus, Department of Commerce; Dr. Bill Harris, Commissioner from the transportation industry, most recently the Texas Transportation Institute, with extensive experience in intelligent transportation systems, railroads and other modes; Dr. Mary Culnan, professor in the School of Business at Georgetown University; Mr. Paul Rodgers, the former Executive Director of the National Association of the Regulatory Utility Commissioners; and Ms. Nancy Wong, who comes to the Commission from Pacific Gas and Electric Company.

I'd like now to invite Chairman Marsh to give you an overview on the work of the Commission.

CHAIRMAN MARSH: Thank you, Mayor Menino. We appreciate very much your hosting our affair here today. It's a pleasure to be in Boston this morning with all of you, and as you

heard, my name is Tom Marsh. I'm Chairman of the President's Commission on Critical Infrastructure Protection, and 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, for that matter, do to protect these vital systems.

The Commission was created last July the 15<sup>th</sup> 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 implementation strategy for protecting the nation's critical infrastructures and assuring their continued operation.

So what are the critical infrastructures 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 a 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 the issue before a serious problem develops. Many companies, such as utilities, are very familiar with natural hazards. Those of you living here in Massachusetts and other parts of the Northeast are very familiar with such hazards, including blizzards and other severe storms.

Now, this Commission will not stop such 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 manmade.

Technology has created an interconnected world, but each connection creates new exposures and risks. Companies are becoming increasingly vulnerable to theft, unscrupulous competitors, malicious hackers, insider cyber attacks and 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 the critical infrastructures, identify relevant legal and policy issues and assess how they should be addressed, recommend to the President a national policy and implementation strategy for protecting critical infrastructures and propose any necessary statutory or regulatory changes. I want to emphasize that cooperation and collaboration between the public and private sectors is absolutely essential to the Commission's 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. Together, the public and private sectors can develop common solutions to common problems and secure America's future, but we need your help. We need your ideas, and we need your participation. We need everyone's best thinking up-front. So I encourage and welcome your input. That's why we're here today, to listen, and that's the only way we will find solutions that work for everyone.

So again we appreciate very much you being here today. We are especially grateful to Mayor Menino for taking the time to be here, and we look forward to hearing what you have to say. Furthermore, should you wish to talk with 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> —*Ed.*]. Thank you, all, very much.

MODERATOR ABRAMS: Thank you, Chairman Marsh. Before we move on to the public testimony, I need to offer a note about time. We have a very full program this morning, and my job is to encourage all of us to keep to the schedule. Each presenter has been asked to limit his or her remarks to eight minutes, and I will be watching the job. That's my job, and when you hit the seven-minute mark, I will be waving this nice little sign in front of the speaker as a subtle

reminder it's about time for you to wrap up your remarks. And in eight minutes, I'll be indicating that your time is up. Please know that whatever you submit in writing to the Commission will be included in full in the official record of the Commission, and finally, if anyone here would like to address the Commission this morning and has not filled out this card—and some of you may have come to a small event before this meeting and have not yet filled out the card—please do so, so that we can have put into the proper order of presenters.

We're ready to beginning, and our first presenter is Mr. Stephen Heymann, Deputy Chief of the Criminal Division, U.S. Attorney's Office, District of the Massachusetts.

MR. HEYMANN: Thank you, Mr. Chairman, ladies and gentlemen of the Commission. Within a small radius of where you're hearing testimony today, there are computer networks guarding, quite literally, hundreds of billions of dollars at financial institutions, such as Fidelity Investments, telecommunication networks driven by computer networks, which provide the infrastructure for approximately four million people who live in this immediate area and the businesses and computer networks that are now at academic institutions, such as Harvard and MIT and corporations such as Raytheon and Draper Labs. containing state-of-the-art research, both civilian and industrial.

In contrast to these overwhelming demands, they're presently very limited local resources within Federal law enforcement agencies to conduct investigations of intrusions in the computer networks, even ones operating on such common multi-user platforms as UNIX. Up-front, does that mean that the infrastructure in this area is helplessly vulnerable? No, it does not. We have built important relationships with industry, both locally and nationally, and where necessary, we can draw on pockets of expertise. The FBI, for example, has pockets of expertise in New York presently, San Francisco, Washington, D.C., and is planning them elsewhere, but as you would expect when the U.S. attorneys from the 93 and 94 districts in the 50 states are all drawing on what are quite literally are only tens of law enforcement experts, the demand is overwhelming. It forces us on a constant basis right now to do a dangerous triage.

And I want to give you an example from one of my own cases as to why that triage is dangerous, and it's actually a case that's in today's *Boston Herald*. When that case came to our office, what we knew was that someone was breaking into military and academic research sites across the country, primarily on the West Coast. With that information, do you draw, do you tap a significant portion of those limited resources to conduct your investigation, or do you allow the

activity simply to continue? You're struck with that information. Your initial instinct is these are bad sites. It could be spies, military, political or economic, but the same targets are the targets of hackers, the 14-year-old kids that the Chairman mentioned, who just go into plant flags.

At the same time, unlike stealing a computer laptop, stealing a file means just means copying it. You can't tell whether theft is going on a lot of the time. So you're stuck in a position unable to triage with quite limited resources, where if you don't do the investigation, you may well be allowing military or economic spies to steal or damage or obtain the ability to damage major networks. On the other hand, if you invest literally tens or hundreds of thousands of dollars in valuable manpower, it may only turn out to be a 14 year old.

Postponing the investigation is simply not practical in this area, unlike for securities fraud, for example. Not only are the assets that could be destroyed or could be stolen very fragile, the continuously falling price in computers exemplifies this and computer technology, but also with the kind of case that you can only investigate right then and there, you have to be able to track back the attacker, track back the intruder and put their manpower to it.

So is the answer simply training more people? Well, I think I can say, as a prosecutor, you can train us very quickly, because all we need to know is what words to speak, what questions to ask. We can learn that in two weeks, but you can't train investigators in two weeks. They need to be genuine experts. So my first and strongest point to the Commission is that, to protect our critical infrastructures, we must have our own investigative infrastructure in place, and the cornerstones of that infrastructure will always be investigators. We need an aggressive program to hire the people with the critical expertise, not just give people two weeks' worth of training that allows them to use a cookbook program, but to hire the people with the years of academic background that enable them to understand how complex networks work and how to follow the very fragile trails through those networks that lead to perpetrators, and that means additional funding, earmarked to pay salaries that are competitive with industry and that will prepare—will invite an alternative career.

The second major change—and I really view these as nuts and bolts of one that could have a dramatic impact on the ability on law enforcement to do its job, to track down attackers and thus prevent future attacks—are procedural changes. Right now, our procedural law, our law that really just sets up where and when you can apply for search warrants, where and when you can apply for electronic surveillance orders, not what the substantive limits are, what the limits on

when the government can do it, but simply physically do you have to go into this building or that building to make the application, require the government to make the application where the search is taking place. Well, when the search was to go into somebody's house or into somebody's building or into somebody's file cabinet, that made a lot of sense, but on an electronic network, where those boundaries don't exist, it provides no additional protection, no additional civil rights protection to citizens and, in fact, limits the government a great deal. I submit that we need to change those so that we can move around; we can obtain in one location the necessary warrants to do searches and move as quickly as the perpetrator's move.

Similarly, on the international level, we need to get in place multilateral accords that allow prosecutors to pick up the phone and investigators to pick up the phone and get the help of their counterparts in foreign countries, not again to allow foreign countries to conduct searches here or us to conduct them in foreign countries, but rather so that we don't have to work through letters, which takes months or years, mutual legal assistance treaties, which take weeks or months, all to simply track down who's on the telephone at your Internet service provider that's attacking us right now. Those simple changes, all procedural, along with the additional manpower, will dramatically increase our effectiveness.

Thank you very much for your time.

MODERATOR ABRAMS: Thank you very much. Our next presenter will be Mr. Donald Devine, Deputy Superintendent, Boston Police Department.

MR. DEVINE: Thank you, Chairman Marsh and members of the Committee, for this opportunity to testify on this important subject of infrastructure protection. My name is Deputy Superintendent Donald Devine, the Boston Police Department. I am Assistant Chief in the Bureau of Field Services, which is responsible for all the sworn uniformed officers on the department, and within our bureau, we have the telecommunications center of the operations center, the E-911 unit, all of the patrol divisions throughout the city, and we also have a specialized operation division, which includes the explosive ordinance units, entry and apprehension personnel, the SWAT team, the motorcycle unit, the mounted unit, the K-9 unit and so on.

Every disastrous situation harbors a threat to the general public, the emergency service providers, public utilities and physical distributors of goods and services. It is quite conceivable now as a result of new levels of technology sophistication that a threat may not be immediately apparent, such as the aftereffects of biological or chemical releases or disruption of sensitive

communications directing response effort of public safety personnel or computer crimes suffered by corporations, financial institutions, government agencies or universities.

Let me present some interesting facts about Boston. We have 36 foreign consulates, 28 institutions of higher learning, 28 major hospitals, two liquid natural gas facilities, two major rail yards, thousands of research laboratories, numerous financial institutions and numerous Federal, state and city buildings. These structures and facilities offer very attractive target opportunities that are located right here in the city. They do not, by themselves, represent the true threat level. Within the larger outlying Metropolitan Boston area, the number of high-risk locations increase significantly.

Heavy reliance on telecommunication and computer technology has increased within the Boston Police Department and with it the increased vulnerability, not only from the terrorist community, but from persons who delight in circumventing computer security in order to leave his mark. These acts create a disruption which jeopardizes either the database or the entire computer system.

Attacks such as these are unfortunately no longer in the realm of pure fiction. Very few computers are of the stand-alone type, and the telecommunication links are subject to and vulnerable to interruption and interference. Our telecommunication, E-911 system: In July of '97, a new Computer Aided Dispatch System was installed in Boston Police Headquarters. The system has a primary and backup system located at headquarters and another secure facility within the city. In the event of failure of the primary system, the backup system will automatically take over. To ensure continuous electrical power, all of the computer equipment receives power from an uninterrupted power supply that will act as a battery backup in the event of power failure until normal electrical power is restored. These communication lines have redundant separate feeds and redundant access points into the building.

There are some critical concerns. In the event that a terrorist or critical infrastructure interruption hits the city, sudden and dramatic impacts on the telecommunications system may require the immediate activation on many different types of telecommunication resources, including command posts, two-way radio systems, faxes and interfacing local and national databases. A very important concern, if the infrastructure is the affected, is that sensitive communications used by local agencies, including Boston, have to be secured from unauthorized interception. Therefore, there would be little time for communication personnel to assemble additional equipment

that would support on-scene personnel for sustained community time. The necessary equipment: Employment and activation of the on-scene command post may be required. For example, in East Boston, where local and central communication may be disrupted, unavailable or unusable, essential personnel would be available to respond to public safety concerns. Therefore, satellite capability as a replacement to the NYNEX lines or cellular system may be necessary, as well as stand-alone repeaters, repeater amplifiers and various electronic equipment. Training procedures and equipment for telecommunication personnel are necessary to ensure that during a catastrophic emergency, when there will be a lot of confusion and urgency, they can perform their duties safely and with a minimal direction.

Computer Technology: Over the past several years the Boston Police Department has introduced computer technology to increase efficiency and to provide the required tools to increase public safety within the city. Technology has been integrated into previously expensive tasks in order to redeploy officers in support of neighborhood policing, as well as provide the required information for crime analysis and increased officer safety.

One outstanding example of how important the upgrading and expansion of Frame Related Technology is the state-of-the-art IDE Imaging and Booking System. This is the most advanced identification technology in law enforcement, and Boston is presently the only police department in the country certified by the FBI to electronically transmit live and scanned images of fingerprints and descriptor information to the FBI for criminal information. The return response time for this critical information has been reduced from several weeks to within 2 to 24 hours.

The future concerns that we have with the growing number of requests in connection with outside agencies and data sources, such as the Internet, our security concerns will grow considerably. The most currently utilized concept in the computer industry is the construction of a fire wall and a router that acts as a traffic cop to direct requests to the correct system for maintaining the direct desired level of control. The traffic cop simply acts as a barrier to grant access to authorized personnel and to deny access to those who are not authorized.

To this end, the command personnel believe that the fight against the attacks on the city's infrastructure is best accomplished through developing preventive and intervention strategies, specialized training and education, increased communication and coordination with other agencies, both public and private. To achieve the goal in counteracting a threat to our infrastructure, a

partnership provides a level of service and safety beyond the aggregate of any individual entity's contribution.

Thank you very much for allowing me to make the presentation today, and it is extremely important that we establish a strong working relationship with other governmental agencies and the private sector to address this critical problem. Thank you.

MODERATOR ABRAMS: Thank you very much. I'd like now to call upon two representatives of the Boston Fire Department, Martin Pierce, Jr., Commissioner, and also Kevin MacCurtain, Chief of Operations.

MR. PIERCE: Good morning, Mr. Marsh and members of the Commission that are here in Boston. I welcome you, and I certainly am grateful for having this opportunity to give you our views and perspectives on this issue.

Boston's worldwide notoriety, population, and housing density and unique infrastructure makes us the perfect target for a terrorist action. When I look back two years ago to the scenes of Oklahoma, which certainly we are refocusing on now in the newspapers with the trial in Denver and so on, it brings back memories, sad memories, of a disaster, a terrorist act that took place there.

I want to emphasize the need for Federal assistance in preparing local fire and emergency service personnel to handle chemical, nuclear and biological incidents. The needs of first responders must remain at the forefront of Federal terrorism response planning. The local fire and rescue personnel need the military training, high-tech equipment and the personal protective equipment for this type of incident. Local authorities still lack the resources to provide adequate protection.

I recently attended a Metro Chiefs Conference in Minnesota, where the chiefs of all the major cities in the country that protect 80 percent of the population met to discuss issues affecting their respective departments. It was agreed that local authorities, the first responders, still lack the resources to provide adequate protection in the event of a chemical, a biological or terrorist incident.

Last year President Clinton signed an anti-terrorism law, which was widely supported in Congress, to provide \$1 billion to local law enforcement agencies but not fire and emergency response units. The act also required the U.S. Government to train how to respond to terrorism.

The fire service, I feel, at times is being ignored when the funding is appropriated. The local fire departments and EMS personnel and police will be the first to respond and arrive at the scene of a chemical or biological incident. I agree with Congressman Curt Weldon, the Republican out of Pennsylvania, that the Pentagon's most up-to-date equipment from bomb and chemical detection devices, to biological weapons, protective masks and suits must be placed into the hands of fire fighters and EMTs, who are the first call to emergency scenes.

All of the funding in the world will not do any person in this country any good if training and equipment are not delivered to those people who need it the most. All public safety agencies must be trained to the operational level.

I thank you for allowing me this time, and the next speaker, I believe, is Chief MacCurtain, my Chief of Operations with the Boston Fire Department. Also present with me today is the Deputy Fire Chief in charge of the Emergency Management Division, John D. White. Thank you again.

CHIEF MacCURTAIN: Thank you, General Marsh, ladies and gentlemen. We live in an open society. We are free to travel from city to city and state to state. This freedom that we all enjoy does not come without a price. We have recently been reminded of how easily an incident, such as the World Trade Center or the Oklahoma City bombing, can occur from actions of one or more terrorists. Terrorism can come in many different forms.

One thing is certain in this world that we live in; it's becoming easier for a terrorist to strike. Our infrastructure is vulnerable. We have an obligation to protect this city's infrastructure. This city's first line of defense is the emergency service of the fire, police and EMS. In many bombings in Europe and recently in Atlanta, Georgia, the first responders were the target for the secondary device.

The fire service in the City of Boston is a well-trained, well-disciplined, semi-military organization that operates under a nationally-recognized incident command system. We are Boston's small army that provides the first line of defense after an incident occurs. Although we are very familiar with handling emergencies, such as multiple-alarm fires, weather-related storms and provide an array of emergency services, our goal is to protect life and reduce property damage. We are ready to take on any natural disaster that may occur and then restore order to a chaotic incident. In doing so, we rely quite heavily on the infrastructure support system. It's imperative that that system be there to support our efforts. The failure of our city's water supply from the

Quabin Reservoir, which supplies water to the entire Metropolitan Boston, area over three million people, would seriously impact in our ability to control a major fire in this city. A eight-alarm fire that's currently burning in the City of Chelsea next door to us would probably continue to spread to our borders had we had a problem with the Quabin Reservoir, the failure of our telecommunications, computers, the 911 system and digitized communications, which affect our command and control capabilities. Our message to Washington as the nation's first line of defense, the American fire service is not prepared or equipped to handle a nuclear, chemical, or biological incident. We know we'll be the first on the scene, but without the needed training and equipment, many of our first responders will become victims themselves.

At a recent New York City multi-agency drill simulating a biological incident in the subway system, such as the one that occurred in Tokyo on March 20th, 1995, it was estimated that the first 100 fire fighters who were improperly equipped for this type of incident would have themselves become victims. Boston is no different, and without needed training and equipment, the first responders will be listed on the casualty list.

The complexity of the interdependency of the infrastructure system and the risk of simultaneous failure of more than one system makes it all the more reason to properly train and equip your most important infrastructure, the men and women in the fire service, the first line of defense. As the nation's military has been downsized, so too has the fire service in cities across this country. The strong mutual aid system we once enjoyed, which includes the 34 cities and towns in the Metropolitan Boston area, is slowly eroding. Communities around us have been closing fire stations and reducing staffing, putting more strain on our mutual aid pact and a heavy reliance on the core city.

The fire service role in a nuclear/biological incident is not prevention. However, after the incident occurs, a well-planned, multi-agency, defensive strategy under the incident command system can save hundreds of lives, reduce property damage and restore infrastructure systems. We need to be able to guarantee our ability to maintain command and control over the most chaotic incidents.

We need help from the Federal Government, training, equipment and funding that's specifically earmarked for the fire service. The Federal Government has consistently found money for police services and rightfully so. When we talk about the security of infrastructures and terrorism, I'm sure funding will be made available for police departments, but all too frequently

the fire service is left out of the loop, not only in funding but also in information that could be critical to first responders. When the FBI or the CIA gather information of a possible threat, they quickly call the local police chief. The fire chief, whose men and women will be putting their lives on the line, are typically the last to know.

Boston currently has the largest construction projects in the country. Depression of the Central Artery, Third Harbor Tunnel, Mass. Water Resources Sewerage Treatment Plant creates nearly 30 miles of underground tunnels. Because of these projects, we have been doing extensive training, using specialized equipment in tunnel rescue, trench rescue and confined space and collapse rescue. We have developed a well-trained urban search and rescue team with actual experience in these specialized rescue techniques. There are over 200 members of Boston's urban search and rescue team consisting of over a hundred fire fighters, 37 Boston EMS, paramedics and EMTs, 17 Boston K-9 officers, building engineers, inspectional services, as well as doctors and nurses from St. Elizabeth's Hospital. As always, Boston's bravest stands ready.

However, our urban search and rescue team has not been funded or recognized by FEMA. We have been trained to the FEMA standards; yet funding is lacking from the Federal level. Our message shall include funding for training and equipment and establishment of a go team, a team that would consist of two or more fire fighters from the metropolitan cities to be sent to the scene of a major incident, to learn the lessons from that incident, bring them back and retrain our staff. Thank you for listening.

MODERATOR ABRAMS: Thank you very much, gentlemen. I'd now like to call Armen Der Marderosian, Executive Vice-President of the GTE, and I'd also like to begin to identify who's on deck after the speaker that I am calling. It's Barbara Farrell of Bay State Medical Center, Manager of Ambulatory Grants.

MR. DER MARDEROSIAN: Good morning, General Marsh, Commissioners, all the invited and submitting guests.

We've talked a lot this morning about information warfare, economic warfare and information systems, and I think that's an extremely important. However, I think there's a much more important and immediate problem that is just now starting to get the attention that its deserved for the last five years. Many of you have probably heard of the problems with computers and software's nomenclature, the year 2,000 problem. That is, in fact, I think the single most and

largest threat to the United States infrastructure, whether foreign, domestics, governmental or civilian.

I won't go into the details of the problem, just to say that it has been around for an awful long time, should have been receiving attention for the last 15 years. In fact, it's only gotten attention from techies really for the last 10 to 15 years. It's now again starting to get attention from management in companies and the government, and for the most part, people look at the problem and say, oh, that's just a software problem; we ought to be able to fix that real easy; don't worry about it; it's the information and technology programmers who are trying to make it a big deal so that we can, in fact, continue to maintain the levels of manpower to solve the problem.

That's being debunked daily. I'll give you two pieces of evidence. First, *Newsweek* just recently had an article on the subject, stating its severity, but the most compelling piece of evidence, of which nobody can have any doubt as to how serious this problem is, is the in current version of the *ABA Journal*, the front page, "The year 2,000 booming crash." In the year 2,000, they talk about how they are going to have billions and billions of dollars worth of lawsuits against companies, directors, governments, employees, whoever, because of the damages that are going to be caused by the year 2,000 problem, and when trial lawyers start to smell trouble, you know it's a real problem. Several very respected consulting companies throughout the United States, Gartner Group being one, estimates the problem worldwide will be \$600 billion. That's more than all the money spent today in developing and maintaining information systems. The U.S. is going to be well over 300 million.

The problem is going to be centered mostly in those organizations that use large computer-based interactive programs, many of which use dates, whether it's for Social Security, IRS, telephone billing, telephone conveyance, insurance companies, whatever. They're going to be the hardest hit, but everybody gets hit by this, because every one of you deals with one of these groups, telephone company, government, et cetera.

For the most part, telephone companies have been working this problem maybe for the last year or two. They're working hard on the problem, probably will solve the problem in time so that there won't be catastrophes. There will be trouble. There won't be catastrophes, at least to the individual telephone companies and communication companies. They may, however, be islands unto themselves, because if your neighboring telephone companies or communication

providers do not solve the problem and solve it the same way that you solve it, in fact, you won't be able to communicate. Worse, their method of solution will become a virus in your network if you start to talk to them. That is a major, major problem getting all these companies to work together to come up with the same solutions, using the same software.

Banks have been doing a fairly good job. They are also working the problem, as are insurance companies, but again, everybody interacts with them so you have to make sure they're solving the problem the same way you are. Every financial transaction, whether it be major, bank to bank, worldwide, whatever, has to have the same set of algorithms so that people can talk to each other.

Unfortunately, at least in my estimation, the Federal Government and most state and local governments are not solving this problem well at all. That's probably the biggest risk we have as a nation. There has been some attention paid to it. Social Security has been working the problem for a long time. IRS has been working it. Some others have been working it, but I have been to talk to a lot of these people. GTE was the first major company to start a program, an active program, and we've been talking to government and other companies trying to get interaction so that we'll make sure that our systems are all solved the same way. In talking to the government or any number of other organizations, I have come to the conclusion that we are not going to fix the problem. The problem will not be fixed by the year 2,000. It is so large, so pervasive, and it is caught up in bureaucracy, budgeting. I mean, they're talking \$2 billion to fix something that is easily 30 to 50 billion worth of activity. Without the budgets, without the attention, without the tiger teams to fix it, it's not going to happen. The only solution is we're going to have to legislate the year 1999 all over again. That may, in fact, be the only solution. I don't know how one does it, because the rest of the world is silently waiting for the U.S. to solve the problem. They're going to take our solutions and introduce them into their systems.

Two problems, one, if we solve the problem it will be late in 1999. You actually have to solve it by the end of 1998, so you've got 1999 to do all your interactive and regressive testing, but that's not going to happen. We're lucky if we solve them by mid-1999. That means there's no time to integrate them into European and Asian companies. Worse yet, most of the solutions are unique, because we're talking about very old systems using arcane and less than well-documented systems. So they won't be usable in any event.

It's a major problem. I wanted to bring it to your attention. I don't think it's getting enough attention, either in the domestic, civil or state and Federal Government as it should, and I end with what I started with, the *ABA Journal*. Trial lawyers are starting to circle overhead, and that means we're all going to have fun. Thank you very much.

MODERATOR ABRAMS: Thank you very much, and now, Miss Farrell of Bay State Medical Center. And then Louis Rana will be next, Consolidated Edison Company of New York.

MS. FARRELL: Good morning. Thank you for this opportunity to bring you a perspective that I hope will influence the way you view the changes being thrust upon the citizens by managed health care and the educational policy of inclusion which will come directly from your ABA, your Americans With Disabilities.

In the past, technology-dependent citizens were in a hospital until they were able to maintain life without reliance on the infrastructures we're discussing today. This means that the plan that centers on the hospital will no longer be sufficient. Today, our schools house children who depend on technology for life. The state has begun emergency medical services planning for children, and the group met last week in Framingham with health professionals working in the schools. And I think that's an important thing.

We need to recognize that people still have a role within this technology piece that we're talking about, and that's the people that the fire chief was talking about, all of the training that needs to happen to get people up to speed.

At the same time, I'm talking about children in schools with technology dependency, be it life-support systems. You wouldn't believe what used to be in the ICU is now in a classroom. At the same time we're looking at this, we're looking at aging infrastructures, and I look back to three years ago. I think it was three years ago on the second day of school in Springfield when a major water main broke, an aging water main, and what we had to do that day with children and what went on for several days with bottled water and all of that sort of thing, not life threatening, but certainly a preventable occurrence if we begin to look at what are those aging infrastructures that create emergencies.

Just last week, I heard that the electrical companies in Western Mass. were beginning to talk to hospitals about what's going to happen this summer with all of the nuclear plants down and looking at what those occurrences may be, because we're not sure that we have the electricity

necessary when all of the high usage clicks in for the air conditioning, et cetera. And that's what struck me, that we immediately go to the big places where we traditionally think, and I'm asking you to think a little less traditionally and to look at more what's happening, not just in where the bottom line is affected, but where our resources for the future are affected.

Every school houses anywhere from 500 to 2,000 to 3,000 of our best resources, and we need to begin to think about how do we make sure in this changing day and age we have professionals, health professionals, available and that we really think about communications systems within those schools. I think we're all familiar with those scratchy overhead speakers that no one could understand in the morning anyway, and we're all very familiar with the fire drills which everyone participates in. How do we make those be more effective? How do we use those opportunities that already exist to keep the level of awareness and the level of learning and the level of safety for the children? We know—and I spoke with our chief of emergency before I came yesterday afternoon. He says the trauma system is working great. The Enhanced 911 is doing its job, and so I still say that we need to maintain our vigilance and respond where our children are.

One of the things that is happening in our schools that could be very helpful is if you look at not only at what's happening at the level of the classroom and what the restrictions the children have, but look at all the technology that's coming into those schools, the distance learning that's happening, the ability of talking back and forth, having discussions with children in Washington, D.C., and children in New York and children in Boston all at the same time, with our health links that happened over this past two years with the Massachusetts Corporation for Educational Telecommunications. Those are opportunities to get ourselves out of the box of thinking of how training can happen, how lessons can be learned down at a level, how we can take real lessons learned from how we responded to an emergency and teach those things across the country. If there were some really good things to have learned from an emergency in a Boston high school, can we then bring those, what we learned from doing those things, out to other areas that may not have ever had to deal with a gas leak or some kind of a spill? In fact, one wonders why we're all here in person, although it's very nice to be in person, when we do have these wonderful opportunities of technology to be able to interact with distances between us.

And just one other thought that I bring to you from the perspective of the hospital and, that is, in terms of information systems and the medical record online. There's a great deal of need to protect the confidentiality of the person whose medical record is online. At the same time, there's

a great deal of desire with rural physicians and rural hospitals to be able to share information quickly, efficiently, to be able to get the kind of information that an emergency medical services person needs to treat someone properly, and that becomes a high priority as hospitals more and more are moving to this electronic medical record. Thank you very much.

MODERATOR ABRAMS: Thank you, Miss. Farrell. Our next speaker will be Mr. Louis Rana from Consolidated Edison, and after Mr. Rana, Mr. David Lucht, the Center for Firesafety Studies at Worcester Polytechnic Institute.

MR. RANA: Good morning, Chairman Marsh, members of the Commission. My name is Lou Rana. I'm the Chief Engineer for the Consolidated Edison Company of New York, and I thank you for giving Con Edison the opportunity to express publicly its support for the work of your Commission and to share some of our concerns and also to give you the benefit of some of our experiences and solutions.

Con Edison supplies electricity to all of New York City, except the Rockaway Peninsula in Queens, and to most of Westchester County. We also supply gas to much of that same territory and to steam in parts of Manhattan. Our three million electric customers, which involves a population of a little over eight million people, are among the most diverse in the nation in every sense of the term, and disruption of power has consequences ranging from financial, to environmental, to health related, to social. The Federal Reserve Bank, the water pollution control plant, the hospital, the nursing home and the small apartment all depend on us for their operations.

Just as our own lives have become more complex and interconnected through technology, whatever, whether it be the local ATM machine or credit cards or surfing the Web, so too have infrastructures become more sophisticated and mutually dependent, including the cascading effect of trouble on one system to another. For example, if, through an accident or a terrorist act, we lose power to the mass transit system, the thousands of people that do things that like processing financial transactions may not get to work. If the financial system in New York suffers, the effects are not merely local.

Con Edison has the best service reliability in the nation, and we must. In a yearly national survey of utilities conducted by the Theodore Barry and Associates Company, we were found to be the most reliable in the country. In 1995, the average utility in the United States had an interruption rate of 1180 customers per thousand. Con Edison's rate for that year was 83 customers per thousand. Reliability means keeping service under adverse conditions, as well as normal

conditions. Those adverse conditions could be caused by man and nature and may affect multiple segments of the infrastructure.

Now, we achieve our reliability level by our system design and also the method we use to operate our system. Most of our distribution system consists of many interconnected networks, and we operate these networks for the loss of any two components. We call that a second contingency design. Now, during non-peak-load periods, we can actually lose more than two components without a problem. Our service territory is relatively small. We serve about an area of 600 square miles, and we have in that infrastructure a systematic development that delivers annually 40 billion kilowatt-hours of electricity, 20 million dekatherms of gas, and 30 billion pounds of steam. The gas and steam systems are, of course, underground and, therefore, less susceptible to accidental or intentional disruption, and being an urban utility means much of our electric system is underground. And that includes 35,000 miles of overhead distribution and transmission wires.

Now, while preparing these comments, I was reading the testimony of Georgia Power's Wayne Dahlke, given at your Atlanta hearing, and of Marcie Edwards from Los Angeles, and I really thought for a few moments that if I changed a few names we could give you basically the same kind of analysis for the Con Ed. system. The fact is that utilities across the country have basically a similar design, and our exposure to acts of terrorism is really also similar.

Like our sister utilities in California and Georgia, we have emergency response plans. We conduct periodic drills. We cooperate with other utilities under a mutual aid agreement, under EEI, Edison Electric Institute, and we also separate our informational computer system from our operational computer systems. We also hire professional hackers to try to break into our cyber infrastructure, and we also have a dedicated full-time department to look after company-wide security in all aspects.

In line with the recognized interdependence of infrastructures, New York City has consolidated broad-based emergency planning under the mayor's Office of Emergency Management. We refer to it as OEM. Con Edison and OEM have developed a very tight partnership to deal with real or potential crises. We have a very defined communication protocol, and we also send representatives to each other's control centers during emergencies and potential emergencies. Now, this cooperation benefits both parties and especially the public, whom we both serve, and I

recommend such private and public reliances to those concerned with protecting the infrastructure.

In our case, in the recent past, earthquakes and brush fires have not been a significant problem for us, but hurricanes and floods has been. By the way, manmade flood is what happens when a large water main breaks in midtown Manhattan, and we have roughly 500 water main breaks a year in New York City. Some of them are little trickles, and others are torrents. One that occurred in the summer of 1983 found and flooded our last below-grade substation. It knocked out power to an eleven square-block area, roughly a thousand customers in midtown Manhattan. It tested our restoration ingenuity in the middle of a labor strike, but this event prompted the company to really examine all the vulnerable facilities in what we call the possible but probable study. We studied train derailments, tidal waves and terrorists, and we devised a degree of risk versus costs-to-eliminate matrix. And we either removed vulnerabilities, or we developed contingency plans. I'd also recommend this approach to all owners of infrastructures as an in-house first step towards protection of facilities.

We certainly support your goals and support the passage of legislation that furthers the protection of the infrastructure. This would include tax incentives or revision to the penal code. We have supplied a detailed response to your questionnaire that was sent out in February, and we also had several discussions with one of your consultants from the Argonne National Laboratories. I hope the information supplied will help you prepare a plan that further enhances the protection of our critical infrastructure.

The electric utility industry is going through a period of almost unprecedented change, as we move from a regulated, vertically integrated monopoly to deregulated, unbundled, competing enterprises. Deregulation of the electric utility industry will necessarily mean giving the public a lot more information about transmission lines routes, capacities and interconnections, information that a terrorist like the World Trade Center bomber could use to impact more than just one building. This is an area that I believe the Commission should pursue with state and Federal regulators. That concludes my remarks. Thank you for giving Con Edison the opportunity to address this Committee.

MODERATOR ABRAMS: Thank you very much, Mr. Rana, and thank you for coming all the way from New York.

Next, Mr. David Lucht of Worcester Polytechnic Institute. Following him, I'll be calling on Dr. Bill Munn of the National Emergency Number Association.

MR. LUCHT: Thank you very much, Mr. Chairman, members of the Commission. Thank you for traveling to New England to give us a chance to share some of our views with you. I'm going to speak about the vulnerability of the American infrastructure to the threat of fire as viewed from the point of view of one who works in the science and engineering community.

To begin, I'd like to give you a little bit of information about Worcester Polytechnic Institute and our capability in the fire safety area. Worcester Polytechnic Institute is located about 40 miles west of here. It's the third oldest private technological university in the United States, and started in 1865, the school has been changing to meet societal needs as they have evolved.

In 1979, WPI created a center for fire safety studies to put intellectual energy into the nation's fire problem, and the school created a first-of-its-kind master's degree program in fire protection engineering. We now enroll about 100 fire protection engineering students in WPI. We have five full-time professors. We've doing fire research for almost 20 years now.

I'm going to base my remarks on about 30 years of experience in the fire safety field, both at Worcester Polytechnic Institute and in several policy positions in government and industry. I think it's fairly clear that the critical infrastructure in communities throughout this country are highly vulnerable to fires. In just a few minutes time, electrical power utilities, telecommunications networks, traffic and rail control centers, energy storage facilities can be crippled well before the best-trained and best-equipped fire department can arrive on the scene and intervene. Even a small fire in a very small computer room can cripple an infrastructure communications network that has both regional and national impact.

I'd also like to mention that the impact on the civilian population, as well as our local infrastructures, is equally significant. The risks of fire for the American population is the highest among all industrialized world countries. Our fire death rate in the United States is five times worse than Switzerland on a per capita basis, three times Japan, 2.7 times West Germany, and twice Sweden. Unlike floods, earthquakes, tornadoes and hurricanes, fires happen every hour of every day, and they're preventable. In the aggregate, the total drain on the U.S. economy is approaching \$130 billion a year. Six years ago, under a grant from the National Science Foundation, I had the privilege of studying fire safety methods in other countries. I wanted to find out why their loss rates are lower than ours. I conducted site visits in particular in the United

Kingdom and Australia. Even though they have loss rates that are well below ours, I found that their national governments today are undertaking aggressive programs to totally reform their fire safety practices. This is in recognition of the fact that modern fire research results offer new opportunities for achieving even higher levels of safety in these countries at less cost.

The idea of reforming fire safety practice in the United States is not entirely new, even though our loss rate is among the worst. In 1983, Dr. Dorothy Simon, who was then Vice-President at AVCO Corporation, testified before the Senate Subcommittee on Science, Technology and Space, stating that fire-related costs of building construction in the United States could be reduced by 40 percent through the use of modern fire technology. Unfortunately, unlike many other governments in the world, our government never mounted an aggressive effort to undertake a program to take advantage of these opportunities.

In 1973, another Presidential Commission, similar to yours, submitted a report to the President of the United States, after holding hearings in five U.S. cities. This Commission was known as the National Commission on Fire Prevention and Control. On Page 1 of its report, it stated, "Appalling, the richest and most technologically advanced nation in the world leads all major industrialized nations in per capita deaths and property loss from fire." This Commission concluded that fire safety is and should remain the state and local responsibility. However, the Fire Commission also emphasized that the Federal Government has a responsibility as well and a role to play in areas like technical and educational assistance, collecting and analyzing information and research and financial assistance.

Mr. Chairman, I would urge that your Commission thoughtfully consider fire as a major threat to the integrity of America's critical infrastructure and to the safety of the population at large. I would urge that your report make sure that the President and the Congress are aware that the critical infrastructure is vulnerable to devastating attack from fire and explosion; that the American public is at higher risk than the citizens of other countries; that the governments of other countries are undertaking aggressive efforts to change the way that they do business to take advantage of higher levels of safety at less cost; that the state and local governments in the private sector are already investing heavily in protecting the public and the critical infrastructure in the United States; that the investment can be made most cost effective through aggressive reforms such as those being taken in other countries; and that it's in the national interest for our Federal Government to help. Specifically, I think of three Federal agencies that could do more to

support and assist state and local governments, as well as the nonprofit, private-sector organizations that help achieve fire safety in America. These agencies would include the United States Fire Administration and FEMA, the National Institutes of Standards and Technology and the Department of Congress and the National Science Foundation.

This concludes my oral remarks. I've submitted more complete commentary for the record. Once again, thank you for traveling to New England and giving some of us the chance to share our views. Thank you.

MODERATOR ABRAMS: Thank you very much. Next we'll hear from Bill Munn of the National Emergency Number Association, and following Dr. Munn, Robert Curran, CIO of PictureTel Corporation.

DR. MUNN: Good morning. My name is Bill Munn. I am the incoming President of the National Emergency Number Association. The people who actually pay my rent are the Tarrant County 911 District, which is headquartered in Forth Worth, Texas, and provides 911 service to about a million and a half people.

The National Emergency Number Association has grown, as has the 911 industry in the United States, particularly with the growth of Enhanced 911 service. In 1985, when I attended my first NENA conference, we had 200 members and nine vendors. This year our membership is passing 5,500, and typically, with every conference, the vendor hall is sold out by the time the current year conference is over.

Now, 911 depends on the public switch telephone network. Typically, when 911 service is lost to a community, it's more likely to be a backhoe, a post hole digger, possibly a lightning strike or simply a mistake on someone's part rather than even a disaster. 911 survived Hurricane Andrew. 911 survived the California earthquakes, but typically, when 911 is overwhelmed, it's the factor of convergence. After the Oklahoma City bombing, the call volume in the 911 center did not return to normal for at least a week, because when people want information, people want to know why the sirens are sounding, they pick up the phone and they call 911. That is the primary impact of a disaster on 911 typically today.

Now, our current emphasis in NENA is on developing the ability to provide contingency plans for 911 systems. My assistant director and I conduct an annual meeting at the conference to teach our members how to do contingency plans. This has become an annual function. We tell them about the need for a plan. We tell them that a plan needs to be all inclusive, because if

there's an element that they leave out of their plan, Mother Nature will find it for them. We tell them that plans need to be distributed. A plan does no good if it's in a captain's desk when he's on vacation and it's actually needed. We point out the story of the San Francisco fire chief who had a comprehensive plan around the turn of the century for use with the water distribution system to control fire in the event of an earthquake. He was killed within the first few minutes of the earthquake. The plan was found in his desk in the rubble of the central fire headquarters after fire had destroyed most of the city. We teach people that the plans need to be tested and changed, and they need to be drilled.

And we do talk about terrorism. Will 911 be a victim of terrorism? Statistically, probably not. The main threat is probably still Bubba and his backhoe, but we point out the fact that a typical terrorist organization's objective is to make the public lose confidence in their government. And what is a more visible sign of government and a citizen's way of accessing emergency assistance from his government than 911. We are very visible. We have intentionally made 911 visible and a part of the American culture, and we have been helped along by Rescue 911. And will 911 eventually be a target somewhere? Probably so.

We also point out things such as the ad I clipped out of Soldier of Fortune Magazine just as a typical example of what we find in a free society, a little advertisement about "C4 - It's a Great Explosive". The problem is you can't buy it at Home Depot, but this ad says that all is not lost; we have a recipe you can use to make it at home with ingredients that you can find at any store. There are over 1,400 publications, brochures, other sources of information that tell the general public how to blow things up, how to disrupt communications, how to kill people. They're out there on the street. This is part of being a free society, but we tell our 911 people their job is not to go home from the conference and begin fighting terrorism; their job is to make their 911 system a hard target. If they have security systems, they need to make sure they're in place and they're followed. They need to totally control anyone who has access to that 911 call center. If they're a commercial member, if they're with the Telephone Company, they need to make sure their plans are effective and they're in place for controlling access to not only the facilities, but to the network and to the database. The database of the 911 system is absolutely crucial to effectively delivering service, emergency service in response to any incident.

Now, over the next few years, the entire way of delivering 911 calls in the United States is going to change. The entire 911 system is going to be replaced over the next four years. What's

driving this is recent FCC rules that will require wireless companies to deliver location to 911 call centers. Now, if wireless communications deliver to location today, we couldn't handle it. 911 centers do not have the capability of providing a graphic display showing the location of a wireless caller. That will change over the next four years, but with that change becomes more dependence on networks, on computers, on advanced intelligence networks, ISDN systems and, of course, more vulnerability along with it.

The implementation of 911 in the United States has been a story of partnerships, partnerships between the telephone companies and the local public safety providers, partnerships between the FCC, the telephone companies, organizations like NENA, and the public safety providers. As President of NENA, my objective this year will be to forge a stronger relationship between NENA and FEMA. FEMA training typically does not include 911. It does not mention 911.

Typically, your 911 leaders locally do not know about emergency planning processes. They are not involved in emergency management. In your typical American city, the emergency management activities are on the fire side of the house; 911 is on the law enforcement side of the house. Typically, there is not adequate communication between the two functions. We need to train 911 professionals across the country how to do emergency planning, how to do contingency planning and how to enact them, and we need to teach the emergency management side of the house that 911 is a resource and an asset and how to protect it. Basically, it's partnerships that have provided 911 services to over 80 percent of the American population, and it will be a series of partnerships that will protect it in the future. Thank you.

MODERATOR ABRAMS: Thank you very much and thanks for coming from Texas. Next, Mr. Robert Curran of PictureTel Corporation, and following Mr. Curran, we'll be hearing from Mr. Paul LaShoto of Bay State Gas.

MR. CURRAN: My name is Robert Curran. I'm the Chief Information Officer of the PictureTel Corporation, and it's a honor for PictureTel and for me to be asked to testify before this Commission. My remarks may differ a little bit today from what you have heard, in that I will probably be talking a little bit more about the adequacy and the dependability of our infrastructure as much to the disaster threats.

PictureTel Corporation is the world's leader in videoconferencing. We have approximately 1,600 employees worldwide, with sales of \$500 million or more in 1996. We operate videoconferencing systems that operate over the digital telephone lines that are part of the public switch

network. We, in fact, helped develop the standard that is now used by the industry for videoconferencing, and recently, we announced and demonstrated products which provide videoconferencing using the IP protocol of the Internet. We have more than 50 percent of the world's market share in videoconferencing, serving several thousand customers, primarily mid- to large-sized customers in education, health care and financial services all across the board. We have sales offices in 37 cities in the United States, more than 60 countries, and of course, our customers use the product worldwide.

We are totally reliant upon telecommunication services. Without them, we would not exist as a corporation. Internally, we use our dependency on e-mail, videoconferencing, the Internet, the World Wide Web, voice mail, which have made us almost completely dependent on them. Each day we, 1,600 employees, send and receive nearly 10,000 external messages over the Internet. We are virtually a paperless society.

To support all of this, I currently operate at PictureTel one of the most sophisticated telecommunication environments in this area. NYNEX has compared it to that of a medium-sized city. We have installed dual SONET rings, which will link our locations to multiple locations of our carriers. We are connected to all of them, and in addition to our own internal requirements, we are managing videoconferencing for some of the world's largest companies, such as Proctor & Gamble, Ford and, of course, Guinness, a good Irish company for Boston. We have in recent years stretched the capacity of these vendors to provide such productivity. Daily in the conduct of our business, we use Internet, IP video, a 5,000 client switch ATM and an internal FDDI ring, an ATM to the desktop. We also operate ATM lines and switches and are conducting significant videoconferencing testing with some of the more advanced Internet providers.

I will not describe for you our backup procedures. They are in what I will supply you in detail. I would like, however, to go directly to some of your concerns, which are the services we receive and provide, reliable, have we ever had to use these plans, and what instigated those incidents. I would like to tell you that the telecommunication services that we receive today from our providers is outstanding. Unfortunately, I cannot. To this point, the ISDN infrastructure, the mainstay of delivering videoconferencing, is spotty in the United States. Unfortunately, our customers are hampered by the fact that carriers, particularly the local telephone companies, have not been able to provide. In addition, the ability to communicate the ISDN between carriers is not always what it should be, and ISDN, interestingly enough, is much more prevalent in Europe,

where the public policy has led to its widespread deployment. We've had multiple power failures. We've had cable cuts both before and after our installation of our SONET ring. A SONET ring, when it's cut, the traffic reverses direction, so that you don't lose service. Our carriers have all had some kind of outage, and to our knowledge, we have had no major security breach. But we have experienced problems with viruses, and what's worse, through nuisance Internet mail activity experienced problems. We have plans of increasing the safety of this network, including the addition of alternate carriers and even more SONET rings to protect it.

What is the role of the business leaders and the government officials in assuring this infrastructure? Well, the President and again the Commission are rightly concerned with protecting the infrastructure in the United States. We should not lose sight of the fact that this is a worldwide economy, and we must—we must, we must, I repeat, review the protection and enhancement of this as a worldwide problem. Today, the United States leads in the development and use of information technology, but this is changing. The world is becoming both more accommodating and more competitive at the same time. The PTTs, like British Telecom with its merger with MCI, and Deutsche France Telecom, et cetera, merging with Sprint, are on their way to creating multinational worldwide corporations that rival the oil companies. These changes may create certain valid concerns about the effect on the United States infrastructure, foreign ownership, et cetera, but I believe the need and, in fact, the necessity for a most robust or more robust dependable and economical worldwide telecommunication infrastructure makes such news inevitable.

What can we do together? We need to ease the export restrictions on equipment technology. I'm sure you've heard this many times. What is happening is that these restrictions are actually causing us more problems than if they weren't there. Since we can't export it, what it means is that very often international calls, international data, are being transmitted in the open, meaning there is no protection at all; that hackers can get in more easily on international calls than they can on national. The Department of Commerce recently recognized this issue when they eased the restriction on banks. This is not sufficient. It is clear that the only people being restricted are the honest people with legitimate needs.

The government and the private sector secondly need to cooperate in the development and use of standards, without a doubt one of the most important areas that we face. Encouragement and leadership is needed. Companies are often reluctant to adopt other than their own standards,

using them to create product differentiation. Vendors do not, where standards exist, provide linkage to their proprietary offerings. Nowhere is the need more evident than the Internet. The incredible growth here has proved that, while if it's not dependable enough, secure enough or scalable enough, everybody wants it. It will not happen, however, without a clear, clear set of visions and standards adequately funded and supported by industry and government alike.

Cyber threats must be eliminated. The glamorization of the hacker needs to be debunked. The Computer Security Association said last year that in the last 12 months macro-viruses have increased five-fold. Prevention, detection and penalization of these activities need to be emphasized.

The quality must be addressed. We must find modes to help the companies build the quality. The spending on this is enormous, and I believe the reason for the consolidation of this industry is heavily that cost. We must take steps to provide funding, either through investment credits or direct funding, to provide for a stronger, more dependable society. We have to look at improved measures for performance, and we should consider the establishment of a national council on telecommunications, similar to this Commission, but somewhat more familiar and more lasting, that could not only create measures, but could measure performance against those measures. It is no longer sufficient for us to have 98.5 percent or 99.8 percent dependability. We must have 100 dependability on the telecommunications infrastructure.

Thank you.

COMMISSIONER RODGERS: Mr. Curran?

MR. CURRAN: Yes, sir.

COMMISSIONER RODGERS: In terms of setting these national standards you talk about, do you think there should be a new agency? You mentioned a national council in telecommunications. Why not an existing agency like the Federal Communications Commission?

MR. CURRAN: Yes, basically one of the problems is that standards take so long to get established, particularly through the bureaucracy that exists today. We've talked now about Internet time, regular time and government time. There is a nine-fold difference—somebody recently said—between those.

So one of the problems is we need the agency actually probably particularly in the measurements of quality and in helping us in the facilitating of industry in getting those standards established, the FCC or any of these others, if they acted as facilitators in a more active manner,

in addition to legislative activity, to address where is it and how can these standards be more adequately addressed. The Internet is the No. 1 area that is suffering from that today, domain naming, domain control, et cetera; that you can read every week about the problems of these things not being established.

COMMISSIONER RODGERS: Thank you.

MODERATOR ABRAMS: Thank you, Mr. Curran. Now, we'll hear from Mr. Paul LaShoto of Bay State Gas Company, and following Mr. LaShoto, Dr. Lawrence Mottley of Boston Emergency Medical Services.

MR. LaSHOTO: Good morning. Thank you for allowing me to testify on behalf of Bay State Gas and on behalf of the natural gas industry.

Geographically, Bay State Gas is the largest natural gas distribution company in New England, serving over 300,000 customers in three states, Maine, New Hampshire and Massachusetts, through more than 10,000 miles of pipeline. To serve its customers, the company relies on supplies from interstate transmission lines and operates its own interstate transmission line extending from the Quebec/Vermont border to Massachusetts. Peak winter demand is served using nine propane, five liquefied natural gas or LNG plants with storage capacity of 3.8 million gallons of propane and 2.2 million gallons of LNG.

There are two aspects of our infrastructure that I want to address today, protection from physical threat and protection from cyber threat. Natural gas lines and fuel storage facilities are vulnerable to physical threat, but this is not new. Our products contains a great deal of energy and could at any one point be used to cause considerable damage. However, because most of our equipment is below ground in public ways, it is difficult to access, providing us an added measure of security. Natural gas distribution networks are complex systems, webs of pipeline supplying large geographic areas. If damage were sustained in any one location, service would continue to most customers without interruption. The sole exception would be for isolated systems relying on single-line feed, and these are rare.

The natural gas industry in New England has worked closely with the Federal Bureau of Investigation in the past to minimize physical threats and considers the FBI to be the primary mechanism for preventing terrorist activity. The New England Gas Association, a regional trade association, has provided the linkage between gas utilities and the FBI. Our facilities are built and operated under regulations administered by the Department of Transportation's Office of

Pipeline Safety. Those regulations specify how they are to be built, operated and maintained and go into particular detail on the security requirements at LNG plants. The regulations mandate that each gas utility maintain an emergency procedures manual, which provides a plan of how we both address curtailments, supply interruptions and weather-related problems. All of this places us in relatively good shape to address damage to various components of our system.

While we have been conscious of the dangers of physical threat, we have only recently begun cyber threats. Operationally—and that is in our ability to continue uninterrupted service to our customers—we believe the threat is minimal. Pressures and flows throughout the Bay State system are controlled through a central gas dispatch point in Western Massachusetts. Were someone to disable this dispatch center or somehow tamper with the computer-controlled logic there, the gas distribution system would continue to operate safely although not necessarily economically. The reason for this is that we transport and deliver a physical product through a mechanical system. Our valve regulators and controllers in the field are mechanically fixed to allow a range of settings from high to low. Settings can be adjusted remotely over dedicated telephone lines by a computer but cannot exceed the equipment's physical limits. Typical designs call for redundant equipment installed in series; if one device behaves erratically, the other takes over. These safeties, put in place because of both industry and regulatory insistence that our product be properly handled to reduce risk and assure the safety of our customers and the general public, serve us well in this time of computer hackers and cyber threats.

Computers allow us to operate efficiently and economically. Cyber threats may potentially tamper with our supply mix, interfere with billing, temporarily damage our information systems, but in this regard, we're not much different than any company operating in today's technologically advanced environment. Operationally, we are different because of our historic need to assure continuous safe service.

The Department of Transportation Office of Pipeline Safety has adopted a new philosophical approach called risk management, which attempts to systematically identify vulnerabilities in the natural gas industry and address them with an efficient allocation of resources, spending time and funds where a return on investment in terms of risk mitigation is greatest. We encourage the Commission to take a similar approach. For the reasons I have touched on today, we believe the natural gas industry is less vulnerable than many of the nation's other critical infrastructures.

Thank you for your attention.

MODERATOR ABRAMS: Thank you very much. Now, we'll hear from Dr. Mottley, Director of the Boston Emergency Medical Services, and then next—and I apologize if I'm mispronouncing it—Iang Jeon, VP Electronic Commerce, Liberty Financial Companies.

DR. MOTTLEY: Chairman Marsh, Commissioners, thank you for the opportunity to address you.

The City of Boston Emergency Medical Services supplies emergency medical care for the entire City of Boston, including Logan International Airport. Our emergency response agencies within the City of Boston have within the last week jointly participated with the Federal Government's initial designation of Metropolitan Medical Strike Teams, a response to the threat of nuclear, biologic or chemical incidents which may occur in our nation's urban centers. As such, we are acutely sensitive to the importance and magnitude of the threat to our country's infrastructure. My remarks primarily address the effects of such incidents, as well as the other incidents addressed in your mission, on the emergency medical system's ability to provide continued medical care should such an incident occur. Let me pause here by saying I completely concur with the remarks of Fire Commissioner Martin Pierce, whose remarks are all independently developed. I'm entirely here with my own.

The ability to continue to provide emergency medical care depends on both the sufficient stock of medical supplies, medical personnel and medical facilities, but also the ability to maintain adequate supplies of each of these resources for the entire duration of the event.

Specially trained personnel are perhaps the most important part of the nation's infrastructure and cannot be easily replaced on short notice. The single most effective method to ensure sufficient resources in a critical incident is to ensure that your initial resources do not become casualties of the initial event. Both actual event experience and realistic training scenarios clearly have demonstrated that the simple recognition that a critical event is occurring is not usually made until the initial resources are already in danger, as shown in New York and in the actual events in Tokyo.

In the Tokyo Sarin nerve gas attack, videotape of the arrival of patients' arrival at a local hospital's emergency department was quite revealing. It showed a complete and universal lack of personal protective precautions on the part of the hospital personnel. Had the attack been based

on a liquid instead of a gas, hospital personnel would become patients themselves, and the hospital essentially ceased functioning.

Training is the key to avoiding this pitfall. We were all trained to be aggressively protective of our patients, to get in there immediately and try to care for them and however relieve situations that can be a danger and counterproductive. Infrastructure protection requires initial and ongoing training of emergency response personnel to recognize such incidents prior to the loss of medical and other emergency response personnel. Equally important is the immediate availability of personal protective equipment appropriate for the medical environment. There is no such equipment currently available to the civilian sector. Armed Forces research has reportedly produced working prototypes, but these must be quickly perfected and deployed prospectively to emergency medical personnel to prevent the loss of critical personnel at the time of greatest need. You must be able to actually perform medical procedures while wearing this protective equipment, and the current protective equipment is not so designed.

Equally as important is real-time access to the specialized medication and equipment needed in these special situations. Indeed, in the event of a nerve gas attack in any American city, the stocks of the simple antidote, atropine, which is a common, everyday hospital medication, would be exhausted immediately, even in a medical mecca such as Boston with all its hospitals. Again, the military has faced and met this challenge by recognizing that such medications may not only be immediately available in large quantities but must be able to be used by minimally trained personnel. Large caches of these supplies and medications ought to be in place today in every metropolitan region in the country, but they are not. Similarly, antibiotic stocks sufficient to meet the threat of the most likely biologic threats, such as anthrax, must be maintained in quantities and locations sufficient to respond in hours, not the days currently recognized by the FEMA program.

Lastly, recognition of the effect of the contraction of health care resources must be noted. Fewer medical personnel are expected to perform more medical tasks, and to the extent that these personnel have conflicting duties in a major incident, there may be insufficient resources to meet the emergency medical demand. Response of supplemental medical personnel from remote locations is not often timely enough to meet the emergent needs of the immediate severe casualties. As we watch the loss of hospital emergency departments and other infrastructure services primarily responsible for medical care, we must recognize that this loss lessens our capacity to

mount an adequate emergency medical response to extraordinary situations. Whether the incident is nuclear, biologic, chemical, high explosive or an earthquake or any other disaster, a common thread is emergency medical care and must be adequately supported.

There are a host of other issues which would impede the response of an emergency medical system, but they fall more properly in the discussion of communications and energy as you've heard from my colleagues today. I tried to focus your attention on these three issues for medical personnel: training in threat recognition, personal protective equipment and adequate supplies and medication, equipment and personnel dedicated to emergency medical care.

Thank you for the opportunity to share these views with you.

COMMISSIONER RODGERS: Have you done any estimates as to the cost of this training and providing of equipment and providing these vaccines to stockpiling of this? Do you have any estimates of what the cost would be to the Federal Government, or would there be as well state and local contribution for this?

DR. MOTTLEY: Yes, indeed, we had the opportunity within the last week to meet with the Disaster Preparedness Program under the U.S. Army on this issue and proposed to them our contribution on behalf of the City of Boston and what we expected from them. It is in the order of for—I believe it's EMS and fire personnel, who are first responders, in the order of the upper hundreds of thousands to the low million of dollars for the City of Boston, not a tremendous amount of money, most of which is a one-time expenditure.

COMMISSIONER RODGERS: A one-time expenditure?

DR. MOTTLEY: In other words, it's mostly equipment and supplies. The training is a cost which the City of Boston is prepared to take on its own.

COMMISSIONER RODGERS: Thank you.

MODERATOR ABRAMS: Thank you, Dr. Mottley. Now, we'll hear from Mr. Iang Jeon, Vice-President of Electronic Commerce for Liberty Financial Companies. Then following him will be Dr. Mohammad Noori of Worcester Polytechnic Institute, and I'd also like to announce that if there is anyone here who would like to speak and has not yet filled out a yellow card, please do so at the table outside. Thank you.

MR. JEON: Thank you. My name is Iang Jeon, and I am Vice-President of Electronic Commerce for Liberty Financial Companies. Let me explain a little bit about our company and what we do. Liberty Financial Companies is a diversified financial services firm with \$47 billion

in assets under management. Liberty Financial operates a number of brand-name companies, including Stein Roe Mutual Funds, Colonial Mutual Funds and Keyport Life Insurance, which sells annuities. We have developed leading-edge Internet web sites, with state-of-the-art security systems for our Stein Roe and Keyport operating companies and are currently developing similar services for other companies that we own. This security system, involving the use of digital certificates, allows our Stein Roe mutual fund shareholders to safely purchase our mutual funds and allows Keyport brokers and agents to get much needed information and to securely access client account information over the Internet. Thus, we use the Internet to enhance and expand our existing business models.

Unfortunately, simple user-name and password-based access schemes are not secure. These authentication methods are fundamentally weak and present significant risks to financial relationships. We think the answer to the security problem is the use of digital certificates, along with strong encryption and strong authentication procedures. The government has announced that it intends to allow banks to use stronger encryption for financial transactions online, but there is still some question as to whether these new rules would apply to other financial institutions, such as mutual fund companies and annuity companies. Liberty Financial, along with much of the financial services industry, including many trade associations, encourages the consideration of mutual fund companies and annuity companies in the classification of financial institutions that the Department of Commerce is looking at in relaxing the restrictions against the use of strong encryption devices. The Investment Company Institute, for example, which is the trade group for the mutual fund industry, also encourages the use of stronger encryption for mutual fund companies.

Mutual fund companies and annuity companies, like banks, are relying more and more on electronic systems, including the Internet, to conduct business around the globe. It is common, for example, for mutual fund companies to do business electronically with their customers, their brokers and dealers, their custodial firms and their transfer agents. The stronger the encryption used to protect these transactions, the more secure the transactions will be. We are talking about considerable sums of money here. In aggregate, the mutual fund industry stands at roughly \$3.8 trillion in the U.S. and more than 6,000 mutual funds serving 59 million shareholders. Billions of dollars in transactions take place every day, much of it done electronically.

In some ways, the need for strong encryption is even greater in the investment business than in the banking industry. In our industry we are dealing with confidential information about the markets and about individual securities, and the investment world is highly competitive. Often, we develop information about the economy or an industry sector. In order to keep our market edge over our competitors, we must keep that information confidential. In today's global marketplace, with financial institutions trading in securities from all over the world, that confidential information often is coming from business associates who are overseas.

This use of strong encryption will also aid the traveling business person. Many business people who travel extensively also log on to personal computers, that is, laptops, when they are traveling. While at home, they may use the Internet to get news and information and to conduct financial transactions. Why should they be hindered from similarly managing their finances while traveling because a laptop is not allowed to contain a secure browser? While there is some allowance for conducting such personal business requiring extensive documentation procedures, this process is so cumbersome to the point that it tends to strongly discourage use of this electronic medium. There are also a number of American citizens abroad, including military personnel, who would like to take advantage of these new security methods to securely access their financial information on the Internet, but cannot because of the strictures against overseas use of strong encryption.

Strong encryption is also useful in offering financial planning tools and other important services to individual investors. Because of our use of digital certificates at the Stein Roe Web site, for example, investors are able to input personal information, such as their financial holdings and the types of investments they are interested in. Our investors do not have to be worried about whether the personal information that they input on the site will be "hacked" or used by someone who is not authorized to do so. Because our customers can enter their private information, we can keep track of their investment portfolios and better service their financial needs in areas such as planning for college costs and planning for retirement.

The financial services industry is growing by leaps and bounds, and it is increasingly conducting its business online. The stronger the encryption and security that is allowed by the U.S. Government for use by individual brokers, individual investors and agents and the financial services firms that service them, the safer and more competitive this business will be.

Thank you for the opportunity to share our concerns with you today.

MODERATOR ABRAMS: Thank you, Mr. Jeon. Next, we'll hear from Mohammad Noori, Professor at Worcester Polytechnic Institute, and following Dr. Noori, Miss Diane Modica, City Councilwoman, City of Boston.

DR. NOORI: First, I would like to express my gratitude to Chairman Robert Marsh, Mayor Menino and members of the Commission for the opportunity to testify before you here today.

My name is Mohammad Noori. I'm the head of the Mechanical Engineering Department at Worcester Polytechnic Institute. I also chair a committee of the mechanical engineering department heads in New England. By my training, I'm a civil engineer, and I have practiced civil and mechanical engineering for the past 20 years. And for the past 13 years, my research has been focused in the general area of civil infrastructure systems, their reliability, safety and also their vulnerability under hazardous environment. I've also recently served as a member of the U.S. delegation on a joint U.S./Japan meeting, which was focused on the importance of research on civil infrastructure systems, and moreover, we have recently taken an initiative to bring together a partnership of several major universities and industries to focus on research into areas of civil infrastructure systems. Therefore, my testimony here today represents on a broad base the view of the civil infrastructure research community.

Investment in civil infrastructure systems basically consists of a very integrated network of private and public works that provide basic services essential in meeting the challenges of an increasing competitive global economy and sustained at high quality of life in the United States. This extensive infrastructure is the product of centuries of technological development and decades of construction, maintenance and management. The national investment in civil infrastructure research systems has been estimated over \$20 trillion.

The existing civil infrastructure system, once the backbone of the fastest growing economy in the world, is unfortunately deteriorating due to excessive demand, misuse and neglect. For example, according to recent data by the Federal Highway Administration, of 5,021 bridges in the State of Massachusetts over 58 percent of them are either functionally obsolete or deficient. Washington, D.C., the nation's capital, in the same report was like the worst in the percentage of bridges that are structurally deficiency or are obsolete. In 1994 alone, the losses due to national hazards to the civil infrastructure systems exceeded \$40 billion and over 5,000 lives. Similarly,

the studies indicate that the current decline in the U.S. productivity and increase in deficit are partly the result of a deteriorating, eroding and inadequate civil infrastructure system.

The Federal Government is estimated to be the principal source of civil infrastructure systems research spending. Although a very small portion of the total government R&D is devoted to infrastructure research, in fiscal year, 1992, approximately only 1.6 percent of the total R&D expenditures was devoted to research on civil infrastructure system. The same year, the Japanese outspent the U.S. by a factor of 30 and the European by a factor of 8. The construction sector, a \$410 billion industry, is only spending 0.25 percent of its gross sales under research in civil infrastructure systems. The contribution of transportation and public utilities business is only two-hundredths of 1 percent. Members of the infrastructure professional academic and research communities have expressed concern that these spending levels are too low and, therefore, the U.S. is losing out substantial opportunities by spending so very little on infrastructure research and development.

Several years ago, the National Science Foundation drew together academic, industry and government leaders to study and envision a fresh approach to civil infrastructure research. This collective thinking resulted in three major goals. Also to meet these goals, NSF strategy and the recent report by the White House, Technology For a Sustainable Future, re-emphasized on implementing four key areas:

No. 1. Deterioration science. Research in this area examines basically how materials or structures break down and wear out, understanding the deterioration is essential to maintain a viable civil infrastructure system.

No. 2. Assessment technologies. We need to determine how durable and how safe an environment totally benign of civil infrastructures are. The current methods are relatively primitive and prompting unnecessarily costly decisions.

No. 3. Renewal engineering. We need to extend and enhance the existing life of civil infrastructure systems.

And No. 4. Economic and social aspects of civil infrastructure systems.

Let me mention that just the experience of the Kobe and Northridge earthquakes demonstrated the conventional engineering approach to the civil infrastructure system is not effective, particularly for a large national urban disaster such as that. As a member of that U.S. delegation as I refer to in my recent visit to Japan, I realize the Japanese are no longer in a better financial

situation than we are. However, on the contrary, for the first time this year, they unfortunately surpassed us in terms of the dollar amount invested in research infrastructure. Just one point. The Kajima Research Corporation, one of the companies that basically focuses in research in civil infrastructure systems, its research budget is more than the entire budget of the National Science Foundation.

As I have had the honor to appear before this Presidential Commission, I would like to summarize my recommendations as follows:

No. 1. Over the past five years, the National Science Foundation has taken the leadership roll in formulating key research issues in CIS. It is essential that the present level of the NSF budget, particularly that of the engineering director, approximately about \$370 million, supporting six major divisions to be expanded.

2. An integrated and enhanced productivity approach is needed to promote the best informed decisions about CIS research, promoting university, industry and professional practitioners. Partnership can be a key element in this regard.

No. 3. We should support the development of global partnerships, and an international cooperative research programs addressing the civil infrastructure needs to be increased. These cooperations will assure the leadership of the United States researchers in the international community.

No. 4. CIS research in the areas of emerging technologies and the utilization of advanced technologies should be funded and supported.

No. 5. An educational paradigm for civil infrastructure systems, inclusive, that takes into account education at K2 through 12, education, undergraduate and graduate student and so on should be considered.

As we approach a new millennium, what better aim for the 21st Century than that of a civility of a civil infrastructure system?

I would like again to thank you for the opportunity to appear before this Presidential Commission, and I would like to congratulate you for taking on the task that you have undertaken, which I believe is important to future prosperity of this nation.

MODERATOR ABRAMS: Thank you, Professor Noori. Now, I'd like to invite Diane Modica of the Boston City Council to address the Commission. Following Miss Modica will be Eileen Rudden of Lotus Development Corp.

MS. MODICA: Good afternoon, Chairman Marsh and members of the Commission. Welcome to Boston and welcome to the Boston City Council Chamber. We are very pleased to make accommodations to you today for this very, very important public hearing.

My name is Diane Modica, and I'm a Boston City councilor. I'm a member of the City Council, but I specifically represent District 1 in the City of Boston. I'm Chairman of the Council's Committee on Economic Development and Transportation.

I thought it was important, first of all, to commend the President for organizing this Commission, because I think it is a very timely opportunity for all of us to take a real hard look at the vulnerabilities of our infrastructure within this nation and to really address them as optimally as we can.

What I'd like to do is just give you an idea of the kinds of environments in which many of these vulnerable infrastructure problems may arise, and certainly using my district, which is District 1, I think I can drive home the point to you. When you arrived, no doubt you arrived at Logan International Airport. East Boston, which is part of my district, plays host to that international gateway. As many of you might know, there are over 400,000 operations annually at Logan International Airport. It is unique, I think, in many respects in the nation because of its proximity to abutting neighborhoods.

You probably made your way through one of three tunnels, either the Ted Williams Tunnel, the Callahan Tunnel or the Sumner Tunnel. The northern portals of all three of those tunnels are located in East Boston. The southern portals, at least two of them, the Callahan Tunnel and Sumner Tunnel, open into the North End of Boston, which if you haven't eaten, you really should go to the North End and eat. Those portals are in the North End of Boston, and again more than a hundred thousand cars a day go through those portals. The Ted Williams Tunnel, as you know, is part of the Central Artery Project, newly constructed. It's not open to the general public yet, but abutting neighbors get to use it on a regular basis, as do commercial traffic. So that's picking up as well. Also, you probably came up against construction of the Central Artery Project, no doubt. If you came through the Ted Williams Tunnel, you definitely had to be a jack rabbit to get around some of that construction staging there. If you came through the North End of Boston, you probably saw at least evidence of its activity as well. You probably won't have a chance to go over the Tobin Bridge. That's located in Charlestown. That's another major connection between communities north of Boston and Boston and handles thousands of cars a

day as well. I also represent most of the waterfront of Boston. All of the neighbors have some place in the waterfront, and much of that is a working port. The old Charlestown Navy Yard, many of you might have heard about, is probably a prime example of the restoration of a Naval facility and now plays host to thousands of residents, as well as some commercial users, and of course, the working port of Boston remains primarily in Charlestown and South Boston.

There is an increasing level of recreational boating on Boston Harbor, as we clean it up and we encourage the use of it by residents and businesses alike. We have an increasing tourism industry, with tour boats visiting Boston on a regular basis. So our harbor is very, very active and hopefully will increase over the next several years.

I'd like to return to—in addition to that, let me just tell you that I also represent where we are today, which is sort of the heart of the city. It includes all the major banking and financial institutions, as well as other academic institutions in the City of Boston, so sort of the brain center, although Cambridge would argue with that, of the Commonwealth. I'd like to return for a minute to the Central Artery Project. As you all know, known by its common name, The Big Dig, that is a \$7 billion project. It is underway in earnest as we sit here today, and with it comes all the associated construction impacts and inconveniences that businesses and residents will have to bear with over the course of this project, which has at least another seven years to go.

One of the concerns we have in the City of Boston is keeping the city moving, keeping businesses open and operating and really reducing the public health impacts of this project on residents, but another concern that I have is the potential for major catastrophic events associated with the Central Artery Project. I'm sure you probably heard from the Boston Fire Department and maybe the Emergency Medical Services today that they have identified, the project has identified, at least thirteen catastrophic and mass casualty incidents that could occur—God willing, they will not occur—which include everything from ramp, bridge and structural collapse to major building damage, to derailments and collapses of railroads, vehicular accidents and collapses of a major portion of a large project component. Thus far, the public safety measures that the project has taken have worked well. We have had no major injuries or deaths related to this project, and we hope that we can maintain that record.

We have probably the premier public safety entities, I think, in the nation, the Boston Fire Department, the Emergency Medical Services and the Boston Police Department, all who work in coordination with providing public safety for this significant project. In fact, I believe our

Emergency Medical Services learned a lesson from an unfortunate incident in Oklahoma City in terms of how to treat victims in tunnel collapses, because obviously there were some major issues for public safety officials there. I don't know if they were prepared to deal with them, but what they did find is that compression injuries sustained in building collapses have to be treated very differently than other types of injuries. And so our public safety entities in the City of Boston are preparing for that. I guess, hopefully preparing for nothing, because I think that preparing this is really key here.

I'll just conclude my remarks by saying that, prior to my being elected to the Boston City Council, I was Licensing Commissioner for the City of Boston for nine years. I served as the Commissioner for the entertainment licensing. A lot of people would say what's the problem with entertainment. I used to be accused of preventing people from having fun, but the fact is that we license entertainment with the look towards preserving public safety. And I think one of the key incidents in the history of this city that stands in the minds of all of us is the Coconut Grove, where over 400 lives were lost just because of the lack of preparation in terms of addressing public safety. So we learned that the old adage, that an ounce of prevention is worth a pound of cure, really makes sense when it comes to licensing establishments in the City of Boston, and so we always made sure that people were prepared for the worst-case scenario. I guess in closing what I would say is that, as you move across the country and you gather information from individuals and from government officials and the private sector, that you make certain that whatever standards are developed, they are not only uniform in terms of their application across the nation, but also that in urban areas, with very unique situations, that you curtail the strategies to allow for the optimum planning.

And that brings up funding. Obviously, in order to protect infrastructures, you have to have people in place and programs in place, and as I say, I think it is worth every penny of it to put funding into the kinds of preparedness that we are looking to attain through the work of this Commission.

I'd like to thank you very much for coming to Boston. I hope that you gather very valuable information today and make sure you put us on your distribution list when the report is done. Thank you very much.

MODERATOR ABRAMS: Thank you, Councilor Modica. Thank you to the City Council for your hospitality here today. Next, I'd like to invite Eileen Rudden of Lotus Development

Corporation, Senior Vice-President of Lotus, to address us, and following Miss Rudden, Daniel Shimshak, Professor at the University of Massachusetts.

MS. RUDDEN: Thank you very much, and I'm pleased to have the opportunity to address this Presidential Commission today. Lotus Development is the primary, leading supplier of electronic mail software in the world today, and together with our parent company, IBM, we have provided more than 30 million mailboxes to companies around the world. And my remarks are going to be addressed to the emerging national information infrastructure, which we perceive to be an extraordinarily critical infrastructure for the nation and for the world.

I'd like to speak first about the foundation of that critical infrastructure, and that broad support from the public is probably the first requirement for successful and secure infrastructure. And I would like to point out that it is—we believe—the responsibility of our industry, and we applaud the involvement of the Vice-President and others in the government for bringing broad support for the development of the national information infrastructure.

We, ourselves, are involved in many initiatives to bring our employees, our software and equipment to classrooms around the Commonwealth, so that there can be more equal access to this important technology as the national information infrastructure is evolving. We have not only supported the Net Days and Massachusetts Tech Course and switched on classroom efforts, but also, we are working with a community-based computer-access network, including local organizations that are providing access to people that don't normally have computer access, like Freedom House in Roxbury, the United South End Settlements in the South End, Somerville Community Center, the computer classroom at the Computer Museum and so forth. We believe that this is the first foundation of a secure infrastructure, broad public support and access.

The second foundation, of course, is the hardware, software and services industry that is up to the task of the reliability, security and availability that will be required as increasingly our critical personal and business and matters of national interests are flowing over this infrastructure, and we indeed, as the representative and, as I said, the leading developer and supplier of electronic mail software, believe that the industry is the most competitive in the globe and is up to the task to step up to the requirements for reliability, security and availability. Indeed, even within the private sector, when I meet with chief information officers, who are my customers, that is the one thing that they want to talk about with me, 99.999 percent availability of their systems.

There is, however, a foundation piece of this software infrastructure which has already been mentioned to you today, most recently by the gentleman from Liberty Mutual, and that is, the need for strong encryption and digital certificates to further protect the users of electronic means of communication. And the strong encryption scrambles the bits as they are going over the wire, and the digital certificates identify the sender of the information as who he or she is as a trusted party with the person with which they're trying to communicate. And this is today a critical issue for our industry, that is in really the hands of the Federal Government.

For some time now, the Government has forbid us from exporting our encryption and authentication products, and this really has created quite a dilemma for the industry. First of all, it is stimulating investment in these areas abroad. Since it's such a competitive industry, we will soon—we believe we will soon have suppliers of security software coming from outside the United States. So as of today, we have the benefit of being the industry that has—where we are actually creating these products within the United States, we believe we are now in a situation where those products are increasingly being created abroad. Secondly, this is, in fact, limiting the adoption of these technologies, which are more secured technologies, because of the patchwork of adoption across the world, and, in fact, in France has their own requirements. Other companies have their requirements. We would like you and we would strongly recommend that you urge the Department of Commerce to remove the export, the export limitations, to support really the types of industry initiatives, such as key recovery, that responsible members of the industry have come up with.

We understand the need for law enforcement in this area, as we have more of the communications being conducted electronically. Obviously, there's a need for law enforcement and for technological eavesdropping, if you will. However, the course that we're following right now, we believe will benefit and cause the development of security systems outside of the United States and will limit the adoption of these more secure forms of enhanced security for these communications in the United States.

Lastly, we would like to encourage the continued support of the government and investment in R&D in these critical areas. Basic research in computer security and operating systems research and hacker techniques research and anti-virus research and autoimmune systems for computers and computer network intrusion detection, all of these are very important ways in which government investment can benefit and enhance the security of our national information

infrastructure. We would also like to compliment the National Science Foundation and the other government agencies which, of course, have really been the creators of the Internet, which has caused and is enabling the explosion of these new forms of electronic communication.

Thank you.

COMMISSIONER HARRIS: If I may ask you a question.

MS. RUDDEN: Yes.

COMMISSIONER HARRIS: Are you deeply concerned about the possibility of serious erosion of the utility of these systems because of external threats of a variety of kind, hackers, criminal elements and so on? Do you think that from your perspective we right now, unless we change our policies and practices, potentially, we'll lose the advantage of the initiative currently under way in these technologies and their universal application?

MS. RUDDEN: That's our concern, Commissioner. We are deeply concerned that in this—it's a very fast-moving industry, and that if we are not allowed to keep pace by having access to a world market, that that will enable the rest of those world markets to be served by other suppliers that come from outside of the United States. In fact, what is happening right now is that in some of the products people are now picking up security and encryption products that have been developed in Russia and in other places, because we simply must have access to a world market in order to keep our competitive edge.

So that is a very deep concern that we have today, and in answer to the first part of your question, there's nothing more important that I see in our customers, which represent a wide range of business customers today. They are all extremely concerned about the security of their networks, and they are all engaged in extensive reviews on a regular basis of the security of their network. They are all intensely interested in adding the level of security provided by encryption and authentication. In today's environment, many of them are using the lowest common denominator of encryption because of the problems with the export regulations, and then they feel that their security is, in fact, lower than it could be. Thank you.

MODERATOR ABRAMS: Thank you very much. Next, I'd like to invite Professor Daniel Shimshak, Chairman of the Department of Management Science and Information Systems at the University of Massachusetts, and following Professor Shimshak, Edward McGann from Megapulse.

MR. SHIMSHAK: Thank you very much. Well, you just said it. My name is Dan Shimshak, and I'm the Chairman of the Management Science and Information Systems Department at the University of Massachusetts, right here in Boston.

I'd like to take the opportunity to address you concerning computers and telecommunications and their impact on my life. I will conclude with specific recommendations for the Commission. I have a feeling I'm going to be bringing this down to kind of a personal level as I talk. Not surprisingly, I spend a great amount of time at work in front of my computer. I prepare lectures, develop class assignments, analyze student grades, conduct scholarly research. I report notes on many, too many, meetings, and in every course that I teach, I use, students use and work on a computer. Nearly everything that I do as a professor involves a computer.

When I finally get home from work, the first thing I do is turn on my home computer. It stays on throughout the entire evening until everyone in my house retires for the night. There's always a constant battle over who gets to use the machine at what particular time, and aside from the battles, the computer has had a major impact on my life, though I'm not exactly sure how. If I tried to express it in words, I don't know how. I'm not sure I have more free time, because I seem to be busier than ever. I don't think I can think any faster or clearer. I can't play chess any better, and I'm not sure what it is. But I do know that if my machine goes down, I'm lost; I'm really lost.

Unfortunately, more and more of computers are following victim, not to technical problems, but to things like viruses. The viruses really violate the computer owner. They break into the home, to the workplace, and it's not just for the purpose of getting and stealing something oftentimes, but for the sole purpose of doing wanton damage. I've not only become dependent on my own machine, but also on the machines of others. The Internet, of course, where has it been all my life? It's become my library, my researcher, my information gatherer, my communicator, my idea sharer, my purchaser. Just before I arrived actually today, I purchased a couple of tickets for my sons for a concert. I don't know the name of the group. That's their problem. Sadly perhaps for the Post Office and Phone Company, I've become fully dependent on the Internet.

At the same time, I'm very concerned about what lurks out there in cyberspace. The Internet has continued to grow and evolve, but I don't know who's in charge. And I'm not sure exactly about the security. So I read about people who are able to build a bomb off the Internet. I read about children who are enticed to leave home and meet some dangerous strangers and criminal

hackers who break through the security system at a bank to empty some customer's savings account, and then I also know about data files or cookies and crumbs, that great terminology that is being developed, that are compiling personal information about Internet users at many of the World Wide Web pages. So again, I wonder who is in charge and where is the security.

Now, if you take my situation and you multiply it by millions, how many people and companies and industries and agencies, universities and government are like me? They can't function today without their computers and telecommunications systems. They too have become more and more dependent on the Internet. The outbreak of a serious virus could do unimaginable damage, and a computer hacker could wreck all kinds of havoc. And the question is though: Should someone be in control?

And we face these concerns every day. I have with me actually and attached to my comments a copy of an e-mail message that I received last week about a new destructive virus spreading via the Internet e-mail. It's called Deeyenda. The names are always so clever. This message came from, of all places, the Office of Representative Wolf, of the U.S. House of Representatives. Just to read a few excerpts, it says, "If you receive an e-mail message with the subject line, Deeyenda, do not read the message. Delete it immediately." That's in all capital letters. "Some miscreant is sending e-mail under the title 'Deeyenda'. If you get anything like this, don't download the file. It has a virus that rewrites your hard drive, obliterating everything on it." And then it goes on to say, "But also it can look for valuable information, such as e-mail and passwords, credit card numbers, personal information. It can copy the information and send it out to an unknown address."

That is scary stuff. How did I receive the e-mail message? It was sent to me by a friend, who received it from another, and I, following suit, forwarded the message to as many friends that I have that I could possibly send to. A strong sense of community has developed within the Internet, kind of an informal camaraderie among people who know each other perhaps only by their screen name, yet are willing to help a cyber friend avoid the evils of a dangerous virus.

On top of it, last week, I received a copy of my *Newsweek*, a week-old *Newsweek*, and the front cover asks, "Can we fix the 2,000 computer bug before it's too late, or will we have the day the world crashed?" *Newsweek's* assessment is that the world depends on the computer, and if a bug that affects how machines recognize the year 2,000, can cause the world to crash, then you

can imagine what destruction the Deeyenda would cause if there's a virus outbreak. Maybe the whole Earth will stop spinning.

On top of this, I pick up my newspaper last week, and I read about this criminal hacker who broke into the computer system of an Internet service provider in San Diego. He stole 100,000 credit card numbers of their customers and tried to sell them to, of all people, an FBI agent. This could have amounted to a crime or a theft of about a hundred million dollars of credit, and you wonder why I'm so concerned about what's going on.

So what am I doing to help resolve some of the problems? I've taught hundreds of students about computer systems, application software, system development, telecommunication, data support systems and on and on, but more so, I've taught my students about computer crime, including illegal access and use of data, data alteration and destruction, data and information theft and software privacy. I've taught students about ethical issues in information systems, issues about privacy, accuracy, property and access. I have encouraged students to become familiar with professional computer associations and their code of ethics. What is private industry doing? Companies have built security systems or fire walls to prevent outsiders from invading their own private networks.

However, this security has not been as successful on the Internet. There are many telecommunications companies that are working to develop software to help the Internet user protect themselves from threats to their privacy and security, but these software are often cumbersome and difficult to use. And then what can the government do? I'm not willing to give up my freedom of speech on the Internet, and I don't want another bureaucracy being created to take control. But I do expect the government to protect me and my property. Almost all states have computer crime bills, and the Federal Government has the Computer Fraud and Abuse Act. But these bills are not effective for several reasons. Many people in companies do not always actively try to detect computer crime. Security is inadequate, and convicted criminals are not seriously punished. We need new and stronger legislation, particularly based on recent concerns and the use of telecommunications on the Internet. Computer system users must be made aware of the harsh consequences of computer crime. It will take education, technological advances and strong laws to safeguard our telecommunication systems. Only then can we be sure that some cyber threat won't make the world come crashing down. Thank you.

MODERATOR ABRAMS: Thank you. Our next presenter will be Edward McGann, Executive Vice President of Megapulse, Incorporated, and after Mr. McGann, Major Gregory Rattray of the United States Air Force.

MR. MCGANN: Thank you, Chairman, members of the Commission. I have to apologize for the form of my notes. At 8:20 this morning, I was reading the paper. I had the opportunity of being at the earlier meetings in the Washington area and somehow missed the date of this one. I could have gone to my computer and done the notes. I just decided to take off my pajamas and look a little bit better. So with your apologies, I'll do the best I can. This is Boston, so a little blarney is allowed.

I'm here not to speak about buildings or bridges or money or whatever. I'm really here to speak about navigation policy, certainly not Boston policy, not New England policy, but U.S. navigation policy, which flows over directly into international policy.

I am the vice-President of the Megapulse. We're a company that's been in the Greater Boston area for 27 years. We are in the navigation business. I'm also the vice-president of the International Navigation Association, and I'm a member of the Board of the International Navigational Association, so I'm very much involved in navigation policy around the world.

The concern of members of the navigation community is that this country, with the policies that it is presently pursuing, will become solely dependent on one system, not only for its position fixing, not just for its navigational, but for many elements of precise time distribution. Precise time distribution is the basis of control for power networks and for communication networks, so when I talk about navigation systems, I'm not talking just about boats, not about trains, not about airplanes. I'm talking about the communication networks that we've all heard today are so vulnerable of interference. They're also very vulnerable that, if their precise timing disappears, they'll collapse. Twenty years ago this country had two clocks, like that, and that, when was Ma Bell was Ma Bell, and that's how we ran our telecommunication network. Today, we have tens of thousands. Every time there's a new cell network, somebody has to tell it what time it is, so it can precisely clock the data as we send more and more of it around.

The system to which we appear to becoming dependent on is a satellite-based system called the Global Positioning System, in which you and I, as taxpayers, have spent \$15 billion and which we will continue to spend a billion dollars a year. Now, I'm not critical of the system. Great technology, great stuff, better used for surveys, and somewhere you can check it, but if it's

the only system on which the military—and the military will never become solely dependent—but if it's the only system which the Federal Aviation Administration can use—and after the year, 2005, that may be true—if it's the only system that the Coast Guard can provide maritime navigation services—this is a cup, but if I put a hundred dollars worth of electronic equipment in that cup, I could prevent all aviation activities within 25 miles of this building and all navigation services along the coast of Massachusetts and Boston Harbor.

This can happen. Has it happened? No, and nobody ever bombed the World Trade Center before. Now, the World Trade Center bombing won't bring us to our knees. The Oklahoma building won't bring us to our knees. Poisoning a reservoir won't bring us to our knees, but if we lose all the infrastructure on which we move goods, equipment and services and we time our communications and power networks, we might. So my recommendation to this Commission, please, in whatever way you can, inject yourself into the policy-making process which is evidenced between the Department of Defense and the Department of Transportation in the form of the Federal Radio Navigation Plan, the late 1996 revision, almost up for decision at the secretary's level.

Remember, we're not just talking about U.S. policy. The satellite-based system provides signals around the world, and we've done that. We've exported a weapons delivery system to the world, without policy decisions as to what might happen on the day after Afghanistan launches a weapon against Israel. We have no policy on that area. It's all part of the infrastructure that we're making for ourselves but giving to the world.

Let me bring to mind a little more of the threat. Just a couple of weeks ago, before the British elections, if you remember, the IRA—it's tough to be speaking in Boston like this with a name like McGann; you're likely to get bombed. The IRA threatened the British Government by putting bombs in various highways and so forth and by not putting them there. The threat is exactly the same. Put yourself in the position where instead of the word, bomb, you use the position, sole dependence on a navigation precise-time system. You don't have to do anything to interfere with it. You just call up and threaten to interfere with it.

Earlier, one of the fire captains said maintain command and control. He's worried about Boston. I'm worried about the entire United States. If we have one system and it's controlled by the military and the military wants to do something with it, it should, but where does that leave the civilian area? So we either leave the military no flexibility; we take it away from the civilian

area. And if we get mad at somebody, what do we, shut it off over Ireland? Now, we can't do that, because we already agreed in the international community to provide it.

I think that we're talking about critical infrastructure—critical, critical, infrastructure. Let me also just comment, going by, there are lots of rollovers. The 2,000 rollover is a real-time rollover in 2,000, but you get lots of rollovers. It all depends on what system clock you're using. In the navigation world, we have a number of system clocks that we roll over regularly. Sometimes we're prepared for them; sometimes it's a disaster. The rollovers come and go.

Dependence on a single system, here in the Boston area, not too long ago, we have the Royal Magistry cruise ship that went aground off Cape Cod, and the memory was gone like that. Why? Because we didn't have a thousand lives lost. We didn't have any ecological damage. Why did they go aground? Because the crew was told to solely depend on this magic new system, not look out the window, not turn their radars on, don't set that pathometer, that one system they were using. It could have been a tragedy. Let's hope it doesn't.

Thank you for the opportunity. I hope that perhaps this Commission can have an impact on policy, because I'm tired of addressing it. Thank you very much.

MODERATOR ABRAMS: Thank you, Mr. McGann. I'd like to call upon Gregory Rattray, and following Major Rattray, Mr. Jim Nickerson of the National Disaster Medical System.

MR. RATTRAY: While I am an Air Force officer, the Air Force has allowed me to attend the Fletcher School of Law and Diplomacy for the past two years and a further year, and my remarks this afternoon spring from any academic research and are certainly not the position of the Air Force or the Department of Defense on any of these issues.

What I would like to highlight this afternoon for the Commission are some findings at this point from my research regarding how to analyze large-scale or strategic threats to the United States based on the potential opponent's ability to attack our information infrastructure. I appreciate the opportunity to highlight two significant issues that I think have gone under-emphasized in development of our thinking regarding what the Commission terms cyber threats through this infrastructure.

Numerous declarations now exist in the press by government officials and informed parties in the private sector that, despite the absence of known large-scale attacks on U.S. information infrastructure, such a threat is of real national security concern, and I believe there's probably three primary reasons we see such fairly peremptory declarations.

First, due to the U.S. dominance in other types of means for ways and conflicts, especially on conventional battlefields, opponents with strategic intent may well see infrastructure attacks as their only viable way of directly getting at U.S. centers of gravity in a conflictual situation.

Second, this perception is heightened by the fact that the technological tools for conducting these attacks are widely available, very difficult to control and relatively cheap. This situation also means non-state actors may be able to create the capacity to inflict considerable damage and pain in the United States.

Third, due to the nature of the cyber space environment, its rapid pace of change, the U.S. would have difficulty discerning whether an information infrastructure attack was under way and who was responsible for the attack. U.S. policy makers and planners also face significant ambiguities, especially in the legal realm, about what appropriate responses are allowable if the nation was to suffer large-scale cyber attacks on unsecured infrastructures. I believe all these concerns are valid, but in terms of logic, if no other considerations are operative, why do we have so little evidence against a large-scale, disruptive effort against the United States? Alternatively, why have we not yet suffered an electronic Pearl Harbor? I do not think it's because the U.S. faces no potential adversaries who harbor ill will towards us. Rather what I think is generally missing is the recognition of additional challenges facing potential adversaries who would use information warfare on a large scale. I'd like to point out two of these considerations I think are worth addressing.

To begin, one must consider the fact that the widespread availability of the technological tools is not the same as creating organizations with the sustainable capacity to understand the weaknesses of their target, in this case the very complex U.S. information infrastructure and related infrastructures that the Commission is studying. Assess the damage that such attacks would inflict and stay at the forefront of technology, as both the means of attack and the targeted infrastructure rapidly changes. While creating vulnerability, the complexity of the U.S. infrastructure may also make the task of targeting and damage assessment more difficult.

Additionally, the use of new technologies to perform wholly new missions, such as a strategic information-based warfare, faces significant barriers in terms of technological assimilation and fitting into existing organizational and political contexts. History demonstrates in the commercial realm, as well as for military forces, that the effective incorporation of new technologies to improve and transform organizations is more often than not a difficult time-consuming and

uncertain process. While we tend to recognize such challenges for ourselves, we tend to downplay them when assessing our adversaries.

Also, the discussion about large-scale information attacks pauses opponents who continually probe our infrastructures for weaknesses, ready to pounce when a condition of significant advantage is perceived. Yet if information infrastructure is understood as a means to achieve political objectives, such means might be used in the context of a surprise strike, but may also require a capacity to use on demand in light of an actor changing objectives in a political situation. A strategic information warfare campaign can very possibly be waged as a one-shot, premeditated conflict against the United States when the opportunity was right, but such conflicts do not comprise the norm in international affairs. While use of surprise attacks may be relatively commonplace, such attacks generally occur in response to evolving crises and are not complete bolts from out of the blue. The use of strategic information warfare used in response to an emergent crises would have to rely on existing organizational capabilities created for ones created through mobilization.

Finally, the current analysis tends to ignore the objectives adversaries could conceive of achieving through large-scale cyber attacks on infrastructures. Although the potential for widespread disruption and infliction of pain is fairly apparent, thinking through how adversaries could turn such leverage into useful influence tends to be missing from current analyses. If simple anarchy is the goal, then such attacks may prove the perfect tool for both domestic and international terrorists and very difficult to stop. If the intent is an adversary who wants to coerce or deter the United States to be a political influence, the situation may be substantially different. Such adversaries would have to communicate intent and, therefore, assume some level of responsibility for their actions to achieve their goal. Whether the attack is an assumed responsibility or the scale of the attack enabled the U.S. Government to adequately identify the perpetrator, the attacker would then run significant risks of retaliation. The potential for retaliation in kind or by other means would dramatically affect the cost benefit analysis of potential adversaries.

Personally, I think that the strategic threat deserves significant attention. The technological tools for such attacks exist. Very rare are historical examples where available technologies are not turned into the means for a large-scale warfare by organized groups. However, to the extent that existing analysis portrays the simplicity of waging such attacks, I think that it ignores both

historical evidence to the contrary and demonstrates a counterproductive inclination towards worst-case analysis. Development of a robust capacity to wage strategic information warfare will likely take U.S. opponents, whether they be state or non-state actors, significant time. The political motivations and objectives of potential threats must also be analyzed, and confrontations between states, situations of deterrence may evolve if the technological tools for such attacks are so threatening to both sides and outweigh potential gains from their use. Potential use by non-state actors of such tools creates much more difficult situations. I thank the Commission for the opportunity to present these thoughts.

COMMISSIONER RODGERS: Sir, what is your preferred solution for getting this level of needed cyber security? Do you have a recommendation in that regard?

MR. RATTRAY: I do think that diffuse solutions by the organizations who are dependent on these infrastructures are probably going to be more effective than attempting to define a centrally-controlled solution, and looking to the encryption issue, I do think that self-protection is probably, in terms of reducing our overall large-scale vulnerability, an important step towards that.

COMMISSIONER RODGERS: Thank you.

COMMISSIONER HARRIS: If I might ask another question, as you have thought through the processes you have, have you come on the following possible scenario: A set of disruptive attacks, by a group seeking to minimize the capacity for continued development of the United States, with that set of attacks leading to a very disturbed public reaction and then to a possible legislative response which shuts down development in these fields, reduces the capacity or regulates in a harsh way access to utilization of these new technologies?

Under that scenario, one would imagine significant loss of competitive capability on the part of the United States. Is that a scenario that you've examined in any detail to see whether it's plausible, sensible or, indeed, has potential for occurring?

MR. RATTRAY: I think that it's a scenario that is actually increasingly raised. I've had a number of conversations with people about this very recently, and they term—some of the people I talked to term these sociopathiable attacks; that continuing eroding of confidence and high value information systems could kind of incrementally erode our willingness to rely on these systems.

My sense of it—and I'm not sure it's a researchable or an answerable question in any kind of definitive way—is that that's unlikely. To do this, you would first have to have an objective that required a very sustained view of eroding our economic competitiveness. I do not think that any of our trading partners, while they might commit economic espionage, would actually physically disrupt or damage information infrastructures, because that would change the rules of the game so dramatically that I think the retaliation they'd beg by doing that, they would recognize was not worth the gains they might make. The other thing is few entities are capable of sustaining the will and have such long-term objectives to successfully carry out such a gain.

COMMISSIONER HARRIS: Thank you.

MODERATOR ABRAMS: Thank you very much. Next, we'll hear from Jim Nickerson representing the National Disaster Medical System; following Mr. Nickerson, Mr. Raymond McCabe, who heads up the Electronics Benefits Transfer Department of the State Comptroller's Office in Massachusetts.

MR. NICKERSON: Thank you for providing me an opportunity to provide input on your work in addressing vulnerabilities to our nation's critical infrastructures and to provide a public health emergency preparedness perspective to your deliberations. The commission's charge, as directed by the Executive Order, is an important and large mission—to assist the president by recommending a national strategy for protecting the nation's critical infrastructures from a spectrum of threats and assuring their continued operation. The Commission has identified emergency services (medical, police, fire and rescue systems) as one of the eight critical infrastructures.

As a member of the National Disaster Medical System and having served on the executive steering committee of the Metro Boston Disaster Medical Assistance Team my comments are directed towards the medical and rescue component of the emergency services infrastructure. As a past chairman of the National Section On Emergency And Crisis Management of the American Society For Public Administration, I have interacted with emergency management officials and academia at the national level to critically examine our nation's response capacity. Also, having served as the regional emergency medical services coordinator for the Metropolitan Boston EMS Council at the Massachusetts Hospital Association, and also having served as the emergency planning coordinator for the Massachusetts Department Of Public Health, I have evaluated

disaster response capacities of our local EMS system and facilitated planning efforts to coordinate an integrated response to public health disasters at the regional and state levels.

My comments will summarize the critical role the National Disaster Medical System (NDMS) plays in medical response to natural disasters. The system, which has been operational for a number of years, has been highly effective despite very limited funding. I will describe the important work underway in the development of specialty medical teams, called Metropolitan Medical Strike Teams (MMST), to respond to acts of terrorism. Also, I will briefly highlight recent presidential and congressional action which has accelerated the program's development, and finally I will recommend additional measures be taken to ensure the future growth and success of the national disaster medical system and associated specialty medical teams.

NDMS was designed to: 1) supplement state and local medical resources during disasters; 2) provide backup medical support to the military and VA health care systems during an overseas conflict; and 3) promote the development of community-based disaster medical service systems. NDMS provides a national program, coordinated by four federal agencies (HHS, VA, FEMA, and DoD) to help develop state and local disaster medical resources prior to major emergencies, and then support the localities after disaster strikes. Disaster medical assistance teams, or DMATs, provide medical care in a disaster area following a presidential disaster declaration. There are presently 60 DMATs located throughout the country—Boston having been designated as one of 21 level one/first deployable teams.

It is this infrastructure that allows activities such as development of MMSTs to be carried out and supported with national assets should the need arise. The MMST is a cooperative federal/state/local government venture which will develop 27 MMSTs, in selected U.S. cities including Boston, composed of non-federal health professionals who will be specially trained to provide medical and other health services to victims of a terrorist act. As mayor Menino stated, Boston has been selected as the pilot model city nationwide for implementation of Nunn, Lugar II.

The primary effect of a terrorist act, be it nuclear, biological or chemical is its impact on the life and the health of the victims. We have learned that throughout our country, states and localities are not prepared to rapidly and appropriately manage the effects of terrorism. As we most recently saw in the bombing in Atlanta during the centennial Olympic games, the public has very high expectations for the governments response after a terrorist incident; during the first few hours it will be the local government that will have to manage the incident. It has been

consistently recognized that if lives are to be saved, the local communities—the local medical first responders—must be adequately trained and equipped to deal with unfamiliar injuries and unfamiliar decontamination activities that they are currently not trained and equipped to handle.

The goal of the MMST is to reduce the mortality and morbidity associated with the use of weapons of mass destruction. This program provides a national infrastructure and means to empower localities to turn victims into patients, not fatalities, and to treat these patients successfully so they can be returned to being productive citizens. The national infrastructure is a critical element within the overall program. The NDMS provides the most important portion of that infrastructure.

In 1995 president Clinton spoke to the United Nations about the challenges that the UN and the United States will face in the next 50 years. He said, "...today the threat to our security is not from an enemy's missile silo but from a briefcase or a car bomb in the hands of a terrorist." He signed Presidential Decision Directive 39 which stated: "It is the policy of the United States to deter and defeat and respond vigorously to all terrorist attacks on our territory and against our citizens." FEMA was directed to review the Federal Response Plan and the adequacy of the NDMS and procedures for DoD support which included support with medical facilities and decontamination. In July 1995, the U.S. Public Health Service's Office of Emergency Preparedness sponsored a first of its kind seminar entitled "Responding To the Consequences of Biological and Chemical Terrorism" in Bethesda. The city of Boston sent a delegation of EMS officials to attend the conference as well as participate in the development of a terrorism annex to the Federal Response Plan.

Last year (1996) Congress passed legislation (Public Law 104-201) which includes a program to train first responders throughout the nation to recognize and treat victims of NBC terrorist attacks. This program is now in the early stages of implementation which will better train and equip our first responders. Since it is likely that both local and state resources would be overwhelmed in the aftermath of a terrorist attack, an integrated federal, state and local response infrastructure system is required. However, significant funds will continue to be needed to implement this important initiative to increase the number of these medical strike teams in key jurisdictions across the country. The initial federal efforts to assist first responders will be for awareness training; a higher level of training (e.g., operational level) will also be required.

In summary, I would urge the commission to carefully examine the NDMS system, identify further funding gaps and requirements to implement and expand the MMST concept to other major cities, and formulate policy options in your report to the president to stabilize and expand this important national critical infrastructure. To do less would be a disservice to our first responders and the American people. The future threat will attack our human assets to take over our physical assets. Our first responders must be ready to meet that threat.

Mr. Chairman and members of the Commission, thank you for allowing me this opportunity to testify. I would be happy to answer any questions that you and the Commission members may have.

MODERATOR ABRAMS: Thank you, Mr. Nickerson.

CHAIRMAN MARSH: Again, may I say to all present, I appreciate very, very much—we, the Commission, appreciate very, very much—your fine participation, and I think we’ll continue on for a few more minutes. But I must catch an airplane, and I’ve got an important engagement back in Washington. Again, thank you so much for helping us with our endeavor.

MODERATOR ABRAMS: Thank you, Chairman Marsh. Next, I’d like to call on Raymond McCabe, Electronic Benefits Transfer Coordinator for the State of Massachusetts Comptroller’s office. Following Mr. McCabe, we’ll hear from Roberta Croce of Boston University.

MR. McCABE: Thank you and good afternoon. I’m just here to fill in for my boss, William Kilmartin, the State Comptroller, and I’m, on behalf of the State Comptroller’s office, here to express our views on the use and protection of commercial infrastructure.

Right now, the Commonwealth is actively engaged in electronic commerce. We use electronic commerce on a daily basis, and we rely upon it. We currently use the Internet for procurement solicitation and for financial reporting. We have other Internet applications on the way. On the payment side, we have selected vendors who are utilizing electronic data interchange and electronic funds transfer for ordering, invoicing and payment of state contracted goods and services. Electronic benefits transfer is being utilized for the distribution of means tested state and Federal benefit programs. Of all the electronic programs I have just enumerated, the one I would be concentrating on is electronic benefits transfer.

In September of 1993, Vice-President Gore issued a report of the National Performance Review, “From Red Tape to Results.” This report called for the rapid development of a nationwide system to deliver government benefits electronically. The Federal Electronic Benefits Task

Force was chartered in November of 1993 to develop a national plan for this implementation. Massachusetts happily, I'm happy to say, was one of the states that participated fully with the task force and helped in the creation of a report of a benefit delivery system that works better and costs less, and that was done in May of 1994.

In April of 1995, Massachusetts, along with the other New England states and New York, formed the Northeast Coalition of States to develop and implement the regional EBT system. We are also members of the National EBT Council, which was formed in May of 1996, which established a uniformed set of operating rules and national operating procedures for electronic benefit transfer. NCS, the Northeast Coalition of States, is a chartered member of the EBT Council and has a leadership role in the ongoing development of the national policies.

Massachusetts and Connecticut are currently implementing electronic benefits transfer on a statewide basis for both Federal and state-funded programs. The other states in the coalition are scheduled to rollout during the next 18 months. When fully implemented, EBT will service over 2 million recipients and 27,000 certified food stamp retailers in the seven-state area. The NCS represents 20 percent of the nationwide total benefit programs.

In 1993, the potential scope of national EBT implementation for all pooled Federal and state benefit programs was estimated to encompass \$111 billion in cash and food stamp benefits. EBT is currently online real-time, and that is the crux of the problem. We use a magnetic stripe card, and the technology is compatible with the current commercial infrastructure structure. We have "smart" card technology in the future. However, the current electronic infrastructure does not support it. The key to the cost-effective implementation of nationwide EBT is utilization of the existing infrastructure. It is this utilization of the existing infrastructure which causes a potential problem. We are the deployer of last-resort terminals. Those terminals are commercial terminals, but they have a restrictive software. Our recipients rely on automated teller machines and point-of-sale devices. These devices rely on banking and telecommunications.

EBT recipients are issued magnetic stripe cards by the agency, and the recipients select or are assigned a secret PIN, personal identification number. The benefits of these recipients are transferred on a scheduled basis to the EBT account. Recipients access those benefits online in a real-time environment through the commercial settlement. Cash benefits can be obtained from ATMs. Food benefits can be obtained from point-of-sale terminals, in addition to cash benefits. They are run through the normal commercial networks. However, unlike commercial networks,

the EBT accounts don't have monthly statements, nor do they have check-writing capability. Therefore, they are only accessible online real-time. EBT costs less, and it works better. Recipients receive their benefits seven days a week, including holidays, and can access those benefits in a more secure, 24-hour-a-day environment. Check-cashing fees are eliminated, and the stigma associated with food coupons is replaced with debit card access. Recipients are included in the mainstream of financial transaction processing and introduced to new commercial services previously unavailable. EBT has a positive impact on contingency planning for infrastructure failure.

Our participants have to meet high standards, hot site protection, 99.9 percent availability. Our reliance on this commercial infrastructure has increased the consequences of financial or telecommunications infrastructure failure. The interdependence of the telecommunications and financial infrastructures has been moved to a new level. I am here to bring you the recognition and hopefully your awareness of this increased interdependence. Private enterprise and government combined to make EBT a commercially viable service. Now, there is need for a combined strategy to minimize disruptions and protect this critical infrastructure.

Thank you.

MODERATOR ABRAMS: Thank you, Mr. McCabe. Next will be Miss Roberta Croce, Director of Information Sciences of Boston University, and then our final presenter will be Benjamin Tartaglia, Executive Director of the International Telecommunications Disaster Recovery Association.

MS. CROCE: Good afternoon, Commissioners. I thought you might like to hear from a security practitioner, and that is my job. I am Director of Information Security Administrative Data at Boston University, and I am very honored to have been asked to speak on such an important issue.

Back when I was in elementary school, we practiced infrastructure protection by listening for the terrible whine of a siren, and when it was heard, we followed our teachers silently to the basement, where we all huddled under a stairwell, with our arms over our heads to save ourselves from the threat of that day, an atomic bomb attack, atomic bomb attack. We've come along way from that innocent time.

I have been at Boston University for the past 18 years, and I love what I do. The university has always provided its support to do what was needed to protect the university's information

assets. Like many corporations, we have been a main frame shop. All information was stored in one place. Backups were taken on a regular basis and shuttled to a remote site for safekeeping. With 30,000 bright, enterprising and inquisitive students in our environment—and they are one of our finest assets—we had to take appropriate measures for information security. From ensuring personal privacy of information entrusted to us, to keeping out intruders and all the while allowing staff to perform their job functions was our responsibility. It was a manageable challenge.

The main frame was that enclosed environment, and having established an information security policy and having implemented authentication and authorization techniques for our 30,000 users, with appropriate security layers, we began to look at a proactive approach to monitoring for exposures and vulnerabilities. We wanted to electronically survey our system and be able to notify support staff in a real-time mode as the attack was occurring and before damage could be done. A system was developed that woke up every 15 seconds and verified that all operation system critical libraries had not had any unauthorized changes. If so, a member of my staff would be called on a beeper to investigate. It was a 24-by-7 security monitoring system called SLEUTH, Security Looking Electronically Under The Hood. This system has given us a fairly good level of comfort about the exposures of our main frame operating system, to both internal and external threats.

So one of our recommendations is to automate monitoring and provide real-time notification. We also established thresholds that we felt, when exceeded, could indicate a potential threat such as a number of password violations occurring within a given amount of time. Obviously, a cracker program would create multiple violations before it made a hit. Manual monitoring would never catch this kind of attack until after it had occurred, but with automated monitoring, it would notify us when it was occurring and allow us to have a chance in identifying who was attacking us.

Recommendation 2: Establish violation thresholds. We hire a security consultant each year to do penetration studies on all new software purchased for our main frame. You may be surprised that over the course of three years two commercial products were found to have holes, as witnessed by my password being obtained by the consultant directly through these products. The vendors gave us a patch to plug the hole. However, one vendor continues to the sell its product with the vulnerability still in it.

Recommendation 3: Please certify commercial products that claim to be secure and make it a feature to have passed certain security requirements.

All in all, we were feeling pretty good about the security at that time, and then we connected to the Internet. All bets were off. We found ourselves back to square one, and in 1994, on a Friday evening, I heard Tom Brokaw announce that thousands of passwords had been obtained on the Internet using a “sniffer” type of software that allowed one to see the data as it went over the wire. No one knew who had been hit. That Monday morning, all users were notified to change their passwords, but so what? Who could stop someone from buying “sniffer” and doing it again? I found sniffer software being sold in a popular catalog that came to our house for as little as \$150. We purchased the product and, sure enough, within minutes we were able to capture the password of a manager who had just logged onto the mainframe over the campus network. It was clear that with re-usable passwords in the clear we were dead. The university supported the recommendation to purchase smart cards as a way to provide assurance that “Fred is really Fred” by using a two-prong authentication method: Something you know, for instance, a password and then something physical that you have. This smart card produces through a proprietary algorithm a different six-digit number every 60 seconds, so even if your password was compromised and you didn’t know it, it would be useless without having this second problem, the card.

Recommendation 4: Establish a contingency plan, practice it, and, most important, keep it current. We established a Disaster Contingency Plan, implemented it, updated it and practiced it every year. You could begin operations on a remote site within 24 hours of a disaster.

Recommendation 5: Demonstrate the worst case and then attack it to find a solution. We began to develop fine server and Web applications. Words like spoofing, spamming, hijacking, piggybacking and flaming were bantied about. CERT, the Computer Emergency Response Team, continued weekly to put out warnings and messages of vulnerabilities in commercial software and how to close those exposures. We were out of breath trying to keep up with this ever changing environment. Our passwords were now Kerberized with Kerberos, a password/ticket granting scheme developed across the river at MIT, which authenticated users using encryption and never allowing the password to leave the client’s machine.

Today we are using Kerberos passwords and smart cards to authenticate users on sensitive Web applications. We still don’t feel as comfortable as we did when the implementation occurred

on the main frame, but the benefits and opportunities that come from using the Internet to communicate and share with people all over the world require us to seek out a better way to secure this method of communication, while allowing us to take advantage of its full capabilities. Open and secure networks are not necessarily exclusive.

Recommendation 6: Define and establish “Trusted” systems and networks. I asked my colleagues at other universities what messages they would like me to convey to you, and two items mentioned over and over were: One, please include funding to support academic programs and computer and Internet security and computer ethics, and two, ask Congress to approach a stronger encryption scheme.

I cannot think of one item on your list of infrastructures that could not be rendered inoperable or worse by the sabotage of its computer systems. It is critical that you study and gather all the expertise that is available to assist you in addressing these issues. I commend you all for taking the charge and seeking input from industry and academia. Please call upon us for any assistance you think we could provide you in the future. I wish you all well in your efforts. Thank you.

MODERATOR ABRAMS: Thank you so much, and finally, Benjamin Tartaglia, Executive Director of the International Disaster Recovery Association.

MR. TARTAGLIA: Boy, this reminds me of the loyal, dedicated fans at a Red Sox game, last of the ninth, in the rain and the Sox behind by 10 to nothing. Really, thank you for having me today, Commissioner. I was going to thank Chairman Marsh, but I’ll thank you. You can pass it on to him.

I’m here today to talk about the criticality of telecommunications in my role as Executive Director of IDRA. You have heard all day today over and over how important telecom is and all the problems there are. I’m here to offer a solution to that.

IDRA was founded in 1989, and it’s International Disaster Recovery Association. planning professionals having a special interest in telecommunications. IDRA recognizes the unique role telecommunications plays in all organizational activities and the importance of continuing an adequate level of voice, data, image and sensory communications during interruptions in normal service levels.

We provide a focal point for those involved in telecom disaster recovery planning. We act as a clearinghouse for issues. We provide meetings and educational events. We do a lot more, but just to keep it brief here, one of our objectives is to work with the other associations, government

agencies, and private industry to promote disaster recovery planning, contingency planning and business continuation, all using telecommunications.

Working towards that objective, we act as a clearinghouse, and we hold an annual conference each year that deals entirely on telecom disaster recovery. All the exhibits, all the speakers addressed those issues. The eighth conference is going to be held in Boston next year, March 15th through the 18th, which just happens to fall over the St. Patrick's Day weekend. So we'll have green beer that whole weekend.

Some topics we have addressed in the past are the year 2,000. Just for a minute, there are two problems with the year 2,000. One, of course, is the computer and handling the 2,000 number, but also that's supposed to be the year of the convergence of solar flares. Every 11 years, it's supposed to be a big convergence, and it puts down all the satellite systems if the rays come the right way.

We talk about the Internet, the Internet and, of course, now it's the "extranet," earthquake preparedness, wireless alternatives, toll fraud, physical security, cable plants and many more topics. We welcome any suggestion for topics and speakers, and I invite the Commission, if they can provide a speaker on the overview of the Commission's work and then maybe specifically on telecom, to give me a call or E-mail. By the way, our E-mail is [IDRA@IDRA.COM](mailto:IDRA@IDRA.COM), and our Web site [www.idra.com](http://www.idra.com).

Just to give you an idea of some of the telecom disasters and events that I've been involved with, of course, power failure is 90 percent of your problem. If you add up all of your events, power is the big one. Then we have outages of central office trunks, data communication overloads, sporadic microwave outages, flooding of telecom operations rooms, which I have had the pleasure of living through a couple of times, telephone system software failures, ring no answers. There is about 40 reasons why you can dial a number and get a ring, no answer. My personal favorite about telecom interruptions has to do with Dessert Storm. I don't know if you remember all the activity, but all of a sudden about 7 o'clock one night, an announcement came up that they were starting operations. Immediately, after that, one of the central offices of the Telephone Company was just submerged with phone calls, was actually put out of business for several minutes due to the amount of phone calls going through. At first you think, well, yeah, everybody is calling to see how they are. Not so. The reason was that central office was the one where all the calls for the lottery went through, and the operation announcement had preempted the

lottery numbers being given out over the TV. Well, everybody picked up the phone and called the lottery.

In conclusion, I just want to urge the Commission to emphasize the importance of telecommunications in support of the nation's infrastructures, and if there's anything we can do to help, please give us a call. Thank you.

MODERATOR ABRAMS: Thank you very much, and let me ask finally: Is there anyone else who wishes to address the Commission who is here?

Thank you. This concludes the public testimony for our meeting today in Boston, and we appreciate very much all of the contributions, the valuable, and specific contributions that you all have made to the work of the Commission.

If anyone would like to submit further testimony to the Commission in writing, we would be happy to accept it, and we'll put it into the record of this public proceeding. We'd also like to encourage you to continue in this dialogue with the Commission, and you can see the table on the outside area as you leave for information on how to be in touch with us.

Thank you very much, and we appreciate your hospitality here in Boston.