THE PRESIDENT’S COMMISSION ON
CRITICAL INFRASTRUCTURE PROTECTION

HEARING AT THE INFORUM IN ATLANTA, GEORGIA

9:00 A.M., APRIL 18, 1997

A PUBLIC MEETING WITH BUSINESS LEADERS AND LOCAL OFFICIALS

Transcript of the above-entitled proceedings heard before the President’s Commission on Critical Infrastructure Protection, Robert T. “Tom” Marsh, Chairman, co-hosted by Mayor Bill Campbell and Sen. Sam Nunn, on April 18, 1997, 9:00 a.m., at the Atlanta INFORUM.

CO-HOSTING THE MEETING:

Atlanta Mayor Bill Campbell
The Honorable Sam Nunn

PRESENT FOR THE COMMISSION:

ROBERT T. MARSH, CHAIRMAN
BRENTON GREENE
JOHN POWERS, Ph.D.
NANCY WONG
PAUL RODGERS
JOSEPH MOORCONES
STEVAN MITCHELL
MARY CULNAN, Ph.D.

Moderator:

MS. JANET ABRAMS, White House Liaison
for the Commission, Director of External Affairs

(IN THE FOLLOWING TRANSCRIPT, A DASH [—] IS USED TO INDICATE AN UNINTENTIONAL OR PURPOSEFUL INTERRUPTION OF A SENTENCE; AN ELLIPSIS [...] IS USED TO INDICATE AN OMISSION OF WORD[S] WHEN READING WRITTEN MATERIAL.)

(IF THE FOLLOWING TRANSCRIPT CONTAINS QUOTED MATERIAL, SUCH MATERIAL IS REPRODUCED AS READ OR SPOKEN.)

INDEX TO SPEAKERS

PROCEEDINGS

THE MODERATOR:

Good morning, and welcome to the Atlanta public meeting of the President's Commission on Critical Infrastructure Protection. My name is Janet Abrams, and I'm the White House Liaison and Director of External Affairs for the Commission. I will be moderating this morning's proceedings.

This is the second in a series of regional discussions being convened by the Commission. Our first was held in Los Angeles last month. And today we're honored to be here in Atlanta.

I would like to begin by thanking our co-hosts for this visit to Atlanta, Mayor Bill Campbell and Senator Sam Nunn. Both gentlemen have provided important leadership on the very issues that this Commission is charged with studying. Last year, Mayor Campbell oversaw the massive effort to protect key infrastructures in the Atlanta area during the Centennial Olympic Games. And Senator Nunn has been a leading advocate at the national level, calling for focused attention on the new and complex security challenges emerging in the Information Age. We thank you both for your hospitality and for your active interest in the work of the Commission. And now Mayor Campbell will officially open the proceedings.

MAYOR CAMPBELL:

Thank you very much. It is a pleasure to welcome you to our city. It is an interesting weekend for you to be here, and we are glad to have you here on this very important issue.

Chairman Marsh and Commissioners and Senator Nunn, ladies and gentlemen, it is my honor to have this Commission meet here in Atlanta. We are also honored to have been selected as one of only six cities that will have these public hearings.

As mayor of a major national economic and cultural center, I believe that the Commission's task really represents the most important study that is currently under way concerning our nation's future in an increasingly high-tech and interdependent world, and I might add a hostile world as well.

Atlanta, perhaps more than any other city, appreciates the importance and the urgency of protecting our infrastructure, our services and our citizens. On three separate occasions in less than one year, Atlanta has been subjected to the devastating psychological and physical trauma of bombing attacks. We have suffered the loss of lives, and we have suffered the loss of peace of mind. And, in fact, we have not fully recovered even yet. Although none of the three attacks targeted our city's critical infrastructure, each bomb nevertheless struck at the very heart of our city.

Our increasing reliance on telecommunications and information technology only heightens our vulnerability as we must now protect ourselves from cyber threats as well as physical threats. We must be aware that today's terrorist can do much more damage with a laptop than with a bomb.

The Commission's recommendations will set the standard for securing the systems and services on which our economy and indeed our existence depends. As Chair of the Transportation and Telecommunications Committee for the U.S. Conference of Mayors and as a member of the FCC Local Advisory Committee, I applaud President Clinton for his proactive approach to this challenge. By appointing this Commission, the President is getting out front on this issue before it becomes a crisis. I call on Atlanta's public and private sector, many of whom I see in the audience today, and on all of our citizens to become involved with this very important issue. National challenges require national solutions. The City of Atlanta is ready, willing and able to find the right solutions to protect our city's and our nation's future.

Chairman Marsh and Commissioners, Senator Nunn, may this public hearing assist you in the accomplishment of your mission. We look forward to assisting you and to being a partner with you as this study comes to a close.

Thank you, and welcome to our city.

(Applause.)

THE MODERATOR:

Thank you, Mayor Campbell. I would now like to invite Senator Nunn to offer opening remarks.

THE HONORABLE SAM NUNN:

Thank you, Janet. The good news for all of you this morning is, being no longer a member of the Senate, I've lost my right of unlimited debate, so you're going to get very brief remarks this morning.

It's my pleasure to join my good friend, Bill Campbell, the Mayor of our great city, Atlanta, Chairman Tom Marsh, Janet Abrams, six distinguished commissioners from around the country, and all of those who have come to testify this morning and also to participate in the audience.

Technology has long been an important instrument of change and power. From the printing press to the steam engine to the light bulb and then the automobile, as well as many other advances, technological advances have altered our lives and changed the course of world history. Today we find ourselves on the front end of sweeping change probably unprecedented in the annals of history. Labeled for lack of a better term and involving a lot of different components all lumped together, we call it the Information Age. Computer networks and information systems are compressing time and space, creating vast improvements in the delivery of goods and services that affect our lives every day, putting huge pressure on dictators that try to have a suppression of information and find that they cannot compete in the world economy and at the same time stifle information in their own society. It's doing all those things as well as, as those in the audience in the military would recognize so well, it's also causing truly a revolution in military affairs.

Ironically, the same technological advances that bring us the advantages of the Information Age, and they are numerous, have given us the tools to disrupt it and to exploit it. Logic bombs, viruses, password sniffers and other tools that can disrupt and destroy computer networks are now available to literally millions of people in this country and around the globe on the Internet itself. In hearings of the Permanent Subcommittee on Investigations, which I chaired last year, we spent about two years looking into this subject, investigating it, working with DOD and Justice Department, as well as others, as well as extensively working with the private sector. After all that, we came out with a series of hearings, and in those hearings it became absolutely clear that our critical computer networks are neither secure nor are they confidential in many, many cases.

A report issued by the General Accounting Office estimated that the unclassified but sensitive network of Defense Department information, that network is experiencing probably — and this is an extrapolation by GAO, but it's a pretty good estimate — probably experiencing as many as 250,000 computer attacks per year, per year, with a 65 percent probable success rate of those who are attacking DOD computers, and, most disturbing of all in terms of the challenge that faces us, a very low detection rate when these incursions occur, and even when detected, a very low reporting rate of the penetrations.

Over 90 percent of all Defense voice and data, about 90 percent of all Defense information transits these networks, including research data, including troop movements, including operational plans, including procurement and including weapons maintenance.

Just as importantly, our nation’s security and our nation’s economy depends on our critical infrastructure. And most of that is owned by private enterprise. And that’s the strength of our system. But we also have to recognize it gives us an unprecedented challenge now, including our transportation system, our telecommunications system, our energy systems and our financial systems, which are probably even more vulnerable to attack and disruption than our government systems.

As these critical elements become more reliant on computers, and they do every day, industry and government will have to cooperate to ensure the reliability of the systems themselves which are not only critical for our defense and security, but also critical for the everyday functioning of our economy.

Our intelligence and law enforcement agencies have unprecedented challenges. Legal challenges are going to be in front of us in the future that we have only begun to even think about today. These intelligence agencies and law enforcement agencies are going to have to have reliable threat estimates that can not only help secure our government systems, but also provide critical data to the private sector that helps them manage their risk.

This cooperation must be a two-way street because much of the information flow has to come from business to government if government indeed is going to be able to put together threat assessments, considering what they have in terms of classified information. So it’s a two-way street, and it will depend on building trust between industry and government in this arena, trust which I must say does not exist today. We had a number of witnesses that were slated to testify before our Permanent Subcommittee on Investigations last year. And at the last moment, they canceled out because they did not want to basically reveal what they considered to be their own vulnerabilities. Now, I understand that. We didn’t subpoena them. We could have. But it tells us the huge problem we have in trying to build a degree of trust. Somehow we’re going to have to create that trust. We’re going to have to figure out how to do it. The government certainly should not be taking over this area. But without that kind of cooperation, we simply are not going to be able to meet the threats of the future.

We should not and we must not wait for an “electronic Pearl Harbor,” as John Deutch has termed it, to begin to address these clear vulnerabilities.

Today we’re very fortunate to have Tom Marsh, and he’s going to be more formally introduced, but he was formerly the Commander of the Air Force Systems Command and has been involved in almost every facet of the new technological age. We're fortunate to have Tom chairing this panel. We're fortunate to have the commissioners with us this morning who are going to be giving so much of their time and effort in this. They bring a great deal of expertise in these areas. And we are also fortunate, most fortunate to have in Atlanta here today a number of eminent witnesses to discuss these issues, as well as the experts who are in the audience.

So thank you all for coming. I look forward to participating, and I look forward to learning. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Senator Nunn. I would like now to introduce the members of the Commission who are with us here today. By Executive Order, the group is a mix of individuals representing both private industry and the government. After these introductions, Chairman Marsh will give a brief overview of the work of the Commission, and then public testimony will begin.

Moving across the dais from your left to right, we have Brenton Greene, Commissioner from the Department of Defense, John Powers from the Federal Emergency Management Agency, Nancy Wong from Pacific Gas and Electric, and then Chairman Marsh, whom Senator Nunn just introduced. He is a retired four-star Air Force general. He's now an executive in the aerospace industry. He has served on the boards of numerous technology companies, and was CEO of the Thiokol Corporation. Then we have Paul Rodgers, former Director of the National Association of Regulatory Utility Commissioners, Joe Moorcones from the National Security Agency, Stevan Mitchell, Commissioner from the Department of Justice, and Mary Culnan, Professor, Georgetown University, School of Business.

And now I would like to ask Chairman Marsh to give an overview of the Commission's work.

CHAIRMAN MARSH:

Thank you, Janet. Thank you, Mayor Campbell and Senator Nunn. On behalf of all the Commissioners, it's a real pleasure to be here in Atlanta this morning. 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, as we view them, 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 15th when President Clinton signed the 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 are looking at? They fall into five basic groups.

First are 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 disruption 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 infra-structures 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 am often asked is, “Why now? Why this Commission now?” The answer is that we want to address this issue before a more serious problem develops. Many companies, such as utilities, are very familiar with natural hazards. Those of you living here in Georgia and other parts of the South are familiar with such hazards, including floods, tornadoes and hurricanes.

Now, this Commission will not stop the forces of nature. We will, however, deliver a strategy to contain certain acts of man. That’s because today we are confronted with an entirely new set of hazards that are man-made. Technology has created an interconnected world. But each connection creates new exposure 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 critical infrastructures, identify relevant policy and legal issues, and assess how they should be addressed, recommend to the President a national policy and implementation strategy for protecting critical infrastructures, and finally propose any necessary statutory or regulatory changes to make that possible.

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, after all, it owns and operates most of the critical infrastructures.

Furthermore, government relies on these private sector infrastructures for services required for national defense and our very well-being.

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. That’s the only way we will find solutions that work for everyone.

So again, we appreciate your being here today, and we appreciate Mayor Campbell and Senator Nunn taking time to be here. And we look forward to hearing what you have to say. And furthermore, should you wish to talk to us at any time after this morning, please write or visit us on the World Wide Web at the address shown on the screen: www.pccip.gov. We thank you very much. Janet?

(Applause.)

THE MODERATOR:

Thank you, Chairman Marsh. Before we move on to public testimony, I need to offer a note about time. We have a very full program this morning. And my job is to encourage us all to keep to the schedule. Each presenter has been asked to limit his or her remarks to ten minutes. I will be watching the clock, and when you hit the nine minute mark, I'll wave this very subtle orange sign and ask you to begin wrapping up. At ten minutes, we will have to let you know that your time is up. And please know that your written testimony will be submitted in its entirety in the official record of the Commission.

And finally, if there is anyone here in the audience who has not yet filled out a yellow sign-in card at the table behind you and you would like to speak, please do so at any time during the hearing.

So we're ready to begin, and our first presenter is Kent Alexander, U.S. Attorney for the Northern District of Georgia.

MR. ALEXANDER:

Thank you, Janet. And thank you, Chairman Marsh. I should start, also, by thanking Chairman Marsh's staff member, Elizabeth Sauer, who called this week to ask me if I needed any assistance with my testimony. Until that call, I thought I was giving "Welcome to Atlanta" remarks. So rather than extol the virtues of the Atlanta Hawks, the Atlanta Braves and my favorite restaurant, I am now prepared to share some relevant remarks with you.

The President's Commission on Critical Infrastructure Protection to my mind is a great idea, not because the President appointed me to my position, but because of my experience with the Olympics. For the two years prior to the Olympics, the FBI organized mock exercises designed to address disaster scenarios ranging from diplomatic kidnappings to massive power outages, to water supply poisonings, to bombings, and so forth. Sadly, the last threat was realized in the form of the Centennial Park bombing, but fortunately none of the other threats were. And based on what I learned prior to the Olympics, all of those threats are very real, and most of them will be addressed today at this hearing.

The particular threat I wish to address today is the threat to the networked communication infrastructure posed by computer hackers. There are today and have been for many years marauding bands of computer hackers and individuals bent on breaking into systems. As these individuals mature and have different financial needs, the malicious nature of these break-ins is going to do nothing but increase.

First I will talk about a case I prosecuted about seven years ago or eight years ago at this point. And then based on that case and later developments, I will try to draw some constructive suggestions to share with the Commission for their consideration.

The case is called the Legion of Doom case. In 1989 I was an Assistant U.S. Attorney. The Chief of the Criminal Division brought in a Secret Service agent to my office as I was behind closed doors, playing a computer game — "Dr. J. versus Larry Bird Basketball" on my Commodore 64 — with a friend. Far from being upset that I was doing that, when the Chief of the Criminal Division opened the door, he swelled with pride and told the agent with glee, "You see? We do have a computer expert." At the time, as unfortunate as it was, I was considered a computer expert. And equally unfortunate, the agent was pleased.

From those very modest beginnings of that case came the Legion of Doom prosecution. There has not been a large number of federal or state hacker prosecutions, but there have been a few, again, that being an early one. Essentially, the case involved a loose-knit band of computer hackers who were bent on breaking into as many systems as possible, viewing the information, often downloading information, and sometimes profiting from that information. They claimed from the privacy of their own bedrooms they had the ability to do any number of things, including downloading medical records, national security information, military records, credit bureau records. They claimed to have the ability to tap into phones. They also claimed that they had the ability to shut down phone service in entire cities. Based on what I saw through this prosecution, I cannot dispute any of those claims.

Essentially they went about breaking into the various systems around the country by first targeting BellSouth, a regional Bell operating company. Through BellSouth, they were able to loop their calls through different carriers and packet switching networks around the country and break into systems in a virtually untraceable way. Fortunately in this case, BellSouth decided to come forward and report this conduct to the Secret Service. In working with the Secret Service, BellSouth was able to trace their activity. If I could get the first slide, please.

(Slide #1.)

And when we executed search warrants, we found a number of items. We found medical records, bank records, credit bureau records, records of wire taps, passwords, dial-ups, tutorials on how to break into systems, and a lot of other incriminating information. Ultimately, based largely on BellSouth's cooperation in this case and their expertise, we were able to prosecute three members of this organization. All three were convicted, and all three served prison time. Also, as a side benefit, BellSouth's system itself was far more secure afterwards than it was before. BellSouth estimated that their cost of replacing passwords was $233,000. Their cost in the investigation itself was $1.5 million. And their cost in securing the system — or resecuring the system — was $3 million. So it was nearly $5 million in damage costs. Now, this case occurred again eight years ago. And in the intervening eight years, we of course have seen in the cyber arena an explosion of growth. Today, unlike eight years ago, voice mail is standard; e-mail is standard; bank tellers have become all but anachronisms; and companies like America Online, which were in their embryonic stages in 1989, now have millions of members, and if service goes down for a day, it becomes front-page news. In some ways, Aldous Huxley's *Brave New World* has arrived.

Now, while I am overall a true cyber fan and very excited about the advancements in our high-tech era that we are living in right now, I'm also a prosecutor who has spent ten years dealing with the criminal element. Based on Bureau of Justice statistics released last month, there is an estimated 5.1 percent of the United States population that will at some point during their lifetimes serve prison sentences in state or federal institutions. If we deal with that 5.1 percent as the "criminal element" and bear in mind that that criminal element through primary and secondary school education is receiving more education in using computers than most of us in this room have received to date, we are in trouble. That is not to suggest that murderers and rapists are necessarily going to be using computers to accomplish their evil deeds, but when it comes to extortionists, when it comes to scam artists, when it comes to anyone bent on doing wrong, they do have computers as a weapon. And that causes great concern. My biggest surprise since this Legion of Doom prosecution until now has been that we have not seen a major disaster in the telecommunications arena. I fear that it is inevitable.

What can we do to address that problem? What can the Commission do to address it? Next slide please. *(Slide #2.)*

I am not going to be presumptuous enough to suggest that I have all or even most of the answers, but I will submit eight suggestions for your consideration.

Suggestion #1: Train law enforcement. There is a gap between law enforcement's knowledge and the expertise in the virtual community that lies out there, even among the 14-year-olds that Chairman Marsh mentioned. Fortunately, that gap is closing quickly. In 1991, the FBI established the National Computer Crime Squad. That same year, the Department of Justice established a Computer Crime Unit headed by Scott Charney, and that unit has now been lifted up to the level of a section within the Department. In 1995, the Attorney General, Janet Reno, established the Computer Telecommunications Coordination Program. That program allows for advanced training of at least one prosecutor in each of the 93 U.S. Attorney's Offices to develop expertise in both computers and telecommunications. There are many other training steps being taken as well, but we need more. So to the extent that Congress can fund additional training for law enforcement, particularly as we still have a gap that needs to be closed, I encourage it.

Suggestion #2 is to update computer hacker laws. Technology, as we all know, is a very fluid concept. It keeps expanding and expanding exponentially. If we don't tailor our laws with essentially escalator clauses for technological advances, those laws become obsolete very quickly. And we also need to revisit the laws that we have on the books now. For instance, under the sentencing guidelines under U.S.S.G. § 2F1.1, you determine what kind of time that someone who breaks into a system will do. Let's say someone breaks into a corporation's system and they steal all of the corporation's records, which is tantamount to taking every file in the corporation out, but they are caught before they can distribute those records. The way the sentencing guidelines are set up now, the loss arguably is zero and the term of incarceration is probation. Those kinds of issues need to be addressed.

Suggestion #3: We need to encourage, as Senator Nunn mentioned, the private sector reporting of cyber attacks. One reason there have not been a lot of computer hacker prosecutions is that very few corporations report the attacks on their systems. BellSouth turned into a model corporate citizen by doing so. When others do not do so, we embolden computer hackers bent on criminally breaking into systems by making them think that nothing will ever happen — that it will be swept under a rug. While I recognize the private sector's need to consider its market share, civil liability and other factors, we need to develop a more trusting relationship in sharing this information with law enforcement.

Suggestion #4: Balance civil liberties with government data collection. I don't want to get into too much detail here because it's a very sensitive topic. But basically, taking law enforcement as an example, the area with which I'm most familiar, we have agencies that do collect data, but there are limitations on what data they can collect on criminals for civil liberties reasons and for other good reasons. I fear, though, in this Information Age that if we place too many limitations on collecting data on criminals, we’re not going to effectively be able to pursue the criminals. Similarly, if the agencies, the law enforcement agencies, don’t share information with one another, we are under constraints as well. Additionally, that information oftentimes needs to be shared with the public to make the public aware of the threats. It is a nettlesome issue, and we by no means want to have a Big Brother society out there, but we need to start taking advantage of the Information Age in the law enforcement environment.

Suggestion #5, next slide, please. *(Slide #3.)* Educate our youth. Right now, there is a disturbing view among many youthful computer users that information belongs to everyone. Put another way, it’s all right to break into a system and steal information. That obviously is not the message we need to be sending. Prosecutions can only go so far, and it’s important that we continue prosecutions to send the message of legality and illegality. But in the Legion of Doom case, one of the college students prosecuted, when asked on *Dateline NBC*, “What’s the lesson in your story for other hackers?” said, “Don’t get caught.” So obviously prosecutions alone are not going to do the trick. I encourage primary and secondary civic education on this matter.

Suggestion #6: Publicize easy steps to avoid attacks. There is a lot we can try to do that will never get accomplished. Publicizing steps like shredding documents, turning off modems at night to avoid after-hours attacks, and watching ex-employees and disgruntled employees are easy steps that we can all take in the private and public sector.

Suggestion #7: Promote international cooperation. It is shortsighted to view only our national infrastructure as the vulnerable victim from within or from a domestic standpoint. The national infrastructure is vulnerable from an international perspective. Going back to 1986 with Clifford Stoll and his Cuckoo’s Egg account of a KGB-paid German hacker breaking into military labs in California, we know that that threat is very real, so we need to guard against that as well.

And finally, Suggestion #8: Do not underestimate the threat. Right now we have been fortunate so far to mostly have accidental attacks on our telecommunications infrastructure. We’ve had a couple of lines of software dropped by AT&T. We’ve had a Cornell hacker back in 1988 design a worm to basically eat memory, but the worm got out of control. Within twenty-four hours, it hit 6,000 computers and caused an estimated $98 million of damage. We have not yet seen a wide-scale malicious hacker attack, and I’m afraid that is coming. The good news in it all is that we no longer rely on Commodore 64’s to protect ourselves from it.

Thank you very much.

(Applause.)

COMMISSIONER GREENE:

One question on your testimony. Your Recommendation #2 on update computer hacker laws, the Department of Justice was instrumental last fall in helping Congress pass the National Information Infrastructure Protection Act of 1996 which significantly advanced the definition of felony-misdemeanor intrusions, laid out the penalties, and improved our ability to do just what your number two recommendation is. Do you feel that that law is inadequate and needs to be bolstered further or do you think that that will answer the mail?

MR. ALEXANDER:

That law, which is Title 18, Section 1030 of the U.S. Code, is vastly improved as a result of those efforts last year. There are still improvements that we need and a broadening that we need. Scott Charney, who is head of the Computer Crime Section, and I co-authored an article in the *Emory Law Journal,* and we list some of the suggested improvements in there. It's more, though, a bellwether for the future. Right now we can rely somewhat not just on that statute, but on Section 1343 of the same code, the wire fraud statute, to accomplish much of what we need. But, for instance, with wire fraud, a question that comes up, with remote communications, wireless remote communications, does the wire fraud statute apply? Maybe not. And does §1030, even with the improvements with unauthorized access, apply? Maybe or maybe not. So it's just an area we need to constantly revisit. And I would refer you to Scott Charney as the real expert in that area.

COMMISSIONER GREENE:

Thank you very much, Kent.

MR. ALEXANDER:

Thank you.

THE MODERATOR:

Thank you. Our next presenter is Dr. Wayne Clough, President of Georgia Institute of Technology.

DR. CLOUGH:

Thank you, Chairman Marsh and Mayor Campbell, Senator Nunn, members of the Commission for this opportunity to testify before you on the important subject of infrastructure. I'm President of Georgia Tech, but by profession, I'm a civil engineer, and I have practiced civil engineering design for about thirty-five years. And so I have worked on projects all over the world that relate to the physical infrastructure. As President of Georgia Tech, I also sit apparently on a hotbed of possible hackers and other individuals who access the Internet on a daily basis thousands and thousands of times to do things as frivolous as tell me why they shouldn't pay their parking tickets to much more serious things as to conduct international research. So I do bring a little bit of a unique background, I suspect, to this subject.

I use the term "infrastructure" to refer to both manmade physical infrastructure as well as the virtual infrastructure which are important to our civilized society. Perhaps one class of physical infrastructure that we shouldn't forget is what the earthquake engineers call life lines. They are very important. These are the systems that typically spread over long distances, such as transportation, water and sewer networks, communication networks, and power networks. Do we need these systems? Of course. Everybody agrees we need the systems. Is society at large interested in them? Not unless they go out. Do our citizens want to pay to keep them up? Not very much, and not very often.

And that's why, having lived in Seattle for a while, I learned that the City of Seattle still supplies water to itself through logs that were hollowed out a hundred and fifty years ago and placed in the ground. That's why the City of Atlanta has a tunnel with unreinforced brick that runs beneath my campus that was built in 1896. And it's still an important part of Atlanta's infrastructure. Known as the Orme Street Sewer, this engineering marvel still works, but it's overloaded and in poor shape. I congratulate Mayor Campbell as being the first administration to recognize this as a serious problem and to undertake the serious efforts to replace this structure. And that is well under way. My only concern at this point, Mayor Campbell, is that the old sewer still runs under the north stands of Grant Field, and I can envision a day when our students see a great play on the football field, jump up en masse, and slowly sink into the ground. That would be particularly unfortunate for Georgia Tech because we haven't had real good scores lately by our team, and we would probably have to call that play back.

But Atlanta is certainly not the only city facing serious infrastructure problems because approximately 95 percent of our infrastructure is built. The interstate system is largely built, and it is aging. And maintenance and replacement of these facilities is now the challenge. And all you have to do is look around to see that. In many cases, we are victims of our own success. The freeway systems are overloaded because people use them far more than we anticipated they would.

Clearly there's a funding issue, not only the present issue, but the long-term funding issue, if we want to have a viable infrastructure system for our children and the generations to follow.

I think it's important to also not neglect the fact that research will be important as we move forward in the future. Already we have new materials to resist extreme environments that could help us. We have improved construction and maintenance techniques. We have dampers and flexible bearings to control building vibrations that didn't exist before. We have smart buildings and highways, intelligent cars, more efficient material transport systems, and even better systems for dealing with contractual disputes. These are here. They need to be used. They need to be implemented as we move forward to replace our infrastructure.

We also can't neglect the fact that we need to do continuing research in these areas. If there is a serious problem in this area that I see, it is that we are substantially behind the areas of the world such as Europe and Japan in our policies for use of research and implementation of research. And so you will find as you go to infrastructure projects today that most of the construction, most of the maintenance, most of the repair is being done using foreign technology and being done by overseas businesses, not U.S. businesses. This is a serious policy area I think that the nation needs to address.

Now, more recently it has become the practice to use the term “infrastructure” to talk about our virtual systems of computing and information networks. Computing and information networks are clearly part of the future, an important part of our future. And recently, Governor Miller spoke at the dedication of our Georgia Center for Advanced Telecommunications Technology and commented that Atlanta had little reason to exist except for life lines and infrastructure because it grew up as a hub for rail traffic. It later recognized the need for interstate highways and a great airport. And today it ranks in the front as a city that has great fiber optic systems. And Governor Miller has proclaimed that Georgia will be the preeminent center in the world for telecommunications in twenty years. And Georgia Tech is assisting with the research and development needed to reach this goal.

There are serious issues facing this country, though, if we're going to continue our research efforts because the federal government is downsizing its funding for research and development.

I will give you one example of a model I think that does work. Working with Georgia Power Company, Georgia Tech recently dedicated a lab and converted it into a national lab from a Georgia Power facility, and we call it the National Electric Energy Testing Research and Application Center, or NEETRAC for short. This center is funded not by Georgia Power or the State of Georgia, but by fifteen partners from all over the country, including private corporations, utilities, research consortia, some federal funding, and the State of Georgia represented by Georgia Tech. I think if we are going to do research effectively in the future in a downsized environment, we have to look to collaborations to make them work. And I cite this as one example for you.

Now, I think the computing and informational infrastructure brings its own special dimensions, but don't forget it's still linked to the physical infrastructure. Because we now have high-speed electronic commerce, any outage in physical structures, the effect of that is magnified. An example was in the Loma Prieta earthquake in 1989 in San Francisco when the Oakland Bay Bridge went out. The losses were magnified in that earthquake because the telecommunications systems also were affected and could have been affected more because two buildings almost fell. So these infrastructure systems are linked, physical and virtual.

Now, our campus also understands what can happen when you have the loss of a communications system. This year we have become much more active in delivering education by on-line techniques, as well as distance learning. One of those methods that we use is satellite delivery. Our AT&T satellite this year went out and went silent. It was a sudden and stunning event. The causes for that event were attributed to solar flares or meteorite strikes. Nobody to this day knows. All they know is that that satellite simply disappeared and never responded again. It was a stunning blow to our delivery of educational services. And it's something I think that this Commission should think about — what happens when we have sudden lapses of important infrastructure venues such as the satellites that we deliver our educational services on. And this will become more important in the future.

Now, beyond the natural disasters that can occur in terms of our delivery of services, obviously we've talked about those issues of sabotage and security breaches already. At Georgia Tech we have extensive studies under way of the issue of cyber security, Internet security. And those issues range from the technical to the question of cost: how much cost will it take to actually implement an effective security system, how will you manage it, who will manage it in each operation, and will these be effective? Because of the importance of this topic, the recently established Sam Nunn International Forum series will devote its second venture to the issue of cyber security. This is a joint venture of the University of Georgia, Emory University and Georgia Tech. And we will host that here in Atlanta probably either in the fall or in the spring. This conference will bring together the world's experts on the issue of cyber security. And we think that it is a good place to hold that in an area like Atlanta where we have so much invested in the telecommunications industry.

Now, the Sam Nunn Forum is about understanding issues, but also to educate, educate our students, educate ourselves. If we're to succeed in addressing the physical and virtual infrastructure challenges, we need not only to be able to educate the students who are on our campus, but we must educate those who have graduated and are now in the work force about the rapidly changing world of infrastructure. We think Georgia should be a leader of that, and Georgia Tech will do its part. We're working hard to wrap up our offerings in this area, but as you think about these types of delivery mechanisms in the future, realize that old forms of support for these systems will not be adequate and that we really need to develop new ways of supporting the national delivery of educational services. Much of that is already being done through the National Tech University which Georgia Tech supports. But you should think about that as well. There should be some policies in regards to how we move forward in the future.

In conclusion, I think it's clear that this nation's future is underpinned based on both its physical and its virtual infrastructure systems and that there are serious concerns and challenges for us. We need to develop the long-term funding to maintain the huge amount of physical infrastructure that's already in existence. We need to use the latest technologies in the future and to encourage the development of new technologies. We need to develop the means to protect our virtual systems and ensure access to education about infrastructure for the generations that are coming to our campus as well as those who come and then graduate. And we certainly need to create the appropriate policies to encourage the positive research that needs to be done for both the physical and virtual environment systems.

So I thank you and congratulate you on taking on the task that you're taking on, and I think it is very important to all of us in the future. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Dr. Clough. Our next presenter will be Gary McConnell, Director of the Georgia Emergency Management Agency (GEMA) and former Chief of Staff, State Olympic Law Enforcement Command.

MR. GARY McCONNELL:

Thank you, ma’am. Mayor, Commissioners, Georgia’s pride, Senator Sam Nunn, it’s a pleasure to have you in Georgia. I probably, as you can already tell, will vary a little bit from the two presenters who have just been up. I’m more into having to do what this Commission and the leadership of this country decides that we need to do for infrastructure. Some five years ago when Atlanta was announced as getting the 1996 Centennial Games, we created an infrastructure committee to look at the infrastructure in Georgia. What we tried to do was provide a forum to bring the public and the private sectors together and provide some leadership and to try to change attitudes a little bit. What we’ve got to do and what we’ve tried to do in the past five years is to get the Southern Companies and the utilities and the infrastructure owners and corporate folks to sit down with the government, both on the local, state and federal level, to develop some trust, to provide some leadership, and to give each group a forum to openly and honestly discuss our issues. There is a tremendous void, we’ve found, in this area of any one central place for everybody to sit down and talk about those issues. The private corporations certainly know what their conditions are, what to be on the lookout for. Government on some level knows some of that. The information is there. It has been developed. I think our greatest challenge in actually doing it is providing the forum for everybody to sit down and share that information and to look at issues such as open records; what can corporations give state and federal agencies without having it on CNN tonight, how to address those issues where we can get the information we need and they feel comfortable providing that information, but also to protect their corporate rights.

The three or four things that we did I think to have a successful Games as far as the infrastructure is concerned was to try not to reinvent the wheel and to be open and honest about it, but the utmost thing was to send, and I’ll use — I hope the companies don’t mind — I’ll use Georgia Power and AT&T for examples. They know where their critical facilities are. They know where the critical points of disruption would be. Sometimes we forget to get into a room and share that information with each other. You do not have to have a nuclear weapon from somewhere to disrupt the utilities in this state. I know Sen. Nunn will know what I’m talking about. You can take a simple three-feet piece of log chain and cut the power out of downtown Atlanta if you know where to clip the log chain.

What you’ve got to do, folks, in my opinion is to show — and the Presidential Commission is doing that — is to show the leadership. Get your governors across the country involved, because a lot of us, very honestly, do not work for the federal government. We work for our boss at the

State Capitol. If they see the importance of infrastructure, you will see the states certainly more involved in infrastructure protection.

And we also have to change habits, as I said earlier. Historically, we have had very little infrastructure problems in this country other than natural disasters. We're in a different society now than we were five years ago. Folks in Perry, Georgia, or Atlanta, or wherever you want to use for an example, think different. The world thinks different about our infrastructure. It is the single most important thing we can do as a nation to keep this country on the road to success.

If you don't think infrastructure is important, and I don't want to talk about cyber space and all of that because I personally do not understand it, but if you think infrastructure is not important, you go home tonight and go to your main switch box at your house, and you pull that switch box and go out to the street and cut the water off and wait until Monday before you turn it back on. You will see how important the infrastructure is to this country.

If you wanted to disrupt the '96 Games, one person could take an AK-47 down to the Opening Ceremonies, and besides killing folks, it could have caused a lot of us to lose some hair. But if you really want to mess up a major event, turn the power off. Odds are, if we have a terrorist incident in the State of Georgia today, it will not affect you folks being able to get back on your plane and go to wherever you have to go this afternoon. But if we want to keep all of you in Atlanta today, turn the power off at Hartsfield. And you don't have to be a real rocket scientist. Even a former country sheriff can figure that out. You can kill 25 people on the street today with an AK-47, but you can disrupt the financial institutions across this country in thirty seconds with a laptop computer.

Our public safety folks, not just law enforcement, but fire and the entire public safety arena, do not have the capability to deal with that. You can look at the incidents in California with the earthquakes or in South Georgia two years ago with the floods, or in Minnesota today. Those folks can tell you what infrastructure disruption will cause. And I think sometimes we forget how it reaches each one of us. The simple things, ladies and gentlemen, you cannot do without the infrastructure. And I will use one example in closing. The City of Macon, Georgia is a city of 190,000 people. Three years ago, we lost water service in Macon for twenty-one days because of the flood. We could just as easily have lost that because of somebody with a bottle of sarin gas. You try to furnish water to a city of 150,000 — much less what would happen to the City of Atlanta or New York or Chicago — for twenty-one days. The Georgia National Guard and various other folks cannot produce that much water. When you’re trying to coordinate the hospitals’ flushing at two, ten and seven or whatever, three times a day, so you can conserve your water, when you’re trying to figure out how the banks in a metro area get their electronic transfers because the infrastructure does not work, it is the most important issue that we’ve got to deal with today.

I’ve had the privilege of dealing with Dr. Powers and some other folks from your Committee looking at the possibility of trying to provide you with in-depth, how we did the Olympics as far as infrastructure is concerned in Georgia, what worked and what didn’t work. I’m not here to try to tell you that everything we tried in that five years was a success. It was not. The majority of it was.

And I guess the three keys in closing I would like for you to leave here with is that somebody, whether it’s the Presidential Commission or the national governors or whoever, has got to show some honest concern and leadership in the area. Please do not just give it lip service. It has got to be a true team. It’s got to be your private providers; it has got to be the corporate citizens; and it has got to be your smaller utilities, too. It cannot just be the Southern Companies of the country. It has got to be independent telephone providers. It has got to be your small EMC or electrical co-op folks across the country. And I guess this is probably more me than anybody else, but if we’re going to do it, folks, let’s do not talk it to death till it’s too damn late. You cannot solve the problem after it’s over. You’ve got to do something about it before it happens. And if we don’t do that, not only will we be embarrassed, but the folks in this country certainly will have a reason not to trust us, as they do occasionally now. We’ve got to provide the leadership. We’ve got to get involved. And we’ve got to do it on a timely basis.

Thank you. We appreciate your being here and appreciate your time. Thank you.

(Applause.)

THE MODERATOR:

Thank you very much, Gary. Our next presenter will be Bill Killen, Vice President with Cox Enterprises.

MR. KILLEN:

Senator Nunn, Mayor Campbell, Chairman Marsh, Commissioners, thank you very much for the opportunity to address you this morning. My name is Bill Killen, and I’m the Vice President of New Media for Cox Enterprises, which is headquartered right here in Atlanta, Georgia. And for those of you who may not know, Cox is among the largest media companies in the U.S. And we began as a single newspaper in Dayton, Ohio in 1898. The owner of that paper, James M. Cox, went on to become a three-term governor of the State of Ohio. And in 1920, he was the Democratic nominee for President of the United States.

The Governor left us with a great heritage because he believed in developing new technologies to create emerging media businesses that serve all of the communities in which Cox operates. The result is that today, Cox Enterprises owns and operates newspapers and radio stations, TV stations, and cable systems in communities all across the U.S. For example, here in Atlanta, we own the *Atlanta Journal-Constitution,* WSB-TV, WSB-Radio. We own cable systems all across the country, serving major cities like San Diego and Phoenix. All of that adds up to a company that has annual revenues of over $4.6 billion.

Our company continues the spirit of the Governor in embracing new technologies. Cox has been a leader in developing the most modern fiber optic cable TV plant in the industry and the new 2-way services, like telephony and high-speed Internet access, which can be delivered over that network.

An example is in 1991, Cox bought control of and helped drive the growth of a company called Teleport Communications Group. Teleport is the leader in what is known as the alternate access or the alternative local exchange carrier industry. Teleport serves big telephone customers by providing an alternative pathway to the local telephone company. Many of these customers want multiple communications paths for their important telephone and data transmissions. So this competitive access business sprang from government policies that encouraged competition and from the entrepreneurial spirit of Teleport and its backers: four of the largest cable TV operators in the country whose cable networks also helped drive Teleport’s growth. So today, telephone customers have choices, providing vendor diversity and route diversity for their phone connections. And the country has a more robust and diverse telephone network which is less vulnerable to single point outages and large scale failures.

Cox is also a leader in wireless telephone services based on our cable TV platform. Cox in fact was awarded a Pioneer Preference by the FCC for its development of cable TV-based wireless telephony, and it is today building out a PCS wireless phone business in southern California, which will compete with cellular and traditional phone companies. But again, these multiple networks provide consumers with a choice, and it provides the nation’s infrastructure with a network less prone to single-point, single-vendor failure. So government initiatives which have encouraged these new services we believe have served the public well.

Cox is also building Internet infrastructure, again using our modern 2-way cable plant. Cox is connecting PC's in consumers' homes with high-speed connections to the Internet. These connections are up to a hundred times faster than a typical telephone line connection and cost only about $45 a month, a price we expect will decline.

Cox is also an investor in a company called @home (At Home). @home is building a national private, high-speed Internet backbone to allow our local cable Internet connections to be even faster. So the development of @home will help ensure the continued growth of the Internet and provide added capacity, and again, network diversity to a rapidly growing industry.

So we hope that government policy makers will keep in mind the importance of the cable TV infrastructure in building a diverse communications infrastructure for the country. Cable TV is not just about video programming. Our broadband networks also deliver wired telephone, wireless telephone and high-speed Internet access to the home, to businesses and to schools across America.

On the topic of school infrastructure, it's important to note that Cox has provided free cable TV hookups to 90 percent of the schools inside its cable TV franchise boundaries and has provided a total of $60 million worth of hookups, wiring, and educational materials to schools through Cox's Cable-in-the-Classroom Program. Now, as this cable infrastructure is being upgraded to 2-way, Cox has begun offering high bandwidth Internet connections to schools as well. As to government policy in this area, Cox believes that any government subsidies which would encourage Internet connections to schools should be apportioned according to bandwidth, which would encourage the building of high-speed, high-bandwidth, many megabit-per-second Internet connections like those that cable can provide. Cox and the cable industry will continue to help meet the President's goal that "every 12 year old be able to log onto the Internet."

Now, in addressing the need to have compelling local content for consumers on the Internet, Cox has also recently created an entirely new division called Cox Interactive Media, which builds Internet World-Wide Web sites with engaging content and information about the cities in which Cox operates. Think of these "city sites" as sort of an online newspaper, only better, because it also includes interactivity and e-mail and chat and forums for all kinds of local special interest groups, from the tennis club to ballet enthusiasts. Cox is building these "city sites" in seventeen markets across the country in the coming months. A good example is our Access Atlanta service which we launched here in January, all about life in Atlanta.

As a content provider on the Internet, Cox is also faced with a number of difficult issues. First is the matter of copyright protection. The Internet allows a very easy transfer of digital files. As our database listings, such as our newspaper classifieds, are posted on the Internet, along with other forms of our intellectual property, they are more prone than ever to unauthorized use. So we would urge that government policy makers should ensure that copyright protection of databases and other intellectual property be extended into the Internet world. And on copyright and hacker intrusions, we encourage the government to be a very vigilant and vigorous prosecutor.

The Internet offers a whole new array of exciting commerce and communication. Cox supports the Administration’s enlightened view as stated in its Internet White Paper, entitled, “A Framework for Global Electronic Commerce.” And that document said that, “Widespread competition and increased consumer participation in marketplace choices, not government regulation, ... should be the defining features of this new digital age.” And I would add that if this policy is followed, private companies like ours will continue to aggressively seek to build new services and diverse routings in cities across the U.S. in the pioneering spirit of our founder, James Cox. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Mr. Killen. Our next presenter will be David Dreesen of the University of Georgia.

DR. DAVID DREESEN:

Thank you for the opportunity to be here. Thank you, Mr. Marsh, Sen. Nunn, Mayor Campbell. My remarks will be somewhat brief, but perhaps a little bit offbeat for what has been said here already.

I’m at the College of Veterinary Medicine, and I’m speaking for our animals I guess you might say. Over the past several years, the United States has been plagued with what seems to be an inordinate number of natural disasters. Hurricanes, earthquakes, tornadoes, floods, and blizzards have all been a real problem to our American citizens. The citizens of North Dakota and Minnesota are suffering as we speak.

When such disasters strike, individuals often voluntarily leave their homes or they are required to do so by various governmental agencies. These individuals are generally housed in what are termed disaster centers, usually schools, civic centers, community centers, or similar buildings. The Federal Emergency Management Agency, along with various state and local agencies, usually do a very good job in responding to the needs of the people that are affected and these people who are required to leave their residences.

The infrastructure has been and is continuing to be developed to aid and assist victims of such disasters. However, from the governmental side, both federal and state, the infrastructure to cope with the companion and food animal victims of such disasters is often woefully lacking. When people are required to leave their homes as a result of some calamity, they must, more often than not, leave their pets behind or make some arrangement for the well-being of the animals on their own. This creates a major problem oftentimes for the agencies involved and for the individuals.

You must remember that the dog and cat and many other species of companion animals are usually regarded as a member of the family. In this era of geriatrics, the pet commonly becomes a surrogate partner when a spouse dies. This displacement thus creates severe stress on the pet owners, often making them very reluctant to leave their homes and not cooperating with the various agencies.

Food animals also represent a significant economic investment, and when lost as a result of a disaster, may cause family ruin. The American Veterinary Medical Association, as well as various state veterinary associations and schools of veterinary medicine, have developed emergency preparedness plans to alleviate and care for such animals. The AVMA has signed an agreement with the U.S. Public Health Service to provide veterinary medical assistance teams to the federal response effort. However, these teams, as well as local veterinarians, are often not requested by FEMA or other federal or state agencies to the detriment of the animals involved, not to mention their owners.

I take this opportunity to urge the Commission to make certain that the veterinary community is recognized as an integral partner within the infrastructure that is continuing to be developed for the multifaceted emergency responses to any disaster.

Veterinarians are experts in the management, health-care and control of animals, as well as diseases that are common to both humans and animals and the transmission of such diseases that often occur as a result of some type of disaster. The Assistant Surgeon General of the United States, Dr. Roscoe Moore, has stated that, and I quote, “Veterinarians are under-represented as members of disaster medical assistance teams.”

We urge you to utilize the doctor of veterinary medicine in all aspects of emergency services, just as the human medical doctor is used in various services. These veterinarians can be used either through various veterinary medical organizations or as individuals. Everyone is going to be better off for it: the owner of the pet, the owner of the farm animal, and their well-being and care.

I thank you for allowing me to present these comments. I know they are a little bit different than perhaps some of those that have been mentioned, but I believe as part of the infrastructure for emergency services, this is a very real problem today. Many individuals do not like to leave their homes because of the pet animal or the farmer leaving his area because of the food animals. These animals must be cared for and taken care of, and an infrastructure must be developed to do so. Thank you.

(Applause.)

THE MODERATOR:

Thank you, Dr. Dreesen. Next I would like to invite Major Jon Gordon of the Atlanta Police Department to testify.

MAJOR GORDON:

Thank you very much. Good morning, ladies and gentlemen, Mr. Mayor. To begin with, let me give you a brief overview of my role regarding the Olympic security preparations. I was in charge of our agency planning office for four years, and I also chaired the day-to-day management committee on the interagency preparations that took place.

One way of looking at our Olympic security preparations I think is to break then down into three phases: the planning phase, the transition phase, and the operations phase. Planning required a lot of effort on our part, but we really didn’t have any sense of whether or not those plans were any good or not until we put them through the testing that we did during the transition phase, all of the exercises that we did to simulate Olympic-like conditions. And I think that is the reason why, when it came time for operations, we were as successful as we were.

But early on we recognized the need to include the infrastructure community in all phases of our preparations, including operations. During the planning phase, we had an infrastructure subcommittee which involved the direct participation of many of the critical providers, such as

Georgia Power. During the transition phase when we conducted all of our exercises, the infrastructure community was right there alongside of us to demonstrate that they had an understanding of what our needs were and how they would participate in the upcoming operations. And of course, during the operation phase, they were with us as well, located with us in our Joint Coordination Center throughout the entire Olympic operational time frame.

I believe that our public safety community here recognized the importance of public-private partnerships throughout the entire experience. I could give many, many examples of how a higher-level of security was achieved because of such relationships.

If you look at our preparations, I think you would find that we focused on both preventive and response strategies. We found many good preventive and response models from the infrastructure community which provided guidance for some of our security preparations. One event that comes to mind is our Olympic workshop that we had, hosted by FEMA at Mt. Weather. The FBI and other federal law enforcement agencies also played a leadership role regarding our preparations, especially in the areas of intelligence, tactical response and explosive ordinance disposal. In fact, many experts consider intelligence to be the first line of defense against terrorism, and it certainly supported many of our decisions regarding the allocation of our security resources.

The FBI, the ATF and others contributed enormous resources and expertise regarding explosive ordinance disposal. They provided numerous training opportunities at no cost to local agencies to help us all get ready. The FBI also contributed enormous expertise and resources to enhance our tactical response capability.

Now, I believe that our diverse public safety community achieved an efficient level of coordination, in large part, through efficient information management.

Our Olympic challenge was how to manage lots of information continually generated by numerous sources over a long period of time.

Through a cooperative intergovernmental initiative between the Office of National Drug Control Policy, the Department of Energy and the Atlanta Police Department, we developed a state of the art map-based command and control system which demonstrated the usefulness and effectiveness of real-time access to graphically displayed information. It improved our ability to schedule and manage our limited resources dramatically. To digress a moment, we scheduled all of our people, all of our Atlanta police officers for the entire event, in under ten minutes. It provided critical tactical support for routine as well as escalated situations. And perhaps most important, it dramatically increased our ability to absorb lots of information quickly.

Looking back, I would say that preventive and response strategies were indeed challenged by the need to effectively establish and manage the flow of information among security providers, especially in preventive and response situations that rely on interagency collaboration. Olympic security operations, which involved the collaborative commitment of over forty federal, state and local agencies, in hindsight provided dramatic proof that this is true.

In fact, our Olympic security preparations were not considered complete until a clear picture could be drawn illustrating the information flow within the entire Olympic security apparatus. I think the success of our Olympic security operations, therefore, can in large part be explained by how strongly information management was emphasized during our transition and training phases.

In my opinion, the 1996 Summer Olympic Games was a showcase of interagency coordination and cooperation between and among the federal, state and local public safety agencies, and it was a showcase for public-private partnerships.

I am encouraged, having read what I have about this Committee, with its emphasis on the need for collaborative efforts and partnerships.

Clearly, the challenge addressed by this Committee is of Olympic proportions. And if the 1996 Olympic experience can serve as a point of reference for this Committee, perhaps it is by lending credence to its stated goals and its approach to this critical issue of infrastructure protection.

Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Major Gordon.

COMMISSIONER GREENE:

Major Gordon, I would just add one point. Where you mentioned that what you did, you were very proud of as a showcase, I would take that even further and say that I think the preparations done by Atlanta and by many of the people in the audience here who worked with you in co-operation with that probably have set the best preparation example in the history of the world in what a city can do. And it points to a lot of lessons learned that we hope to draw upon here at the Commission.

MAJOR GORDON:

Thank you very much.

(Applause.)

THE MODERATOR:

Our next presenter will be Joe Bankoff with King & Spalding.

MR. JOSEPH R. BANKOFF:

Chairman Marsh, Mayor Campbell, distinguished members of the Commission, thank you for holding this hearing in Atlanta and for inviting me to appear and offer an opportunity express my views on a couple of points. I think the mission and the opportunity of this Commission are as critical as any of the infrastructure which it seeks to protect.

I approach the assessment of the vulnerabilities of our national infrastructure resources as a lawyer who advises both private concerns and public policy makers. I'm a partner in a national law firm that has its largest office here in Atlanta. I also chair a group of lawyers within that firm that deal and specialize in intellectual property and technology matters. I have the privilege of serving as a member of the Executive Committee of the Federal Communications Bar Association and I co-chair the Atlanta chapter of that organization. And I have served as chair of the Telecommunications Policy Group of the Georgia Center for Advanced Telecommunications Technology, this GCATT entity that you have heard so much about this morning. And it was in that capacity that I had the opportunity to assist in drafting the Georgia legislation that in 1995 changed the telecommunications regulatory environment in this state, opened up competition at the local switch, and created a new and important role for our Public Service Commission here. Most recently, I have had an opportunity to serve as television and technology counsel for the Atlanta Committee for the Olympic Games (ACOG). Thus my experience basically focuses on communications infrastructures and the process by which communications policy is made.

I want to offer a couple of comments for you this morning. However, I want to make it clear that I am really only speaking for myself and not for any of the organizations that I have had association with.

I believe that the process by which we establish public policy regarding our technology infrastructure is the single most critical aspect of protecting that infrastructure. Let me repeat that for one moment. The process by which we establish public policy is the single most critical aspect of protecting our national infrastructure resources. Some time ago, Walt Kelly commenting about another corner of Georgia, the Okefenokee Swamp, in Pogo said, “We have met the enemy, and it is us.” Because I believe human nature and our inherent distrust of government have fragmented naturally the responsibility for parts of our technology infrastructure among federal, state, local governments, various industries, educational institutions, international bodies and private companies. Frequently, the limitations on the use, development and protection of our technical resources is not a technology barrier. It is not a technology barrier. It is frequently a political and legal issue driven by economic and political interests and fueled by a healthy distrust and concern about change and uncertainty about the impact of new technologies.

Now, this is neither good nor bad. It is just the way things are. This is human nature. But it needs to be taken into account when thinking rationally about what do we do to protect our resources. A rational approach to planning obviously requires a collaborative approach and it involves all of the players. That’s not to say that they’re going to become any less competitive or that the political interests are going to go away. It means that we need to find and live a new paradigm in which we can have simultaneous competition and collaboration.

I want in that regard to mention an example of this that has been attempted in Georgia and that I think is proving successful. It is in fact the Georgia Center for Advanced Telecommunications Technology, GCATT. This is a division of the Georgia Research Alliance, a partnership of academia, industry and government that seeks economic development as its primary motivation and the improvement of the quality of life in Georgia. These are people looking for jobs in Georgia, trying to grow the pie. This is one of the focuses. But GCATT’s overall mission is to provide university-based research which helps shape and support the emergence of the advanced telecommunications technologies and to supplement university research and basically to promote opportunities for jobs and growth and expansion.

But it is the cross section that’s interesting. It is a senior cross section of government, including the Governor’s Office, the Public Service Commission, the State Superintendent of Schools, the Board of Regents, the Department of Administrative Services, and the Georgia Department of Education. It includes cross sections of senior members of our industry here in Georgia: AT&T, BellSouth, Cox, Equifax, IBM, Turner Broadcasting, the Georgia Telephone Association, the association of the local telephone companies. It also represents our higher educational institutions: Georgia Tech, Clark Atlanta, the Advanced Technology Development Center, and the Medical College of Georgia.

The aspects of bringing all three pieces, not just public/private, not just the business and academic, but government, business and academic together creates this opportunity. And in 1993, in assessing what was then a legislative impasse on telecommunications, GCATT created a Public Policy Working Group. The group was a cross section selected by the GCATT Board, and it included six professors at five universities, representatives of the local telephone companies, the cable companies, the long-distance carriers, the service providers. It included large corporate users. It spent a year studying the economic impact of this issue. It looked to the future of what telecommunications could be. It brought about a focus on a vision of where things could go, and it stacked up Georgia with the other states and said, "How are we doing?" And out of that process grew the realization, a political realization, that legislative change was needed, and, most important, possible. Through public and private meetings held in discussing these issues frequently with the active participation of the legislative delegation, it became clear that a consensus could emerge that a competitive balanced change in the regulatory environment was possible and needed. And all of this preceded the federal bill by a year.

I don't want to focus on the substance of what came out. I want to draw your attention to the process, because it was in the formation of the political consensus that permission for change arose. Awareness of the issue, a need to change, and then a participation in the sense that we could have a hand on the balancing, so it was okay. The other thing that emerged was a realization that the status quo wasn't anybody's friend, and, therefore, hanging on wasn't to anybody's particular advantage. So permission for change exists. In my judgment, the effort that had gone on before with a series of bilateral negotiations or unilateral lobbying had simply resulted in a stalemate. And if you could put together, as they did, an opportunity to work in a dynamic that gave permission for change, then you had an opportunity to make change.

I think this Commission, frankly, represents a similar cross section and is embarked on a related kind of process. I think that your process will be as much a product of anything you do as any document you present. But I want to think that we should encourage other successful types of this kind of collaboration.

The second point is a comment, a substantive comment really on a particular piece of the public policy debate in the protection of our national interests. And I realize that political realities may limit what the Commission may say in a public manner on the issue of this country's fascination with the policy of encryption. But I do think it is important to note that our current policy is not achieving protection of our national resources, and it is disabling our commerce in the sale of sophisticated programming and in providing state of the art protection to large-scale commerce in the worldwide marketplace in technology.

We do not need to kid ourselves that those whom we might wish not to have or to be able to use sophisticated encryption to carry out activities that are either unlawful or not in our national interest do not have access to other sources of that technology. There seems to be little justification for the firmly held belief in the United States that if we disable our own technology, we can keep it from others. But technology does not operate in an environment in which it is possible to easily limit within national geographic borders. Thus, we are giving a competitive advantage to suppliers outside the United States. We are encouraging the export of the development of this technology. And we are hobbling the growth of a robust commercial network that will need state-of-the-art security to assure economic integrity as well as privacy.

Now, we do need to recognize that potential threats to the security of our national communications structures are very real. Although they do not wish to admit to computer vulnerabilities, both private and governmental systems have been and are continuously attacked, for amusement and for profit. We need to make a policy that is built upon a realistic assessment of what the technology can do, and then to make that technology reasonably available to protect us. A new balance needs to be found between the right to use technology to protect our systems and ourselves and the government’s desire to protect its ability to use current technology for law enforcement and national security purposes. We are not doing a great job at either at the moment.

I want to thank you for allowing me the opportunity to express my views. I wish this Commission much success in raising the public’s political and practical awareness of this important issue. Thank you.

(Applause.)

COMMISSIONER GREENE:

If you have any documentation that may lay out some of that process, we would be welcome to receive that at the Commission as a reference thing to review that may help us. Your points are very much on the mark, and it would be good to have something more that might supplement it.

MR. BANKOFF:

Thank you very much. I have asked the reporter to do this at the suggestion of the Commissioners I met with yesterday.

THE MODERATOR:

Our next presenter will be Mr. Wayne Dahlke with Georgia Power Company.

MR. WAYNE DAHLKE:

Good morning. On behalf of Georgia Power Company, I am Wayne Dahlke, Senior Vice President of Power Delivery at Georgia Power Company. Georgia Power is a generating and distributing subsidiary of the Southern Company, the largest generator of electricity in the United States. We supply about 5 percent of the nation's energy.

The Southern Company is also the parent company of nine other operating companies. Other power generating entities include Alabama Power, Mississippi Power, Gulf Power, Savannah Electric and Southern Nuclear. The remaining subsidiaries provide a broad range of services, including telecommunications, engineering consulting, and international power supply.

Georgia Power Company is an investor-owned, tax-paying utility, serving about 1.75 million customers. We are responsible for power generation, transmission and distribution, marketing, customer operations, and customer service. We have a presence in all but six of the 159 counties in Georgia. Our net income for 1996 was $580 million. Georgia Power Company employs 8,439 people. Last year, we generated over 100 million, 600 thousand megawatt hours of electricity at our power plants, some of which are co-owned by Oglethorpe Power, Municipal Electric Authority of Georgia, Gulf Power, Jacksonville Electric Authority, Florida Power and Light Company, and the City of Dalton.

Georgia Power Company is the system operator for the state's integrated transmission system and responsible for scheduling and dispatching electricity throughout the state.

As a provider of electricity, Georgia Power Company is obviously highly dependent upon its infrastructure. Of critical importance to us are our 33 generating plants and more than 16,000 miles of transmission lines across the state. They are the source of something equally important as electricity: our company's reputation for reliable service.

Infrastructure protection is an integral part of our operations. While our plants and other site-specific facilities can be physically monitored around the clock by guard services and surveillance cameras, it is impossible to give our wide transmission network that kind of protection. It's not even reasonable to expect that we would do so. So the transmission network represents our greatest exposure and risk to sabotage. The practical answer to mitigating this risk lies in the transmission network design. And like other utilities nationwide, we have adopted design redundancies that make security inherent in the design of our systems.

As a part of the Southern Company, Georgia Power Company uses a transmission grid that was designed with what we call “first contingency redundancy.” Operating the system on a first contingency basis means that the power grid is always operated and transmission elements are loaded so that the first transmission element, if it’s lost, will not cause a failure because of overloads on other parts of the system. Our relays detect within milliseconds failure of equipment and coordinate the removal of service equipment to minimize system damage and to switch the power around to where we can serve the load from another direction. Relay protection also ensures that power systems can be restored in the fastest manner possible after an event.

As with any transmission provider, there are portions of the grid which are especially critical during certain times. A good working knowledge of generation patterns, load durations and maintenance scheduling goes into operating it successfully day to day. Data including line ratings, impedance and transmission configurations are made available between utilities in the Southeast. This is highly sensitive information that without proper attention could get into the wrong hands.

We analyze these threats and vulnerabilities on an ongoing basis together and take these factors into account as we develop and upgrade our transmission components and systems. Operating facilities are kept locked at all times, and access is controlled and monitored by closed-circuit TV, computer systems or by guards. All facilities have card-key access with strict controls and audits in place to make sure that access to cards is only available to those employees who need access. Background checks are conducted on all personnel hired for jobs in critical computing and operating areas.

On a generating basis, Georgia Power, again as part of the Southern Company, operates under the North American Electric Reliability Council (NERC) policies and the policies of SERC, which is the Southeastern Electric Reliability Council. These alliances assure that there are enough generation reserves on the line to meet the load in the event that a single contingency removes a large generating unit or transmission line from service. Under agreements with these two councils, Georgia Power Company is also a part of an extensive communications network providing reciprocal advisements to all utilities should there ever be any threat to the power system.

As a part of the Southern Company, we rely extensively on communication and computer systems that were developed internally, and they also have a high degree of redundancy. The computer systems are protected from cyber threats through what we call “firewalls,” which do not allow access from personnel outside the company. Because the systems are designed by our people, they are unique and familiar only to the limited number of people who have access privileges. Our systems’ uniqueness adds a great deal of security for us. All systems are password-protected, and audits to check the effectiveness of security measures are conducted periodically. We have not experienced any cyber attacks on our power system.

The Olympic Games last summer, for which Georgia Power Company was the official power source, was a large, extraordinary event that provided an opportunity for us to assess several of our security measures. Studies for protection of critical infrastructure at the Olympic Games were conducted in coordination with the FBI and other governmental agencies. While complying with the requirements of these agencies, Georgia Power Company exceeded those expectations. A well-designed, carefully executed security plan, combined with power system maintenance, monitoring and construction measures were critical in meeting our number one goal: Keep the lights on.

The Olympics presented one situation that, while it did not directly affect our generation or transmission facilities, nonetheless did offer a chance for us to demonstrate in real terms the threat of terrorism and the value of operational plans and emergency training. Here I’m talking about the night of the bombing at Centennial Olympic Park. The response of Georgia Power’s Olympic Games Command and Control Center represented a real-time success of our long-term planning. Within minutes of the bombing, the Command Center staff had methodically contacted the on-site crew and used our SCADA system to electronically check our data to eliminate Georgia Power Company’s equipment as a source of the explosion. Shortly after the bomb exploded, Atlanta-based CNN reported that the explosion might have been caused by an electrical transformer. And my phone started ringing about 1:30 in the morning. The information from our internal check helped us quickly dispel that erroneous report.

We of course must protect our infrastructure not only from these kind of terrorist threats, but also from nature. Storms are an ever-present concern, and we have had much experience dealing with them lately.

Most recently, Hurricane Opal struck the state in October 1995, downing some 1200 poles and causing more than 400,000 power outages to our customers. More than 2500 Georgia Power Company crew members, contractors and workers from neighboring states with agreements worked up to 18 hours a day to restore power. Seventy-five percent of our customers were restored within 48 hours. Complete restoration took about five and a half days to get everybody back on.

We followed Georgia Power Company's long-established storm emergency restoration procedures, which were very similar to the procedures we established for the Olympics, which include several sequential steps. Our people make an initial evaluation by "riding the circuits" in areas where damage has occurred to get a handle on how many poles and lines are down and how many trees and tree limbs have fallen on lines and whether the roads are accessible or not.

As all this goes on, information flows in from across the state to our Storm Center to pinpoint the areas that have been hit the hardest. The center dispatches the tree and line crews to the regions that have the greatest need. Larger distribution crews move in to put the main lines back up. Once the main lines are back up and power is restored to critical customers such as hospitals, fire and police departments and emergency services, the focus then shifts to residential and commercial customers. Our attention then turns to restoring low-voltage service to individual customers in remote locations.

A similar approach was employed four years ago when we experienced what has been called "the storm of the century" and what most people agree was the worst snow and wind storm in Georgia Power Company's modern history.

The snowstorm, if you can believe it in Atlanta, hit us in March of 1993, knocking out electricity to over a half million customers of Georgia Power Company, the highest outage we've ever experienced. Winds of more than 70 miles an hour toppled steel transmission towers and lines. All told, an estimated 87 transmission lines were affected in some way by the storm, which is the critical backbone of our supply system.

During this storm, more than 6,000 employees and contractors were involved in storm tracking, coordination of restoration crews and communication. The storm hit on Saturday. By Monday, outages were reduced by two-thirds. Total restoration took seven days.

Our company also provides help whenever needed to neighboring utilities to rebuild their systems after natural disasters. This occurs under the Edison Electric Institute's Mutual Assistance Agreement which we are a part of.

Another type of infrastructure incident that is receiving attention is the disturbance that occurred last summer following the collapse of the southern portion of the bulk power transmission system in the Pacific Northwest and the resulting transmission grid breakup.

THE MODERATOR:

Excuse me, Mr. Dahlke. You've hit ten minutes, if you could wrap up. Thank you.

MR. DAHLKE:

Okay. I have tried to give you a descriptive account of the extensive infrastructure protection already in place in Georgia and throughout the Southeast. Security from threats and the ability to withstand and quickly recover from incidents are inherent in our system design and maintenance. We are the folks who have the most accurate data about the infrastructure, and that makes us immanently qualified to administer it on a company by company basis, as a private industry and enterprise. And we would encourage the Commission's continued support of that. We recognize this as our responsibility and take it very seriously. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you.

COMMISSIONER GREENE:

Mr. Dahlke, just one quick question. With a lot of the energy companies, as you know, there's the Federal Energy Regulatory Commission filings that are available on essentially open source through 1-800 modem dial-up and downloading. Do you consider that to be a potential risk or something that terrorists could take advantage of to identify key links in your systems?

MR. DAHLKE:

Well, the way those systems work, they are just access to data. They don't have any ability to operate any of the substations or critical infrastructure. It's much like the Internet; you have access to the data. It's a matter of public posting for making sure prices are reasonable. But because of the firewall, it doesn't allow them to get into our operating system whatsoever.

THE MODERATOR:

Thank you very much. Our next speaker will be Daniel Robbins with Bank Corporation of Georgia. And if anyone in the audience would like to speak who hasn't filled out a yellow card, please do so now at the table behind you. Thank you.

MR. DANIEL ROBBINS:

Good morning. I have submitted a written statement to the Commission, so I will keep my comments informal and brief. With Bank Corporation of Georgia, we serve a valued customer, and we serve a customer that has a "right now" customer service mentality. With the closed networks that we have had traditionally, this "right now" service mentality has been able to be achieved through cost effective data processing. But today with open networks and online transactions increasing through the Federal Reserve and also through source documents, we find ourselves having to take more time to serve our customer.

In critical infrastructure protection, we are looking at time and being swift in the process to be able to achieve our customer service objectives. In looking at the customer, it is not acceptable in our marketplace to be able to have a "wait-until-we-can-get-the-information" attitude. We need to be able to swiftly and authoritatively validate customer transactions. Cyber threats may not be realized only at the stroke of a key on a keyboard, but also through using technology to create fraudulent source documents. A check is now so easily printed just on a home computer that we need to use technology in protecting our customers' financial status, in protecting our interest as an organization, but then also looking at security, meaning that it must be validated. And at all levels, as far as the network is concerned, validation is the key-but-swift critical aspect of our infrastructure.

Risk management associates with what a customer intends to do with a transaction or a fraudulent transaction, so we use technology within our organization to help us identify those weak aspects of the customer transaction.

Multilevel verification tools are used because it has been determined that over 80 percent of any type of data access that could be fraudulent is perpetrated from within. And within the banking industry, we continue to try and validate these aspects to make sure that not only externally, but internally, that we are fully protected.

In addition, our market definition has now expanded. We used to be a building on the corner. But now with the Internet as an example, our geography has totally expanded to where our policy, we need to be prepared to be able to open accounts from customers that may reside in

Europe, in the Pacific Rim, or any other part of the world, based upon Internet access. So with that, we look at also the validation of someone that — it used to be we could get face to face and open a customer relationship. Now we are face to face with just data, and the need to verify becomes paramount.

Our recommendation to the Commission is a certification process very much like the ISO or International Standards Organization series in the manufacturing realm. We most certainly at the federal regulatory level have certain standards, criteria — our FDIC insurance is evidence of that — but look at the establishment of a certification process that our organization would be a part of, that we would participate in the community of technology users so that we then would be able to also have an assurance that those that we are exchanging data with have met a level of assurance that they indeed take safe data access measures. But then also with the emerging technologies, we know of the "smart card" technology, which is going to so impact our industry — that's a very important aspect to us because of the amount of data that a customer will be able to carry around. And we hear predominately of medical history, but also financial related data will be able to be carried along. So we need to look at how that technology will be able to impact the critical infrastructure. But then also the software distribution industry is something that is emerging where software would be distributed via the Internet. A validation needs to exist through that software distribution maybe in conjunction with one of the various other technologies. We don't see it as a single solution, but in combining firewalls that we've just heard about, encryption that we've also heard about, the smart card technology. But then there's also another emergence that many folks may hear of as far as satellite technology, where if you're lost in a car, you can use satellite technology to chart your path. But in the financial industry, we could look at that to geographically limit network access, based upon a location. So, a combination of those.

We look at using multilevel tools in verification, but then also obviously the financial strength of our industry would need to be brought to bear to help in the investment of hardware and software developers so that incentives would be passed along through your policy to assist these folks. We've heard of unique encryption. We've heard of unique hardware and software solutions. But then we as a corporate citizen would then also feel compelled to participate with that.

I appreciate the opportunity to speak this morning. Thank you.

(Applause.)

THE MODERATOR:

Thank you, Mr. Robbins. Our next presenter will be Michael Hutchins from Atlanta Gas Light Company.

MR. MICHAEL D. HUTCHINS:

Good morning. And welcome to Atlanta, by the way. I represent Atlanta Gas Light Company. We're the largest natural gas distribution company in the Southeast and the eighth largest in the United States, serving about 1.4 million customers in the State of Georgia. We have something on the order of 42,000 miles of underground piping facilities. We believe that our infrastructure is not at as high a risk as some utilities and other infrastructures that you may be concerned with because of that. Being underground, it's less vulnerable, it's harder to get to, and it's harder to attack.

Although there are risks and there are places and opportunities within our system where risk and attacks may occur, there is no one spot that is critical to serving the City of Atlanta. It would be many spots, if it were attacked, to shut down the entire City of Atlanta. So from a natural gas perspective, we believe that our infrastructure is at lower risk than many others that you may be concerned with.

We are regulated by the Department of Transportation's Office of Pipeline Safety, which guides us in the construction, the maintenance, and the design of our facilities, as well as specifying emergency plans. We have a number of contingencies and emergency plans in place to deal with day-to-day cuts in facilities as well as natural disasters, such as hurricanes or that sort of thing. And also the regulations touch on terrorist attacks as well. We have the typical security as far as locks and access and those kinds of things in the facilities that might be targeted.

We worked very closely with the Olympic opportunity in Atlanta. We provided a good bit of information. And as some people have indicated, sometimes industry feels that that information is critical and are reluctant to provide it. We felt that way as well, but we did provide a lot of information as to some of our key points. We were fortunate that none of the infrastructure, the underground or the utility infrastructure, was attacked during the Olympics. We believe that there are certainly many more newsworthy areas that typically are attacked. It's not the utility infrastructure.

If a site of the natural gas system were to be attacked, it certainly would cause loss of service to possibly critical areas, such as hospitals, restaurants and that sort of thing. But because that delivery system is underground primarily, and multi-pointed, it is backed up by loops and different approaches so that we feel like we can restore that service very quickly and promptly, and reduce the impact of such an attack, consequently reducing the appearance from an attacker that, “That’s something we want to go after.”

Because we feel like we are at less risk, we would encourage you to look at the risk aspect of whatever rules or regulations or legislation or however this Commission chooses to promulgate direction in dealing with attacks, and work towards solving the bigger problems first and the minor problems later. We certainly believe that we’re in the “minor problem” category. I appreciate your attention and the opportunity to address you. Thank you.

(Applause.)

THE MODERATOR:

Thank you very much, Mr. Hutchins. Next, John Styron of the DeKalb County Department of Emergency Services.

MR. JOHN F. STYRON:

Thank you, ladies and gentlemen. Welcome to Atlanta. I want to talk to you a little bit about the public safety role in infrastructure protection. We actually have two concerns in that area. One is should there be an attack on the infrastructure, public safety has to be ready to respond to it, and we also have a responsibility to protect it. Secondly, we are also vulnerable to attack as an infrastructure agency. We are not immune in any way from attack, and we have to take that into consideration as well.

I work with the Emergency Medical Services in DeKalb County. The Emergency Medical Services is one of the public safety agencies that provides an essential service to the citizens of the community. The police department and the fire department have a couple hundred years of experience and tradition, but the Emergency Medical Services in the United States is only about thirty years old. And so it’s still very much in development.

The Emergency Medical Services has several types of providers. Unlike the police and fire department which are strictly governmental agencies that provide service, in the Emergency Medical Services there are public hospital-based services; there are public fire department-based services; there are public third service agencies of which my agency is; there are private providers who provide this service to the public; and then there are public utility models which provide this service to the public.

The public safety response to an incident is on two levels. One, are we adequately prepared to respond to it? And to that end, the Emergency Medical Services is very much in a state of flux. It’s still in development because of the fact that it’s only thirty years old. And so some of the considerations that have to be considered when you’re assessing the community’s ability to respond to emergency widespread or local emergency situations is are there adequate numbers of units available to respond to an incident should it occur? Are they properly equipped? Is there a continuing education program within the organization that maintains peak efficiency? Is there adequate medical community participation? That may or may not be the case, unfortunately. And are there adequate community standards for this essential service?

Unfortunately, because of the fact that Emergency Medical Services is so new, most people think of the Emergency Medical Services as the ambulance service, and it is not that. It is the community’s response to sudden, serious injury and illness in the community.

Unfortunately, most elected officials and the public in general are woefully ignorant of what the standards of this service should be. And, therefore, in many communities, there are not adequate standards in place for it.

Secondly, we have to consider the defensive strategies of the public safety agencies. Assuming that they are adequate and that they are in place and are ready to respond in an appropriate manner, the most logical defense of public safety agency assets is the same thing that the military does. One, to widely disperse those assets so that they are not vulnerable to an individual attack. By the nature of police, fire and EMS services, they are normally widely dispersed. And, therefore, no one single attack, unless it was something like a nuclear attack, would disable those assets. Secondly, redundancy. Redundancy has to be in place at all levels and systems.

The most useful tool that we in public safety have is this right here (indicating). It’s a communication tool. It’s a radio. And this particular radio is an 800 MHz radio. And it’s a computer. There are no crystals in it. The frequencies are programmed. And all that has to happen is for it to be plugged up to a computer to reprogram it. Anyone who gets their hands on one of these radios and who knows how to program it can program it to talk on any 800 MHz band frequency just about, if they know what they’re doing. So there is a vulnerability there.

I’m going to read to you a little bit from a document that I have submitted to you. But basically, widespread disaster and chaos that would overwhelm local capabilities are generally handled by activation of FEMA, the National Disaster Medical System, and the DMAT teams, which are the Disaster Medical Assistance Teams. So as far as widespread disaster goes, I think we’re probably pretty well prepared for that. The primary threat exists to the command and control of the public safety systems. In order for emergency service providers to respond to emergencies, the first thing that has to happen is the public or someone has to recognize that an emergency exists. A request for help must be relayed to the communications center via telephone land line, cellular phone, amateur radio or CB radio, or by direct observation of a public safety officer, a police, fire or EMS officer. Once the event occurs and comes into the communications center, it’s entered into a CAD system, a computer-aided dispatch system. The computer-aided dispatch system then assigns units and recommends units to mitigate the situation. Emergency units are dispatched via radio frequency in either the VHF, UHF, 800 MHz or 900 MHz band widths. Event tracking and information management is handled through the communications center. Anything that would interfere with this process could result in a failure of the system to respond to emergencies. Threats might include incapacitation of the public telephone system or the public safety communications system itself. Such incapacitation might be physical destruction of buildings or equipment, or technological incapacitation due to computer viruses, hackers, software failures, etc., or incapacitation of the people working in the communications center due to chemical or biological gas attacks. It could even be something as simple as “sick building syndrome” that suddenly incapacitates everyone in the center. Basically, anything that would interfere with relaying emergency service requests and the transmission of information between public safety officers would result in a failure of the public safety emergency response system.

The solutions to mitigating this risk are to develop, as I said before, redundancies in the communications systems. The public phone service provider needs to have duplicate equipment capable of providing communications service in multiple physical locations. Are there any bottlenecks in the system that would make them vulnerable to attack? As it turns out, I spoke to someone with BellSouth yesterday, and there is one switch for the 911 system. If that one switch is taken out, the 911 calls go down. They are planning redundancy to correct that problem. They have fortunately recognized it in BellSouth. And they are in the process of installing, and hope to have it up by July, a second system. But that points to one of the examples of how the system is vulnerable and how it would disable the entire system.

One of the things that we do right now when we have a hazardous device incident is we establish an 800 foot no-transmission perimeter. It was formerly 100 feet, and it has just recently been moved back to 800 feet because of secondary devices that have been placed in the Atlanta area. If you think about that, we are denied the use of our most essential piece of equipment simply because of the fact that we cannot transmit, we cannot use cellular, we cannot use data communications within that zone. So we have to use runners or we have to lay physical hard line in order to be able to communicate at these incidents.

Since monitoring of public airwaves is widespread and common, people have scanners, etc., they are able to monitor our RF traffic. They are able to tell what we are doing, and they are able to use it for illicit purposes. It is also possible for disruption of essential emergency communications through jamming and transmission of bogus messages. We have, in fact, had people get on our frequency before and transmit bogus messages. And that is disruptive to operations.

Technology threats post numerous possible problems. In some scenarios, a hacker or computer virus might cause complete failure of our CAD system. Another very serious possibility is that undetectable disruptions may occur, such as creating bogus emergency calls to unnecessarily tie up urgently needed emergency units. Unintentional threats exist, also. A year 2000 bug could disable us just as easily as a hacker. As an example of a year 2000 bug and how it might affect us, in one community, prisoners were released early because the year 2000 bug in their software calculated that they had served their sentence. So it can occur, and has occurred. For private provider EMS services, a year 2000 bug could cause them to be denied reimbursement from insurance, Medicare, and other revenue sources, thus causing them to default on payroll. And it might interrupt their service.

I would say that there’s probably two major obstacles that you’re going to have to consider. One is called local community autonomy, and in the private sector, it’s known as proprietary information. An atmosphere needs to be created in which that is overcome and folks do work together to solve these problems.

Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Chief Styron. Our next presenter will be Sheila Pierce, Deputy County Manager for Fulton County.

MS. SHEILA PIERCE:

Good afternoon. Fulton County Government has in it the City of Atlanta, as well as nine other cities, making Fulton County the largest county in the State of Georgia. I have with me today Mr. Jim Cook, who is the Assistant Director of the Emergency Management Agency, which is jointly funded by the City of Atlanta and Fulton County. That agency is housed in Fulton County and jointly funded by both governments.

My background is I have been with Fulton County; prior to that, the Federal Environmental Protection Agency. And my education is in the area of public administration. So I have selected to speak today on the topic of continuity of government and infrastructure protection.

As you may know, tomorrow is the second anniversary of the bombing of the Federal Building in Oklahoma City. Ever since that time, governments of all sizes have been challenged to think seriously about how to ensure that their operations will continue without disruption even in the event of crises caused by terroristic or other criminal acts.

Protecting tangible assets, such as utilities and transportation networks, is what readily comes to mind when this subject arises, but if the people and mechanisms that see to the daily administrative conduct of government are harmed or eliminated, then those tangible infrastructures may be seriously compromised as well. Large urban local governments, such as Fulton County's, are particularly at risk because they sometimes are within a larger complex of government operational structures that include state and federal agencies. In fact, we're a case in point because we're roughly halfway along Government Walk Corridor in Atlanta between the State Capitol and the attendant state office buildings, and both the Richard B. Russell Building, and the new Federal Office Tower. The federal and state governments do not have a division between the policy makers and those having the authority to implement policy. But that is not the case here in Fulton County and with many other counties in Georgia. In Fulton, the Commissioners are elected to set policy. The County Manager's Office is given the authority to implement that policy and supervise the daily administration of government through a number of departments, their directors and staff. As such, a threat to the safety and continuity of governments like ours is more likely to be directed at those people responsible for carrying out policy directives initially proposed and approved by our Commissioners.

The local jurisdictions, even large and seemingly sophisticated ones, don't tend to have the kind of clearly delineated chains of command that the United States Government has to ensure the power to act continues unabated in the face of a catastrophe. If the President is incapacitated in an attack, for instance, the Vice President will take over, if able. And then the line of succession runs on down through the Speaker of the House, the President pro tempore of the Senate, and so forth, through the various cabinet officers. In Fulton County, the Commission Chairman is the political, not the administrative, head of government. The County Manager is lead administrator, and I, Deputy, am second in command. I would assume the Manager's place in the event a crisis indisposed him.

But a large scale action intended to immobilize a local government like ours, if it enjoyed any success, might render large numbers of decision-making officials inoperative. What is clear is that localities, no less than Uncle Sam, need to have unambiguous lines of authority spelling out who takes charge in certain circumstances. In fact, state law requires such a mechanism of local governments, but the requirement is loosely enforced, and most localities do not observe it.

Fulton County is one of the minority of governments, however, that do observe it. The Atlanta-Fulton County Emergency Management Agency requires each of our county departments to prepare continuity-of-government-line-succession forms listing the director and two designated successors in order of succession who would assume command of operations in case a crisis removed the director from control. The forms include beeper and office telephone numbers. Those forms also require the departments to list the names of emergency coordinators, their beeper numbers, if applicable, along with telephone numbers. The Emergency Management Agency's emergency operations plan also includes a tab that spells out the importance of a succession-of-authority plan. And here are some of its pertinent statements. "Continuity of government and direction of emergency functions are essential during emergency operations. The following lines of succession are specified to ensure availability of a service coordinator or head of government. Permanent replacements shall be made as required or authorized by law. Decision-making authority for each service or organization is listed in decreasing order. The pre-delegated authorities will assume command when the primary decision-maker is deceased, incapacitated, or absent from the county at the time of the emergency." The tab also goes on to list officials in descending order who would be responsible for the emergency functions of direction and control within Fulton County and each of its ten municipalities. For instance, at the county, the Chairman would be succeeded by the Vice Chairman, and then a member of the Board of Commissioners. In each of the cities, the Mayor would be succeeded by the Mayor pro tem, and then a member of the City Council. Our tab also specifies three Fulton County officials who would be responsible, again in descending order, for the following emergency functions within the county: communications and warning, emergency public information, and law enforcement, along with fire, evacuation, transportation, and search-and-rescue services.

Continuity of government also has to do with the processing of vital transactions, such as paychecks and the maintenance of invaluable records, such as property tax payments and other tax-related matters. I would like to tell you that Fulton County has a contingency system in place to take care of this in the event of a disaster, but that isn't the case. Several times a week our data processing network allows us to mirror what is on file at the time. This is a snapshot that is stored on tape of the data present and accumulated in the system over a period of days. And that material can be kept only until the next mirroring interval. So if you wanted something from six months earlier that had been expunged at some point, you can't retrieve it.

What we really need for continuity is an arrangement where all your information can be retrieved instantaneously at a remote location on somebody else's mainframe if a catastrophe knocked out your own records. There is an industry providing this service. It's expensive, but you can get it. Many people in institutions find it hard to spend precious time and money on a worst-case scenario that may never or probably won't happen. But it only takes a single once-in-a-lifetime emergency to realize how important that kind of investment can be.

I hope my observations on this subject have given you some helpful information that might contribute to the development of a critical infrastructure protection plan. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you, Ms. Pierce. Our next speaker is Dr. Paul Wiesner, DeKalb County Board of Health.

PAUL WIESNER, M.D., Ph.D.:

Good morning. I thank the Commissioners for spending this time listening so carefully to so many folks. I am going to be submitting prepared remarks, but I wanted to at least heighten the awareness of the role of public health agencies in this issue of critical infrastructure protection. We did have an opportunity yesterday to talk with Commissioner Moorcones and Commissioner

Culnan, and we very much appreciated their spending the time over at the Emory University School of Public Health.

The main points that I want to make is that among the working definitions of the critical infrastructure working definitions — there are actually eight or nine of these listed in your web page — this probably falls in the category of continuity of government services. But local public health is actually — or public health is mentioned once in the discussion of this issue.

I want to contrast what "public health" is compared to what "medical emergency response" is. Medical emergency response tends to respond to a specific event, caring for specific individuals in a critical need. Public health focuses on the whole community of people, the whole population of people. And there are some very essential public health tools that are used for preserving people's health or preventing health problems in populations.

The science of epidemiology that actually measures the trends and presence of threats to people's health is the core of public health. And the other aspect of public health that is particularly important is the relationship that it has to the communities that they serve.

At the DeKalb County Board of Health — DeKalb County is the second largest county in the State of Georgia — I view my "patient" in that sense as the 600,000 people who live in that community. And if you examine the working definition categories of the critical infrastructure outline that you have, failure or disruption or problems in any one of those infrastructures inevitably has the potential for creating significant human health-related problems. Public health's role in emergency response is usually before the emergency occurs in terms of preparing a community, and actually after the immediate response in terms of the very early recovery and remedial phases. And it's not at all unusual that the public health's role must be extended for quite a long period of time after the particular incident.

Everyone is familiar probably in this room with public health's response to the Bhopal incident, and that is still going on in terms of the remedial and follow-up of that episode. Everyone probably in this room is familiar with the Centers for Disease Control's response to establishing surveillance activities throughout large events that affect large numbers of people from Somalia famines to major floods in different parts of the world. I spent twenty years at the Centers for Disease Control. And for the most recent past eight years, I've been the director of a local public health agency. And I increasingly appreciate the importance of having an infrastructure for public health response at the local, state and national level.

This kind of infrastructure in preparation for responding to significant threats is critically important, and actually is itself at some threat. Not every local health department, and there are 3,000 of us — I sit on the Board of the National Association of City and County Health Officials. Not everyone has the capacity to do basic epidemiological investigations and follow-up without support of the state and without support of the Centers for Disease Control.

The main reason for my spending some time with you yesterday — I really appreciated that, Tom — and this morning is to surface the idea that public health is one of those very critical governmental infrastructures that doesn't do much in the immediate response to an emergency, but is critical in terms of building relationships with communities to prepare them to be able to respond should one of these threats occur, and it is certainly critical in establishing surveillance systems for responding and identifying and preventing problems when they do occur.

We played a very critical but quiet role in the recent Olympics. A lot of people don't know, but this is the first modern Olympics in which there was not a major food-borne outbreak associated with the Olympics because surveillance systems and protection systems were in place.

One of the major public health threats in the Olympics, a lot of attention was given to the bomb, but we had a lot of hot weather in Atlanta. And because of the surveillance systems and cooperative work with emergency rooms and measurements and counters in counting these events in an epidemiological sense, we were actually able in a cooperative effort, from the federal public health level, state, and the two local health departments that were predominately involved with this, we were able to detect when the problems of heat-related illness would possibly occur and intervene before they did occur with special distributions of water and other kinds of things that would prevent those problems. We are quite certain that without that kind of public health infrastructure, many people could potentially have died from heat-related illnesses in these episodes and in other episodes in the future.

We did have a discussion yesterday, I want to mention briefly, and this is this issue of public trust. One of the roles of public health agencies is to build community coalitions and neighborhood working groups such that that concept of social capital is supported and actually is built in our communities. I believe very strongly that there are aspects of public trust that are appropriately placed and some aspects of public trust that are inappropriately placed with where our systems and threats exist within our communities. But the concept of social capital being critically important in the ability of a community to respond to a threat as is other harder topics, like infrastructure and wiring and telecommunications and basic other economic capital, is very important. And we're going to be sending to Commissioner Culnan some of the literature on social capital as it affects this issue of public trust.

So I very much appreciate your time. Local public health directors don't get much chance to run down and talk to Presidential commissions. And I very much appreciate the opportunity.

(Applause.)

THE MODERATOR:

Thank you very much, Dr. Wiesner. Our next speaker will be Mr. Richard Simonetta, Metropolitan Atlanta Rapid Transit Authority. I wanted to read out before Mr. Simonetta presents, if I may, I wanted to read out the remaining names of the speakers. And if your name isn't called and you would like to speak, please see the staff members behind you at the sign-in table. John Copenhaver, Gen. Bill Bland, and Alan Porter. Thank you.

MR. RICHARD J. SIMONETTA:

Thank you, Mr. Chairman, members of the Commission. It's a pleasure to be with you. I also would like to thank Ms. Wong and Mr. Mitchell for the opportunity yesterday to spend some time informally talking about transportation, and specifically mass transit, and how the Commission's work applies to our efforts.

MARTA is the seventh largest transit system in the United States and transports approximately 500,000 passengers each day in Georgia's capital city. Because we are so crucial to the transportation network of metro Atlanta, we are also at greater risk of crippling the transportation system in the event that something happens to create a disaster on our system. Damage to our trains, our buses, our equipment, or our facilities, depending upon the severity, could result in the loss of life, loss of power, closure of service for days, weeks or months. And we could really bring the transportation network to a grinding halt in metro Atlanta.

I would like to talk about two possible arenas that I think could hamper the safety of public transit, specifically the threat of terrorism, and secondly, damage and destruction to equipment and facilities.

Public transit systems have unfortunately become targets for terrorism around the world. We all know of the situations that have occurred within the last couple of years in London, in France, in Japan, and in Israel. One basic problem in protecting transit systems from terrorist threats is the obvious fact that the system must be open and accessible to everyone, to the riding public, and therefore, also to the potential terrorist for terrorist activity.

While an actual terrorist event is a very real threat for all transit agencies, the fear and the anticipation of a terrorist activity can even have a greater impact on the transit system's role on a day-to-day basis. A fear of criminal activity keeps people from utilizing the transit system in their daily lives. And bomb threats and suspicious packages that are found on transit systems almost always result in delays of hours that inconvenience people and cause them to think about other alternatives.

In Atlanta, we have had some recent bombings that of course cause us to be extra careful with regard to opportunities for terrorism. And watching how the police have handled those couple of incidents certainly makes it clear to us that in the event that a real incident were to occur that involved the transit system, we would be shut down for days, if not weeks, as the investigation went under way.

Transit agencies that attempt to develop their own capabilities to deal with hazardous devices, chemical attacks, or biological agents are faced with tremendous expenditures that have nothing to do with the basic provision of transportation services. We are considering such an opportunity or such a capacity within our transit system. And our cost estimates for things like robots for dealing with bombs, and dogs to sniff out explosives, and some of the training and staffing would amount to at least a million dollars up front, and an ongoing operating expense in addition to everything else that we have to do.

I think the federal government could become involved in a positive way in assisting transit agencies in maybe as many as four areas.

First, I think methods of information exchange concerning both threats and actual events could be enhanced. This action would help prevent transit authorities from having to reinvent the wheel concerning terrorist counter-measures.

Second, enhanced training on handling terrorist threats and incidents could be provided through the Federal Law Enforcement Training Center.

Third, funding to support enhanced response and mitigation capabilities could relieve transit authorities from major expenditures that are not directly related to the transportation function as a basic function. State law currently provides for the felony prosecution of terrorists who hijack or bomb mass transit, but the Commission might also want to consider the possibility of making terrorist interference with public transportation a federal crime.

And finally, I think research and development opportunities exist to try to develop specialized tools, equipment and procedures that would relate to public transit systems.

In the written testimony that I have submitted, we have included ten examples of events that could take place on a system like MARTA that we think would need to have a very specialized, very tailored response. We have also estimated the damage, both in terms of service delays and in terms of cost estimates. But let me just talk about two of those in the short time that we have together today.

In the event of an aerial rapid transit station structure becoming partially destroyed, several consequences would result. There is always the potential for loss of life. The station would be immediately closed. And train service throughout the system would be shut down immediately and interrupted on an extended basis. We would have to install a shuttlebus system to operate around the portion of the rapid transit system that was nonfunctional. And this could go on for some period of time. Certainly while the station is closed, all structural elements would have to be inspected for damage. Electrical and mechanical equipment and wiring would need to be both inspected and repaired, as needed. Temporary shoring for physical structures would be necessary. And while MARTA might be able to partially open the station, the time required for repairs could take a long period of time. We estimate that this could be anywhere from a half million dollars on up.

Another scenario that relates to our system is because we utilize trackage that is adjacent to freight railroad trackage. It was a lot more economical in the construction of MARTA in the early days to utilize existing rail rights-of-way. And so we are very close to freight trains that in many instances carry hazardous chemicals and hazardous materials. In the event that one of those freight trains was to derail, it very well could run across its own property line into our right of way, causing the possibility of a collision and derailment both of the freight train as well as our own equipment. We certainly would have an awful lot of concern with regard to the impact that that could have on lives, on equipment. And it would certainly require a tremendous amount of emergency response on the part of a number of agencies.

This type of event could have significant effects on the rider-confidence in our system, our revenues on an ongoing basis, because we’re not likely to change the fact that we operate adjacent to freight railroads. And, of course, we could be looking at a significant amount of time to repair any damages to our railcars, and to our track and way.

So those are just a couple of examples. Our engineers have been very creative in coming up with ten pretty good stories to tell.

MARTA’s level of quality interagency cooperation with local police, fire, ambulance divisions and agencies on the state, federal and local level will bode well with us in the event that we were in an actual emergency. The level of teamwork and communication has been tested in several mock terrorism and disaster drills over the years, and especially in preparation for the Olympic Games which occurred last year. We simulated a bus and train collision in 1995 in order to test the response times of the various local emergency units. Participants included the American Red Cross, Grady Hospital, the Atlanta Fire Department, the Atlanta Police, MARTA Police, and other agencies. We had mock passengers with a variety of injuries, both on the trains and within the bus that was involved in the accident. We really were critical of how every agency worked together and how they responded to the unique opportunities for response that were there. And then interestingly, afterwards, we set the bus on fire so that we could allow the Atlanta Fire Department to deal with the various natures of carcinogens and other elements that are caught up in the burning of an actual bus. Fortunately for us, we haven’t had too many real-life experiences like that. But this twenty-year-old bus went to the grave in fine fashion.

Again in order to prepare for the Olympics, we undertook a mock terrorist drill at one of our rail stations. The scenario was kind of interesting and kind of chilling. There were five terrorists who took over the train with several hostages inside. And in conjunction with the SWAT team and Atlanta Police, various emergency rescue squads and MARTA, the incident was successfully resolved over the course of several hours. We did this in the middle of the night so that we would not disrupt our regular service and our regular passengers. Again, we were critical of the results so that we could learn from that experience. And we have done many tabletop exercises to also deal with that.

I hope you can see that public transit is a critical factor in moving people. We hope that the work of the Commission will take into consideration opportunities to improve protection for our piece of the infrastructure. I thank you for the opportunity to be here.

(Applause.)

THE MODERATOR:

Thank you very much. Next we have John Copenhaver of IBM.

MR. JOHN COPENHAVER:

Thank you, Ms. Abrams, and thank you, distinguished members of the Commission. I didn't come here with any prepared remarks, but I was prevailed upon by my friends at the Georgia Emergency Management Agency to say just a couple of things to you.

I have two observations, I have three recommendations and a challenge for you. The observations are, first, that this is an extremely important concept. I might say that it is something that we probably should have been working on from some time ago, but better a little bit late than never.

The second observation is that the concept thus far seems to be operating at a very high level. And there's nothing wrong with that as long as we begin to move it down to get the input of the people who have true expertise in dealing with infrastructure protection and infrastructure planning.

And that gets into the recommendations that I have. And I'm going to keep my remarks blessedly short this morning. First, I would implore you to utilize private sector expertise. There is an entire industry that has sprung up in terms of protecting private sector resources, the fundamental concept of corporate asset management as evidenced by the ability to go in and analyze corporate areas of vulnerability. And since I've heard here today that the majority of the critical infrastructure that we're talking about resides in the private sector, I would like to ask you to take a look at organizations such as the National Association of Contingency Planners, of which I'm director, the Disaster Recovery Institute International, which offers educational programs and certification programs, a number of institutions within the private sector that have tremendous expertise at putting together the kinds of programs to protect individual corporate assets that will be of benefit to you. I have heard the phrase used, "Don't reinvent the wheel." The expertise is out there. And I would ask you please to plug into that expertise.

Secondly, I would like for you to link into some of the initiatives that are taking place currently to bring together business and government to protect communities. One of the phrases that Director James Lee Witt is now using is "disaster-resistant communities." The Director was at the recent IBM summit down in Miami Beach, as well as Gen. Marsh who gave a presentation on the President's Commission.

I would ask that you find out more about some of those initiatives. For instance, there is an initiative taking place here in Atlanta that involves the Atlanta-Fulton County Emergency Management Agency, whom you've already heard from, the Georgia Emergency Management Agency, Gary McConnell and Mike Sherberger and those folks, and also the Region 4 Federal Emergency Management Agency, that I think would give you some perspective on how we're doing it over in the private sector and government sector in the area of emergency protection planning. I believe it would be of benefit to you.

And lastly, if you would, please find a way, if possible, to share some progress reports and let us know what's going on, where are you, where are the areas of challenge, how can we help you? I think that this particular gathering is very beneficial in terms of us presenting to you. Perhaps it would be a good idea if we could hear back from you something that would enable us to see where we might be able to plug in and help.

And that really gets into the last area that I have for you, and that's the challenge. I would challenge you, please make a difference for us all. On behalf of my family, on behalf of my community, on behalf of my friends, I would ask that you take this opportunity that you have been afforded to really look at and begin to do the things to plan for the future to protect the infrastructure that we all depend on and to utilize existing resources and talk to those people that can be of help, and really let us in the private sector help you. Thank you very much.

(Applause.)

THE MODERATOR:

Thank you very much. Our next presenter will be General Bill Bland, Adjutant General for the State of Georgia.

GENERAL BILL BLAND:

Thank you, Mr. Chairman, and distinguished members of the Commission for this opportunity to share some thoughts and some observations and some lessons learned by the organization that I represent. I'm speaking to you today in my capacity as both the Adjutant General and a department head of state government, the department head of the Georgia Department of Defense.

I represent a very unique organization in the military, and that is the Army and the National Guard, as well as included in my department is the State Defense Force, some 13,000 men and women that are in or contiguous to, with organizations in 150 out of 159 counties in this state.

We are indeed a community-based force that brings unique capabilities as far as performing missions. We're dual-roled, and that is our uniqueness. My responsibility as AG is to provide trained, qualified and disciplined personnel to respond to any federal contingency, whether it be war-fighting or humanitarian, whatever is directed by the federal government.

I wear another hat, and that is to provide the same trained and disciplined and capable personnel to serve the citizens of the State of Georgia in the event of an emergency or any contingency when directed by the Governor.

We did this in a very unique application — as many folks said, nontraditional use of the military — during the Olympics. And without a doubt, it was the most demanding operation I have ever been a part of personally in my almost forty years of wearing a uniform.

One of the best examples of the use of the total force, we were part of a joint task force of men and women comprised of active duty National Guard, and Reserve. The National Guard was used to provide security and ensure a safe Olympics. And I can tell you today that we accomplished that mission and accomplished it in an outstanding manner. We were able to do that because of our uniqueness.

In our state status, which is what we are when nonmobilized, we are not bound by posse comitatus. And that enables us to come in contact with the public. We had people truly enforcing the law during that time period with arrest powers while on state active duty.

I was fortunate enough to be part of the State Olympic Law Enforcement Command. That brought together all of the state agencies under one single authority that really demonstrated state government at its finest, serving its citizens. I commend this Commission on your work of developing a program to protect our infrastructure at a time when I think the threat of domestic and international terrorism is increasing rapidly, as well as the deranged individual that just wants to do some kind of damage to authority.

I think the National Guard plays a very vital role in this program. It's not unlike what we are currently doing in our counter-drug role where we're assisting law enforcement in eliminating narcotics, interdicting them as well as running demand reduction programs. And we are providing direct assistance to law enforcement.

Now, what capabilities do we bring to the table? As I said, one of my roles or missions is to provide trained, disciplined personnel for both federal and state missions. We are able to bring technology, organization, special capabilities at the grass roots level. When we have an emergency in the state, when I’m asked by Emergency Management or law enforcement through the Governor’s Office, and many times it’s direct. The local sheriff will call the local National Guard Armory and say, “Can you help me?” And that’s the way it originates. We have armories in communities. We have the ability to provide training. We did this in some capacity during the Olympics, providing training and equipment to local law enforcement, and an immediate response capability that I think can be developed much further. We could be the first responders until the real technical experts arrive on the scene.

It is just another component of military support to civilian authorities that I think can be capitalized on.

As a matter of fact, in a full mobilization, one of our military taskings is to provide key asset protection. As we all know, the potential for full mobilization is not as great as it was prior to the end of the Cold War. This whole program needs to be relooked at.

Subject to your questions, thank you for allowing me to introduce this testimony today.

(Applause.)

THE MODERATOR:

Thank you, Gen. Bland. Is there a question?

COMMISSIONER RODGERS:

I have a question. General, I take it, what you’re suggesting is that the National Guard could be brought in as a major force in the mitigation and response to emergencies which is something that has not been done before. That could be a major resource to the nation. And this is something, I take it, that’s new in the thinking?

GEN. BLAND:

As far as responding, that portion is not new. I think responding to domestic terrorism or terrorist acts is a new concept. And the capability is certainly there. As I said, we are currently assisting law enforcement and public safety through our military support plans.

COMMISSIONER RODGERS:

It seems to me that’s a very valuable resource that this country could call upon because this mitigation response to terrorism and actual disasters requires all the resources we can marshal. It seems to me this could be an excellent contribution to this effort. Thank you, sir.

GEN. BLAND:

Thank you.

THE MODERATOR:

Our next presenter will be Alan Porter of Georgia Institute of Technology.

DR. ALAN L. PORTER:

Thank you, Mr. Chairman, and members, for the opportunity to speak. As an engineer, I need some aids to do this, so we've got a couple of transparencies, if we could go to the first transparency.

I'm at Georgia Tech. The perspective I would like to share is a questioning one, a future-oriented one. The question up at the top says, "What critical infrastructures?" It's too big to fit on the screen. I guess you've got a big task in front of you. I would like to just explore a little bit towards some of the future issues that I think will be coming up. The challenge is to avoid being blind-sided.

If we could get the second? The theme up there of "managing the present from the future" is one that a group of us have leaned on for a while. It's saying, "Certainly there are good lessons to be learned from the past, but there are also some real benefits if we can get ourselves to leap ahead and anticipate." Some of the premises in there, obviously the future is going to be different than what we've experienced so far. We're in an era of accelerating change. And I won't go through the litany of examples. Obviously, the Information Age is part of that. The requirement for foresight as to emerging infrastructures, I sat and pondered a bit about your eight prime infrastructures. I don't have any suggested additions, but my hunch is that a quarter century from now, we will look back and say, "Wow, they've changed a ton." To deal with those requires some creative protection approaches. Again, if you don't know what the infrastructures are, it's hard to protect them effectively. But I think if we look ahead, we can begin to move ourselves up that curve effectively.

And I would like to just point to some of the factors that I think will drive change in the very nature of infrastructures. I've split it into two sets — technological drivers, and social drivers — arbitrarily. Some of the mass changes we are either witnessing or are on the brink of: information, materials, biotechnology, nanotechnology. I've broken out the Information Age a little bit finer because I think we're all experiencing it as that really escalates. The first thing of, "What will be the information technologies?" Telecommunications, data processing, intelligent information processing that we will rely upon and therefore will require protection. I just stuck an "e.g." out there after a few of them. No particular compulsion there. But as we move, for instance, to quantum level devices instead of our current semiconductors, what’s going to be different? The threats to that are not going to be the same, just as we’ve seen as we move from electronics to phototonics or optics.

The modes of information provision are changing. And I think that’s what we’re seeing actively right now. My example there of the linking of different electronic data sources, whether they’re text, numbers, graphics, and so forth, but the coming reliance upon that — it’s hard to get a good perspective on it. I see a little academic one. I teach a class, it’s video-based instruction. And I’m just reading term projects now on emerging technologies. I think every single one I’ve seen has relied now upon World-Wide Web sources, electronic abstract databases to get their information. Two years ago, I don’t think any did. So now the dependence on that goes up as we can’t do our work without it.

To me, the most compelling aspect of the Information Age is the bottom bullet there of emerging uses of information. We are just developing what we can do by having all this distributed or networked information available. We are going to come to rely upon it. And we will need infrastructure protection. Again, I’m broad-brushing it, not trying to point to specifics at all.

The next category of “Designer Materials,” various classifications of how we’re moving forward from the Stone Age to the Iron Age, etc. One labeling for where we are now is, “Designer Materials.” We will produce the materials we want to do what we want with them, whether that’s for structural things, electronics, you name it. There’s going to be a whole new cast of characters involved in the infrastructure, both that we can rely upon and that we will have to adapt to.

Genetic engineering or the whole biotechnology movement, again, a new set of issues is coming upon us. Probably the best depiction I’ve seen of this is a few years back now, in the ecology arena, of just going through a worry list of what are some of the things that could go wrong as we genetically engineer organisms, either for deliberate release to the environment or accidental release? And it’s a pretty daunting set of maybe thirty items to be concerned about. And again, those of you trying to protect us from things that aren’t here yet, the message is, “Wow, what a challenge.”

The most striking change is the nanotechnology. This has become a popular buzzword in the last five years or so. But the gist of it is pretty straightforward, that we will be able to manipulate at the molecular level, design what we want, and that can go several routes. One is electronics, as we get smaller and smaller. Another is biology, as we get down to genetic engineering just above it. It’s basically chemistry, but the message is we may start to do production of various entities, bottom up. If we ever come to that, and I’m quite sure we will, the “ever” is the question, sooner or later. We’re talking quarter century type time frames, not five years. But the whole cast of infrastructure issues, it just will be a different world. But I believe in the Commission’s role of looking ahead strategically, these are some things to at least begin to get us thinking about before it’s a crisis. Thanks.

On the social side, the challenge here is tremendous for you all. Just pointing to some things, economic, political, values, military, demographic shifts that change the nature of the infrastructure issue, issues such as globalization. It’s not just protection within the U.S. It’s electronic funds transfer, information. Obviously, this country has a particular stance with respect to secure cryptography and so forth. What if we were to have some major economic changes? What would a Great Depression do to these issues? Political changes — again, not as a political scientist, but as someone watching, I’m kind of mesmerized by, on the one hand, we’re going through this increased linking together internationally, particularly with respect to economics, and on the other, we break up our nations because we have ethnic or religious or whatever differences. How do you pull that together if you’re protecting infrastructure?

Value changes of various natures. I know looking back, if we go back fifty years, it’s amazing how American values are not this rock-solid thing. If you did something that was totally in tune with what the American public wanted fifty years ago, you would probably be put up against the wall with a firing squad today because our values are different. So how do you protect toward aims that we don’t have pinned down yet?

Demographic shifts, I suspect you’ve all addressed some of these issues, so just to push to my last one here. What to do about this? I don’t know. But I would urge that the Commission begin to try to weave in these sorts of concerns of what are the likelihoods and importances of some of the changes that will be taking place.

One approach as a futurist that we’ve found productive is to think in terms of not just “the future,” but alternative futures, sets of scenarios that can weave together some of the nasty cases, for instance, as you’ve seen on a practical level with the Olympics planning and terrorist acts and so forth. I think on a grand scale, that can be done as well, with utility.

What will be the critical infrastructures, and probably more importantly, the sensitive points ten years, fifty years from now? I think by raising the questions early, there is the potential for a good payoff in protecting them.

Critical issues for analysis? I have not made a real attempt to get to that, but I believe the punch line here is that there is change and that the issues are not going to be what they are today.

Can we move toward generation of effective strategies? I would hope we would experiment and try a whole range of approaches, if we really have areas of high uncertainty, pointing toward adaptive, flexible quick response approaches.

I will quit there. Thank you.

(Applause.)

THE MODERATOR:

Thank you, Dr. Porter. Our final speaker is Richard Daniel of the DeKalb County Water and Sewer Department.

MR. RICHARD P. DANIEL:

Mr. Chairman, members of the Commission, I appreciate this opportunity to speak to you today. My name is Richard Daniel. I direct the Water and Sewer Division of the Public Works Department of DeKalb County. DeKalb County Water and Sewer operates a 128 million gallon a day capacity water treatment plant, two wastewater treatment plants equating to approximately 50 million gallons in capacity, and water distribution and wastewater collection systems each in excess of over a thousand miles. We service a population of some 600,000 people. With our infrastructure spanning the entire cross-sectional area of DeKalb County and our raw water pump station, our source of raw water being the Chattahoochee River, and being located on the Chattahoochee in Gwinnett County, our vulnerability is widespread.

Utilizing surface water as a supply of potable water in the Atlanta region, the entire region shares a vulnerability to chemical or biological contamination of that raw water supply. Though not a physical threat, I and some of the water managers that I work with feel that we have some threat to our supply through federal legislation designed to sell the power management agencies. The Southeast Power Association, SEPA, is involved in the current operation of Lake Lanier, which of course feeds the Chattahoochee River, which is our source of supply. As of today, no contracts are in place that would cause an unscrupulous buyer to provide us the water we need for our citizens and for wastewater assimilations down river.

Returning to the physical threats, we believe our physical threats include our water treatment plant, our river or raw water pump station, our sanitary sewage treatment plants, and to a lesser extent, our water storage and repump stations and our water distribution system. If you think about what I just named, that includes our entire system with the exception somewhat of our wastewater collection system.

Unfortunately, I don’t think this is too uncommon in the Atlanta area, and it may not be uncommon nationwide.

We provide a minimum deterrent to sabotage. You would probably classify it more as vandalism. We man our sites. We fence our sites. We patrol our sites. But when you look at the overall area of DeKalb County, and of course the other counties and cities have this same problem, there are numerous points in our distribution systems that vandals can access our potable water supply. We don’t have any answers. And I apologize to you for coming in here with nothing but problems and no answers. But I’ve thought about it a lot, and I can’t find anything that I can do in my distribution system that could stop someone from introducing some contaminant that might hurt my customers.

Again, I thank you for letting me come to speak to you. And I leave you with that one thought. In my opinion, the water and sewer industry is very vulnerable to threats from sabotage. Thank you.

(Applause.)

THE MODERATOR:

Thank you, Mr. Daniel. And I would like to ask finally, is there anyone remaining who would like to speak? If not, I would like to thank everyone here for participating in this process, for contributing to the work of the Commission. And if you would like in the future to contribute any further remarks, please see the staff people at the table on your way out. And we will give you our mailing address and our e-mail address.

And now, Chairman Marsh?

CHAIRMAN MARSH:

Thank you all very, very much. We really appreciate your cooperation and all of your inputs, and we take them seriously. Thank you.

(Hearing concluded.)