

**THE NATION'S WIRELINE AND WIRELESS
COMMUNICATIONS INFRASTRUCTURE IN LIGHT
OF SEPTEMBER 11TH**

HEARING

BEFORE THE

SUBCOMMITTEE ON COMMUNICATIONS

OF THE

COMMITTEE ON COMMERCE,
SCIENCE, AND TRANSPORTATION

UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

—————
MARCH 6, 2002
—————

Printed for the use of the Committee on Commerce, Science, and Transportation



U.S. GOVERNMENT PRINTING OFFICE

91-395 PDF

WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUE, Hawaii	JOHN McCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAU, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBAC, Kansas
BARBARA BOXER, California	GORDON SMITH, Oregon
JOHN EDWARDS, North Carolina	PETER G. FITZGERALD, Illinois
JEAN CARNAHAN, Missouri	JOHN ENSIGN, Nevada
BILL NELSON, Florida	GEORGE ALLEN, Virginia

KEVIN D. KAYES, *Democratic Staff Director*

MOSES BOYD, *Democratic Chief Counsel*

JEANNE BUMPUS, *Republican Staff Director and General Counsel*

SUBCOMMITTEE ON COMMUNICATIONS

DANIEL K. INOUE, Hawaii, *Chairman*

ERNEST F. HOLLINGS, South Carolina	CONRAD BURNS, Montana
JOHN F. KERRY, Massachusetts	TED STEVENS, Alaska
JOHN B. BREAU, Louisiana	TRENT LOTT, Mississippi
JOHN D. ROCKEFELLER IV, West Virginia	KAY BAILEY HUTCHISON, Texas
BYRON L. DORGAN, North Dakota	OLYMPIA J. SNOWE, Maine
RON WYDEN, Oregon	SAM BROWNBAC, Kansas
MAX CLELAND, Georgia	GORDON SMITH, Oregon
BARBARA BOXER, California	PETER G. FITZGERALD, Illinois
JOHN EDWARDS, North Carolina	JOHN ENSIGN, Nevada
JEAN CARNAHAN, Missouri	GEORGE ALLEN, Virginia

CONTENTS

	Page
Hearing held March 6, 2002	1
Statement of Senator Burns	11
Prepared statement	11
Statement of Senator Inouye	1
Statement of Senator Wyden	13

WITNESSES

Cangemi, Agostino, Deputy Commissioner—General Counsel, Department of Information Technology and Telecommunications	2
Prepared statement	7
Crotty, Paul, Group President for New York and Connecticut, Verizon, Inc.	33
Prepared statement	38
Harris, Gloria, Vice President of Operations—New York, New Jersey and Connecticut, AT&T Wireless	41
Prepared statement	44
Herda, Larissa, Chairman, Chief Executive Officer and President, Time Warner Telecom	50
Prepared statement	53
McLean, Christopher A., Counsel, ComCARE Alliance	23
Prepared statement	25
Nash, Glen, President, Association of Public Safety Communications Officials International, Inc.	29
Prepared statement	31
Souder, Steve, Director, Montgomery County, Maryland 9-1-1 Emergency Communications Center	13

**THE NATION'S WIRELINE AND WIRELESS
COMMUNICATIONS INFRASTRUCTURE IN
LIGHT OF SEPTEMBER 11TH**

WEDNESDAY, MARCH 6, 2002

U.S. SENATE,
SUBCOMMITTEE ON COMMUNICATIONS,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:31 p.m. in room SD-253, Russell Senate Office Building, Hon. Daniel K. Inouye, Chairman of the Subcommittee, presiding.

**OPENING STATEMENT OF HON. DANIEL K. INOUE,
U.S. SENATOR FROM HAWAII**

Senator INOUE. Before we proceed, I would like to apologize to all of you for the lack of attendance. As some of you may be aware, at this moment a special briefing conducted by the Secretary of Defense and General Wheeler on the military activities in Afghanistan is just about to close. That will be followed by a special meeting with President Mubarak of Egypt. So I do not expect too many members to be attending this hearing.

However, because of the significance and importance of the meeting, I will make certain that your testimony will be studied and read by my colleagues.

In the wake of the tragic events of September 11th, a large amount of Congressional attention has rightly focused on matters involving the safety and security of Americans. Indeed, in the last 6 months this Committee has already considered proposals to improve the safety of our ports, our airports, and our railways. In keeping with this theme, today's hearing examines the safety and security of our Nation's communications infrastructure. Through the testimony of today's witnesses, we hope to assess both how our wireless and wireline networks performed and responded to the events of September 11th and how in the future we might improve the reliability and robustness of these networks in emergency situations.

Before going further, let me first express my personal thanks to the emergency personnel, government officials, and the many communications workers who worked tirelessly both during and after September 11th to restore voice and data communications. Their relentless efforts, often in the face of extreme adversity, deserve both our recognition and our gratitude.

The events of that day placed an enormous strain on our communications network in both New York City and Washington, D.C. In New York City, damage to a Verizon central office caused by the collapse of the World Trade Center cut phone service to tens of thousands of businesses and residents in lower Manhattan. In Washington, D.C., as individuals attempted to contact their loved ones, wireless traffic demand spiked to over 200 percent, leaving customers struggling to get a dial tone. In both places, officials on the ground struggled to communicate and coordinate among the various emergency response teams dispatched to Ground Zero and the Pentagon.

While we in Congress, along with all Americans, hope and pray that our wireline and wireless networks will never again face so severe a test, we must continue to explore ways to improve the resiliency and reliability of our communications infrastructure. Moreover, because reliable communication is critical to the success of emergency personnel, our efforts should also include a consideration of ways in which new technological tools such as location information, peer to peer communications, reverse messaging, and broadband applications can be utilized by emergency personnel in order to help save lives.

Accordingly, I look forward to the testimony of the witnesses and their responses to questions that may be posed by Members of the Subcommittee.

We have two major panels. On our first panel I am pleased to call the Deputy Commissioner-General Counsel of the City of New York, Mr. Agostino Cangemi, and the Director of Montgomery County, Maryland, 9-1-1 Emergency Communications Center of Rockville, Maryland, Mr. Steve Souder. Gentlemen, welcome and I appreciate your attendance here. Mr. Cangemi, welcome, sir.

Mr. CANGEMI. Good afternoon.

Senator INOUE. You may proceed, sir.

STATEMENT OF AGOSTINO CANGEMI, DEPUTY COMMISSIONER-GENERAL COUNSEL, DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Mr. CANGEMI. Good afternoon and thank you for this opportunity to tell you the story of our telecommunications restoration efforts in New York City following September 11th. I will tell you about the challenges we faced—

Senator BURNS. Pull that microphone up so we can hear you a little bit.

Mr. CANGEMI. Sure.

Thank you for inviting me to tell you the story of the telecommunications restoration efforts in New York City. I would like to address some of the challenges we faced, what worked, what worked well, the process we used, were there opportunities to improve, what did not work so well, and what we are currently doing in New York City to improve the infrastructure going forward.

It has been 6 months. I did want to kind of couch this testimony in terms of trying to take you back to that day. For many of us in New York, it was an attack on the country, but also an attack on where we go to work every day, as well as you here in Washington.

It was an attack on our families and it was an attack on our colleagues. So there was a sense of anger, anguish, and a desire to do something on the part of telecommunications workers and government officials. We were not at Ground Zero able to actually try to dig out the rubble, but we tried to do as much as we could.

That kind of sense is what pervaded the efforts we had along with the telecommunications providers in New York City, that kind of cut through the clutter, cut through some of the competitive issues that I had witnessed in the past. I had personally been involved in things as mundane as area code proceedings in New York City in front of the Public Service Commission and those things can get pretty heated. But around the time of September 11th that type of competitive edge and clutter was not there and competitors were able to work cooperatively together to restore service as quickly as possible.

Let me first address the challenges that we faced. We in downtown Manhattan had over 30 critical city government buildings. About 50,000 voice lines went down. They were all connected to one central office that had been severely damaged due to the collapse of World Trade Center 7. We also had to migrate our web site. My agency, the Department of Information Technology and Telecommunications, is responsible for all data, voice, e-government and web site initiatives, as well as we are the local franchising entity in New York City. But voice remained the biggest issue.

So what worked? What did we do? Back in the early nineties we established something called the MARC, M-A-R-C. I noticed as I got off the train here in Washington that "MARC" may mean something else to you around here, but to us it means the Mutual Aid and Restoration Consortium. In the early nineties, New York City government officials along with telecommunications providers created a consortium, an actual contractual agreement as well, among the local telecommunications providers to plan for the cooperative resumption of voice and data traffic in the event of a catastrophic situation. In fact, the broadband franchises in New York City or the licenses—what we use franchises for are the right to actually provide broadband services in New York—require participation in this MARC agreement.

Although many competitive issues had kind of allowed this consortium to wane a bit, we were able to immediately convene a conference call of the 40 largest telecommunications providers in New York City by early September 12th. This included the 18 franchisees doing data and voice services in New York City, as well as the six primary wireless carriers, government officials, equipment makers, some of them not officially members of the MARC, but wanted to help as much as they could, so they participated in our calls.

We convened twice-daily conference calls and had an open bridge line, which allowed everybody to communicate and assess the situation as quickly as possible. We shared information. Much of the information was proprietary information that competitors would not necessarily want to share with each other. But it worked to restore service as quickly as possible.

Generally what the approach we used with MARC was the commissioner of my agency would chair twice-daily conference calls.

We had a central Office of Emergency Management that established what the priorities would be for restoration, and that was critical because the telecommunications companies were getting calls from everyone, calls if they could make the calls. But they were getting contacted as much as possible, and trying to assess what the priorities were from a New York City government perspective was difficult for them and impossible without this type of arrangement. So our Office Emergency Management played that role and communicated to us what the priorities were.

We would put out the request to the carriers on these calls and they would offer to assess, do a field survey to find out who can restore service as quickly as possible, as cost efficiently as possible, but primarily we were concerned with restoration of services as quickly as possible.

Verizon had dedicated much of their resources to getting that central office back up and running, as well as working on our police command center—they did a fabulous job there—as well as our stock exchange, which was a priority set forth by the President.

When we set out to do this, it involved having access to the Ground Zero area. Without this MARC process in place, in the early days it was our police department, our local responders, that were controlling access to the area. It would have been impossible for the competitive providers or many of the workers of these companies to get to that area. So we were able to coordinate through the MARC process access and that was one of the most critical functions, and it served them quite well.

I can tell you that diesel trucks that were necessary in order to fuel the generators, the backup generators, in downtown Manhattan did not look too inviting on the days of September 12th and 13th and would not have been able to get down there but for this MARC process in coordination with our local police authorities.

What were the results of this process? Well, our Office of Emergency Management had been in 7 World Trade Center and was destroyed, but through the MARC and through working with the local telecom providers we were able to have an interim physical site established within 2 days. City Hall was restored by September 14th. Our municipal building, which houses many of the critical government agencies and comptroller's office and other city agencies, was restored by September 15th.

What are some other things that worked besides the MARC? Well, we had also developed and centralized much of the Y2K pricing. The Y2K pricing books were in the Office of Emergency Command Center, so many of them were lost. But we were able to have some backup plans in place and wiped off a little bit of the dust, and many of the scenarios that we had prepared for Y2K we were able to kind of use the same processes that worked quite well.

For instance, we had warehoused spare equipment that was immediately available for our command center, as well as cellular phones and telecom equipment that we had warehoused and was accessible for Y2K planning. We were able to supplement that with any of the vendors who were on the MARC calls. So as far as access to equipment, we were able to procure that and obtain that as quickly as possible.

Other things that worked with the Y2K planning was we had an Internet-based communications process. Our Office of Emergency Management had a process for essential personnel and they were connected through Blackberries and wireless-based Internet services, so they were able to communicate at Ground Zero.

We also had a pretty effective GIS mapping process in place that was able to develop maps for emergency workers, describe the restoration process and access points for buildings. That kind of information was critical and we were able to do that remotely.

We implemented Voice Over Internet Protocols. That was something that had been in the pilot phase. We did not have time for the pilot any more. We implemented it and it worked at City Hall as well as a number of other city buildings.

We greatly increased the wireless capabilities by distributing Blackberries and similar types of equipment to essential government workers and that was essential to restoring services.

What are some opportunities for improvement? Well, the destruction made it—the destruction of the central office really created too big of a problem for the government. We had much too many lines, 50,000 phone lines, addressed by one central office without an alternative carrier in place.

The other things we did not think about were some of the human and physical space factors in planning. Even though we were able to restore service, we were not able to get the personnel back into the buildings in downtown Manhattan for sometimes over a week, sometimes 2 weeks, depending on where they were. So that was an area of planning that we could have improved upon.

Also on the wireless front, the wireless carriers were not part of the MARC consortium officially, although they participated in our calls. I think on that front they are an industry not accustomed to local regulation as well as some of the tariff providers who are more accustomed to dealing with public service commissions and local regulatory authorities. So that was probably an industry where we can see some improvement in terms of disaster recovery planning.

Some of the lessons learned. We are going to be developing a disaster recovery plan that includes some of the items I discussed, such as human and physical factors, as well as operations, communications, and technology, and factor in just the stress and the trauma and even the death of some of the critical resources that may be available. We need to focus beyond the IT infrastructure to the relocation and work resumption of business users that rely on that infrastructure.

We did learn that our Y2K plan worked and for other municipalities and other jurisdictions across the country, they may want to take a look at their Y2K plans and think of them in light of the World Trade Center attack.

Lastly, you have to be creative. Voice Over IP, wireless, land line, broadband, we used what worked, as quickly as we could get it.

What I want to address is, quite briefly in closing, is what my agency is doing on behalf of the City of New York to improve our telecommunications infrastructure. I already addressed our GIS application, our mapping application. We are going to be mapping all

of the broadband fiber in New York City onto this GIS application. In the event of another service outage, we will have at our fingertips knowledge as to where all the fiber exists in our city streets, as well as who owns that fiber and an ability to quickly deploy a plan to restore service.

The MARC is something that can work in service outages not as dramatic as something that happened at the World Trade Center. We are going to try to use this with our downtown financial businesses so that they know and they have confidence in New York City's infrastructure and they know that there are options to them to have a redundant, resilient, telecommunications infrastructure in place and they do not need to move their businesses elsewhere.

We are coordinating with those downtown businesses to do just that, so that they have an understanding of what the infrastructure is. We found out very quickly after September 11th that they really did not understand. They asked the kind of questions about wireless, redundancy—they thought that if they paid a bill to MCI WorldCom or AT&T that somehow they were going to have five 9's types of redundancy. They did not understand kind of the infrastructure that depended on going through central offices and how a break point at that central office could really bring down their entire operation.

As far as city government buildings are going, we are actually developing an alternative fiber loop in an alternative conduit system that will link all of the critical city buildings in downtown Manhattan on a completely separate fiber conduit path.

We are also—just trying to be creative, we found out that we had water pipes that used to be used 100 years ago for water. When firemen needed excess water pressure to fight fires in downtown Manhattan, they needed these big pipes in downtown Manhattan. They are just sitting there. They are in still pretty good shape. We are trying to convert those old water pipes for telecommunications purposes and we have seen a lot of interest in having that kind of disaster recovery option.

We are going to be using our city-owned buildings for siting of wireless facilities. In the past we shied away from that—a lot of community concerns. Everybody wants their cell phone to work, but no one wants any cell antennas in their area. But we have made that choice. We are going to be using our city buildings that actually exist in some of the most critical areas to enhance coverage. We view it as both a public safety initiative as well as there will be some revenue perhaps.

The other thing we are trying to address is trying to reduce the cost for telecommunications providers to get to that last mile. In New York City, most of the fiber goes through one central path of conduit that circles around downtown Manhattan in the main area, but there are still hundreds of buildings, large office buildings, that do not have broadband connections. We are going to be issuing requests for proposals to try to greatly reduce the cost of getting into the building through mini-consortiums so that the construction costs of getting to that building will be greatly reduced, and once folks have broadband connections they will not be as reliant on copper connections to a certain central office.

In conclusion, I think we suffered a great blow on September 11th. We were knocked down. We are getting up. We are doing exactly the kinds of things to improve our telecommunications infrastructure that is necessary to get New York City's industry and government back on its feet.

Lastly, if I may make a small plug. I hear that you are interested in coming back up to New York perhaps. It has been I think over 200 years, but it would be a nice shot in the arm to see you come up to New York, certainly a welcome visit. So we look forward to seeing you.

Thank you.

[The prepared statement of Mr. Cangemi follows:]

PREPARED STATEMENT OF AGOSTINO CANGEMI, DEPUTY COMMISSIONER-GENERAL COUNSEL, DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS, CITY OF NEW YORK

Mr. Chairman and Members of the Subcommittee:

I am Agostino Cangemi, Deputy Commissioner and General Counsel of New York City's Department of Information Technology and Telecommunications (DoITT). On behalf of the City of New York, and DoITT, I thank you for the opportunity to appear before you today. I would like to touch on several issues related New York City government's telecommunications restoration initiatives after the September 11 attack: What happened; what worked; recommendations based on lessons learned; and, finally, what the city is doing, and requires, in order to improve its public safety telecommunications infrastructure and preparedness.

WHAT HAPPENED

Clearly, September 11 had a devastating impact on New York City government's communications infrastructure. Scores of buildings, including police headquarters, City Hall, our main Municipal Building and several other critical city government sites in lower Manhattan's Civic Center were thrust into complete communications darkness. These failures were a direct consequence of the severe damage to Verizon's 140 West Street central office caused by the collapse of 7 World Trade Center.

As many as 50,000 telephones on the desks of City employees, and thousands of links that provide data access for critical operational tasks, were suddenly unavailable. Besides supporting most of the city government's telecommunications infrastructure, Verizon's West Street facility also housed the point-of-presence (POP) for the Internet Service Provider of the city's "e-government" website, NYC.gov.

WHAT WORKED

Y2K Preparedness

DoITT managed restoration activities in close coordination with the Mayor's Office of Emergency Management (OEM). As part of Y2K planning, DoITT and OEM had already prepared for the possibility of comprehensive failure in the city's communications networks, and had established a framework for responding to such an event. Among other things, the contingency plan included a protocol for providing essential personnel with immediate access to wireless and Internet-based communications equipment. It included warehousing "spare" telecommunications and computer equipment that could also be immediately deployed. The contingency plan included redundancy for the city's data network at two separate locations. And it provided for the city's mainframe data center to be remotely located and run as an always-on "hot site."

Mutual Aid and Restoration

Contingency planning for a potential telecommunications crisis in New York City truly began in earnest in 1992 with the establishment of the New York City Metropolitan area Mutual Aid and Restoration Consortium (MARC). MARC arose out of the recommendations of a public-private mayoral Task Force, which was charged with developing a plan for voice and data traffic to be handled by alternative carriers in case of a critical disruption to the telecommunications networks supporting the city. Fourteen telecommunications carriers that served the city's Metropolitan area were the original signatories to the MARC agreement, essentially establishing a framework for cooperation among competitors. Under the terms of the city's cur-

rent franchise agreements, new franchisees are similarly obligated to “pursue avenues involving mutual assistance,” as set forth in the MARC agreement.

Clearly, the telecommunications landscape, with respect to technologies, competition and the law, has changed dramatically since MARC’s inception. This evolution may have diminished signatory enthusiasm for the MARC agreement somewhat. Nonetheless, on September 11, MARC was successfully convened as the primary vehicle for delivering alternative voice and data services to essential City government offices and operations. The accomplishments of this cooperative undertaking came primarily as a result of the ability and willingness of the city, MARC members, and participating non-MARC members with telecommunications assets in the city to make spontaneous adaptations to procedures that did not necessarily anticipate a catastrophe on this nature and magnitude. Fundamentally, however, the MARC-based framework worked, and worked as follows:

- As envisioned in the MARC agreement, following the attack, DoITT began chairing twice-daily teleconference meetings with MARC members and non-MARC members with telecommunications assets in the city to organize the restoration of voice and data services to city government buildings.
- Critical restoration sites were identified, and prioritized, by OEM’s Emergency Operations Center. The telecommunications carriers participating in the teleconferences were asked for proposals either to activate existing carrier services in, or to bring new carrier services to, buildings on the city’s critical priority list.
- Carriers who believed they had the ability to provide the required restoration or provisioning services were invited to undertake joint site visits and submit proposals. Vendor selection was based on a carrier’s commitment, and apparent ability, to restore necessary services more quickly or more completely than could other potential vendors. Vendors were also required to include cost estimates in their proposals.

Finally, as also envisioned by MARC, DoITT used the teleconferences to encourage and coordinate the pooling of telecommunications resources among carriers to further facilitate the delivery of alternative voice and data solutions. This took place while Verizon dedicated much of its resources to getting their central office back up and running, while working on restoring the city’s Police command center (where they did a tremendous job), and the stock exchange.

Ultimately, through the MARC process, alternate telecommunication services were delivered to city offices by, among other measures, physically bringing new fiber and equipment into the affected buildings. These newly installed “facilities” permitted the provision of voice and data services. As necessary, PBX systems were also installed to support the restored voice communications. Notably, however, Voice over Internet Protocol (VoIP) solutions more quickly restored voice services (to such essential critical sites as City Hall) than did the PBX systems. In other cases, fixed-wireless solutions provided the most expedient route.

It should be noted that an array of critical activities supporting the MARC process took place concurrently with the teleconferences. Among them, DoITT actively compiled a database of functioning carrier POPs and other network infrastructure elements to augment the city’s already existing geographic information system (GIS). The GIS maps provided information on critical access points for emergency workers. Additionally, this centralized inventory of knowledge facilitated a more efficient coordination of carrier resource pooling during the teleconferences.

DoITT worked with OEM and the Mayor’s Office to help ensure access for utility personnel to affected sites for field surveys and restoration work. The field surveys were undertaken to develop a scope for the specific set of services needed, and to assess the completeness of the alternate carrier’s proposed solution. Ensuring access to “Ground Zero” was not always a smooth process, due to the unprecedented level of security in the area, and the presence of emergency response, law enforcement and relief officials from a variety of local, state and federal organizations. Nonetheless, in virtually all cases, access was eventually secured without inordinate delay under the circumstances. It is indeed questionable whether, for example, the diesel trucks that were needed to fuel backup generators would have been able to gain access at all but for the MARC process in coordination with our local Police.

DoITT also initiated an unprecedented “wireless MARC.” To their credit, all public and private sector entities transmitting in the affected area voluntarily participated. The main purpose of the teleconferences, which occurred twice daily at the outset of the crisis, was to monitor and, if necessary, remedy any interference on the 800 MHz emergency response frequencies. This undertaking was especially important because of the many temporary wireless facilities, including cells on wheels (COWs), being deployed. Although restoration was not undertaken through wireless

MARC, this could have been an additional function of the initiative had there been such a need.

Results of Preparedness and Restoration Efforts

As a result of these efforts:

- NYC.gov, which provided city employees and the public with essential information during the crisis, was physically rerouted by 10:40 p.m. on September 11.
- OEM, which lost its building in the attack, utilized a fully equipped mobile bus before establishing an interim site also on the evening of September 11. Within 48 hours, a new, fully operational facility was built.
- City Hall's communication services were restored by September 14. The Municipal building, including the city Comptroller's office and many other city agencies were restored by September 15.

Ultimately, by quickly restoring communications, the City of New York was able to fulfill its core obligation of protecting public health and safety. A less tangible, but highly important related benefit was that the public was reassured as to the *ability* of their government to do its job in the face of otherwise devastating circumstances. Stated somewhat differently, the fact that we were not only functioning, but soon operating at a fairly sophisticated level, provided some comfort to a city under attack.

LESSONS LEARNED AND RECOMMENDATIONS

The foremost lesson learned, and my recommendation to other states and municipalities, is to establish a comprehensive communications recovery plan. Such a plan should at a minimum encompass an "operational" component, a "resource component," and a "contingency" component.

Operational Component

Governments that have not done so, should consider establishing an emergency management entity, like New York City's OEM, with core responsibility for undertaking a communications risk assessment and for linking this assessment to a business continuity plan. I would further recommend consolidating information technology with voice, data, cable and other communications functions into a single entity like the New York City's DoITT. Such entity would provide centralized expertise to the emergency management entity in its communications risk assessment and business continuity plan.

With respect to risk assessment and business continuity plans, I would further suggest:

- Prioritize "mission critical" applications for restoration.
- Plan for the worst, including both physical and human "loss."
- Rehearse and update the plan, especially as key resources and partners change.

In an emergency, the emergency management entity plays the role of quarterback under the Mayor's direction. It also provides an essential link to other emergency management bodies, at other levels of government, both in preparation for, and in times of, emergency.

Resource Component

As I noted, governments must prepare for the loss of physical and human resources in times of emergency and, particularly, when under attack. For example, the telecommunications and computer equipment New York City had warehoused as part of Y2K planning were made immediately available to OEM when its headquarters at 7 World Trade Center were destroyed. These stockpiled resources, along with donated equipment, were used to help establish an interim site for the agency within two days.

In hindsight, however, we probably did not sufficiently plan for "physical space factors" (i.e., relocation). Even where the city was able to restore telecommunications services, we were not always able to get personnel back into buildings for two weeks or more. And in some cases the city was forced to make very ad-hoc, and less than ideal, arrangements for temporary work space.

Indeed governments should be ready not only to relocate employees, but must prepare for the potential impact of stress, trauma, injury and, even, death in their planning. One possible measure is to create a "knowledge-oriented" database that can be accessed if human resources suddenly become unavailable.

Contingency Component

Finally, I would emphasize the critical importance of voice and data backup and redundancies as perhaps the most critical elements of contingency planning. In New

York City's case, network backup and redundancies made all the difference in data recovery.

Voice communication, on the other hand, was among our most critical problems. I recommend having a contingency plan in place to access alternate carriers, if possible utilizing alternate conduit, central offices and technologies. A robust combination of landline, wireless and VoIP technologies is invaluable for ensuring fast recovery. Such combination provides governments with the flexibility to deploy the fastest and best "fit" under unpredictable circumstances.

WHAT NEW YORK CITY IS DOING AND WHAT WE NEED

What We are Doing

Briefly, I would like to summarize the steps New York City is taking in the wake of September 11, to improve our communications infrastructure:

- **Geographic Information System**—I have mentioned the city's GIS, or mapping, application. We are going to be mapping *all* the broadband fiber in the city, and who owns the fiber, on our GIS. With this knowledge at the city's fingertips, in the event of another service outage, we will be able to even more quickly restore service through MARC.
- **MARC**—The city is revising MARC based on this experience. We are attempting to formalize participation in the consortium by wireless carriers, and to improve the city's coordination with federal and state regulatory and emergency management authorities. In addition to running MARC restoration drills, we will be reaching-out to our business community to determine whether and how the private sector may benefit from MARC.
- **Supporting Business Community**—The city is coordinating with the downtown business community to assist in their development of a redundant telecommunications infrastructure. At the same time, the city intends to work with other private sector representatives and telecommunications disaster recovery experts to gain a comprehensive picture of private initiatives already underway—at the corporate-level, industry-level and business district level—to assess areas in which the city can play a supportive, or complementary, role. We also want to impress on businesses, based on DoITT's unique vantage-point as a franchising agency, that they have options based largely on the infrastructures already in place for redundant and resilient service (and that they do not need to move their businesses elsewhere).
- **New Fiber Loops**—The city is issuing a request for proposals to develop in an alternative fiber loop, that will link all of the critical city buildings in lower Manhattan, on a wholly separate fiber conduit path. Trying to be creative, the city has also found that we have vacant water pipes, which have been unused for 100 years, just sitting there in pretty good shape. We are trying to convert these old pipes into alternate conduit, and have seen a great deal of interest in developing that additional disaster recovery option.
- **Wireless Facilities on City Buildings**—In addition, city-owned building will now be used for siting wireless facilities. In the past, we have been reluctant on this front, due partly to community concerns. Nonetheless, the city has determined that it is in the public's best interest to proceed with an initiative to use our buildings to enhance coverage in the most critical geographic areas.
- **Reducing Last Mile Costs**—We are also attempting to address reducing the cost for competitive telecommunications providers to get access to the last mile. In the City, there are still hundreds of large office buildings that do not have broadband connections. The city is going to issue requests for proposals to try to greatly reduce the cost of getting into the buildings (i.e., by constructing "laterals") through mini-consortiums. This would greatly reduce the related construction costs, and reliance of copper connections to a single central office.

What We Need

Channel 16—As first responders, the city Police, Fire and other emergency services must be assured that they will have sufficient bandwidth to save lives, and protect themselves, in emergencies. In this respect, I can not overstate the importance to the city of being provided with the permanent right to utilize the Channel 16 radio spectrum (482 MHz—488 MHz).

The city will soon be petitioning the FCC to remove the conditions under which it granted a waiver in 1995 to twelve metropolitan area agencies for use of Channel 16 radio to construct a public safety radio network. Under its original terms, the waiver was to last a minimum of five years, after which time it could be terminated by the FCC for digital television use.

The NYPD utilizes Channel 16 for its data communication needs, and has completed installation of Channel 16 interoperability channels for use by first respond-

ers in the Metropolitan area. City Emergency Medical Services (EMS) uses Channel 16 to dispatch ambulance service. And the Fire Department is in the process of deploying thousands of “fire-ground” radios to support firefighter communication requirements at fire response sites. Following a comprehensive consulting study, Channel 16 will be further built-out to support a voice and data requirements of City agencies, including Police, Fire, EMS and other critical agencies, and to provide interoperability between first responders.

A permanent right to Channel represents our most critical post-September 11 public safety spectrum need, which cannot be accommodated via the overcrowded 800 MHz public safety spectrum, or by Channels 14 or 15. Ultimately, it represents a unique opportunity for the City to develop a state-of-the-art communications system. Because City agencies operate primarily in the frequency bands that encompass Channels 14 and 15, a permanent grant of contiguous Channel 16 spectrum would permit interoperability, and enable the utilization of existing radio equipment. This would avoid radio replacement costs running in the hundreds of millions of dollars. Alternatively, the reallocation of Channel 16 to broadcasters could create significant interference with the City’s operations on Channel 15.

Municipal Franchises

There appears to be a trend underway, both regulatory and legislative, to “deregulate” local jurisdiction over telecommunications providers in general, and the so-called “information services” offered by ILECs and cable companies in particular. The city disagrees with the legal underpinnings for such proposals, and we will be filing comments with the FCC making our case. Today, from a policy standpoint, I would like to point out that the city’s experience demonstrates that franchises do not hinder deployment of services. Moreover, franchise fees provide municipalities with fair compensation for the use of public property. Most relevant to this proceeding, however, an overlooked aspect of local regulation is that it provides municipalities with leverage to guarantee carrier to participate in coordinated restoration initiatives, like MARC. And it also provides municipalities with leverage to gain access to critical infrastructure information, such as that needed for GIS mapping.

Finally, there is a need for improvement on the wireless front. Although wireless carriers participated voluntarily and commendably on the city’s MARC after September 11, they are as an industry not accustomed to having any binding accountability to local government. Since wireless plays such a critical function in emergency first response, and in providing communications of last resort in an emergency, it would be useful for the federal government to consider how the industry can be better brought into the fold in disaster recovery planning.

CLOSING

In conclusion, I would say that New York City suffered a devastating blow on September 11. We were knocked down; but we are getting up, I think, faster than anyone expected. We are doing exactly the kinds of things to reevaluate and improve our telecommunications infrastructure that are necessary to revitalize the city government and private industry.

Senator INOUE. Thank you very much, Mr. Cangemi.

Before I call upon Mr. Souder, Senator Burns, do you have any statement?

STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Senator BURNS. I have a statement, Mr. Chairman. I just thank you for holding this hearing and I will just submit my statement for the record.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

I would like to thank the Chairman for holding today’s hearing, which concerns a topic of critical importance to our national security. Today’s hearing will review the rapid response to the September 11 attacks by our public safety officials and commercial wireline and wireless carriers, which required nothing short of heroic effort under the most extreme pressure imaginable. Additionally, this hearing will look to the future to determine how best to create a unified, robust national communications infrastructure. The searing experience of September 11 revealed the im-

portance of redundant networks, multiple facilities-based providers and priority access for public safety officials. Additionally, as we venture into the complex area of comprehensive spectrum reform, we should bear in mind the vital nature of spectrum to those on the front line of homeland defense—our police, fire, medical, public health and other emergency response agencies.

I want to draw particular attention to the very heart of our public safety communications infrastructure, the 911 network. In the wake of the attacks on America, the underpinning of our entire civil defense effort is our ability to communicate during times of crisis. For this reason, we must maintain our focus on building out the next generation of wireless enhanced 911 services. Enhanced 911 is a key component of our national emergency communications system and so is a top priority for this Subcommittee. The tools that will prove most valuable in responding to additional attacks will also save countless lives in individual as well as mass emergencies.

The Subcommittee will certainly benefit from the expertise of our distinguished witnesses as we grapple with these difficult issues. I would like to particularly welcome Chris McLean, who will be testifying today on behalf of the ComCARE Alliance. Chris has been a tireless advocate for the building of the next generation of public safety communications—an integrated, digital, nationwide emergency communications system. I enthusiastically support this worthy goal and look forward to working to implement ComCARE’s “E-Safety Program.” The “E-Safety Program” calls for the support of state planning and deployment of Integrated Emergency Communications Systems in Model States, additional capacity for emergency networks and many other positive ideas.

In 1999 Congress laid out a “Road Map” for Public Safety in the digital age. As the Chairman of the Senate Communications Subcommittee, I authored the e-911 bill, which thanks to the hard work and support of many of my colleagues such as Sen. Wyden, was passed into law. The e-911 bill did a couple of very important things, and recognized some important needs in regards to the activity here today: It made 9-1-1 the universal number for wireless phones. No matter where you are in America, 9-1-1 is THE number to connect to emergency responders via your wireless phone. Wireless knows no boundaries. Safety and security shouldn’t either.

The bill also called for statewide planning and coordination. America has over 60,000 emergency, law enforcement, or similar agencies. Simply put, we can’t go town by town, city by city to improve our emergency response system. There is a need to bring folks together, leverage investments and resources, cooperate with both the public and private sector to establish an infrastructure that improves emergency response.

In August of this past year, Montana did just that. Working closely with ComCARE, we put together a tremendously successful e-911 summit. The summit was attended by nearly 200 public safety officials, industry representatives and interested citizens from around the state who came together to discuss the challenges and opportunities facing emergency response. The focus of both the Montana 911 summit and today’s hearing is on how to utilize the tremendous advances being made in wireless technologies to make sure that our citizens have access to the best public safety network possible.

While the passage of the e-911 bill was a tremendous leap forward in the development of our nationwide emergency response capability, our work is far from finished. In fact, much remains to be done. While the carriers have made some progress on building out e-911, their efforts need to be expanded and accelerated. I was disappointed that they were not able to meet the initial deadline of October 1 of last year, which required them only to begin the process of providing automatic location identification for cellphones.

On February 1st of this year, the wireless carriers reported their e-911 deployment progress to the FCC. In those reports, two of the six major wireless operators—Verizon Wireless and Sprint—reported that they were on schedule. The other four carriers reported that they were not on schedule, and two of those asked for waivers of the waivers that the FCC gave them last year. While I understand that we are in the midst of challenging economic times in the communications sector, every effort must be made to build out these vital e-911 services.

Creating a 21st century, digital emergency communications network will require constant effort and oversight. I believe that hearings such as the one the Chairman is holding today are vital to this nation reaching its goal. As Americans we are facing some great challenges in not only improving our emergency response system but preparing for future unexpected acts of aggression. Addressing these issues together, in a unified approach, we have an opportunity to not only save an individual’s life, but enhance our ability to respond to events of any magnitude. Thank you, Mr. Chairman.

Senator INOUE. Without objection, so ordered.
Senator Wyden.

**STATEMENT OF HON. RON WYDEN,
U.S. SENATOR FROM OREGON**

Senator WYDEN. Thank you, Mr. Chairman. I will be very brief. I think it is particularly helpful that you are holding this hearing right now, Mr. Chairman, because I think this is a question of making sure that we not lose the momentum. There is clearly an opportunity to focus, and I am interested in working with you on the issues.

In addition, as I think people from New York know as well, I am going to be introducing legislation very shortly to create what amounts to the technology equivalent of the National Guard. We have found that there were a tremendous number of people in the private sector, in companies, for example, like Intel, that were willing to donate both personnel and equipment to try to help to deal with these problems. As the folks know from New York, there were some logistical problems in utilizing all that talent, simply because we had never faced a challenge of this magnitude. So I will have some questions when we get to that point, Mr. Chairman. But I so appreciate your leadership, because this is what it is going to take to keep the momentum alive and really get some results.

Senator INOUE. Thank you very much.

Mr. Souder, I am one of your constituents. I live in Montgomery County. So I thank you very much for the service there. It is yours now.

**STATEMENT OF STEVE SOUDER, DIRECTOR, MONTGOMERY
COUNTY, MARYLAND 9-1-1 EMERGENCY COMMUNICATIONS
CENTER**

Mr. SOUDER. Thank you, Mr. Chairman. I appreciate the opportunity to be here. Really, although I do work in Montgomery County, I was for the previous 16 years Director of the Arlington County, Virginia, 9-1-1 center, during the period of time of September 11th and really would like my testimony to be testimony that is brought to the Committee really from my public safety communications colleagues throughout the metropolitan Washington area who collectively worked together to mitigate the events of September 11th.

I am sure everyone in this room has indelibly etched in your mind where you were in that fateful hour between about 8:45 and 9:45 on September 11th. But I would ask the question, does anybody remember where they were 20 years prior to that on the afternoon of January 13th, 1982? Probably not. But for those that may recall, that was a snowy day in Washington, D.C., and there was an airplane on the runway at National Airport preparing to take off for a return flight to Tampa, Florida.

That was Air Florida Flight 90. It took off in the midst of a snowstorm that had blanketed the city and it was unsuccessful. It crashed onto the 14th Street Bridge, into the ice-clogged Potomac River, and all but five of the passengers aboard perished.

Because that event happened where it did, technically in Washington, D.C., less than 100 yards from the Virginia shoreline, and

coincidentally only one quarter mile from the Pentagon, the same group of first responders responded to that event that did the event at the Pentagon on September 11th—Arlington County, Alexandria, National Airport, Washington, D.C., Fairfax County, Montgomery County.

When they arrived, all of them well-meaning, none of them could talk to the other agency, because 20 years ago they were all operating on very divergent radio systems supported by various portions of the radio spectrum. It was literally a disaster within itself, because if you cannot communicate you cannot effectively operate.

In this very room after that event, there were hearings held about that event and the communications difficulties that were encountered were highlighted and discussed. We are pleased and you should be proud that because of those hearings the needs of public safety were addressed, addressed in the fact that the FCC opened up a portion of the radio spectrum heretofore unavailable to public safety, commonly today referred to as 800 megahertz. That 800 megahertz radio spectrum allowed the Washington, D.C., area to, as a result of the tragic events of January 13th, craft a plan, set a goal, for being better prepared to address whatever might befall this community in the future.

As a result of that, in over the past 20 years five major communities within the metropolitan Washington area have transitioned to 800 megahertz radio. By the end of this calendar year, three more major metropolitan area communities will do so. When combined to the communities that surround Baltimore, Maryland, we virtually have a seamless network of public safety first responders radio communications systems between north of Baltimore and south of Washington, D.C.

Consequently, on September 11th when the plane struck the Pentagon and the first responders responded they were able to do so in a far more effective fashion than had been the case 20 years prior to that. The communications was virtually seamless, flawless, and very effective. It was not perfect, but it certainly was very effective.

That is a result of long-term planning, consolidating your resources, sharing information with your neighbors, and having a design for really want you want to do. However, just like my colleague from New York mentioned, there were difficulties. There were challenges. To highlight but two of them—and the chair mentioned in his opening remarks about the impacts of wireless or cellular communications and these little things we call cell phones. There are about 160 million of them in the United States today and they tell me that every 24 hours another 7,000 subscribers sign on.

We public safety have become just as dependent upon them as has the general public and the business community. Surely one of the quick things that occurred on September 11th was cellular gridlock. Although we did have our radio systems, that is not to say it is the only way we communicate, and we could not communicate on cellular telephones. We were in gridlock.

So one of the things that I believe really needs to be looked at very clearly is what is loosely referred to as cellular priority access, but bringing that priority access down to the first responders level, with discipline, with organization, with priority, with a procedure

to follow. But clearly, we need to have access to those cellular telephones in the future.

Similarly, although the event went very well in the early hours of the event, by about mid-afternoon when many other assets arrived on the scene, assets that we do not normally communicate with, assets that were not, like ourselves, equipped with 800 megahertz radios, we could not communicate with them nor they communicate with us. We were fortunate in that we were able to develop a work-around because we had the good fortune of being able to draw upon a stock of excess radios and quickly programmed them and distributed them. But that took time and it took effort, critical time and critical effort.

So we really need, I believe, also to address the issue of how do we establish that interoperability, that word that very few of us uttered just a few short years ago and now is on everyone's tongue? How do we develop that interoperability between not only the first responders who respond every day across county and city borders to assist each other, but to make that interoperability available to the Federal assets, whether it is Defense Department, Justice Department, Treasury Department, or others, so that we can have the same level of interoperability communications with them as we do with our brothers and sisters in the fire and in the law enforcement service.

Although we have been very successful in Washington and are proud of it, the unfortunate thing is that less than ten miles from where we sit today one of our major suburban communities is not able to join in that network of commonality in radio systems because, although the FCC was gracious in allocating certain portions of the 800 megahertz radio spectrum and we have used it, I think, wisely and efficiently, unfortunately, because spectrum is a finite natural resource, at least locally we need more 800 megahertz so that we can bring into the fold, if you will, those other agencies, those other jurisdictions who cannot acquire that spectrum right now because it has all been exhausted.

I think one of the persons that will testify in the second portion of this hearing, Mr. Glen Nash from APCO, will speak to the Committee about that very issue and the importance of spectrum to public safety, because in the wireless age in which we all live and where it is the cell phone and the pager and the PDA and a host of other wireless devices, we are all competing for that finite natural resource that we call spectrum.

So it is very, very important that priorities be set, that the public's need can be recognized, but also that public safety's needs can be recognized also.

I, like my colleague from New York, thank you for the opportunity to testify.

Senator INOUE. Thank you very much, Mr. Souder.

If I may, I will begin the questioning. The events of that day soon became a matter of national concern. Everything from blood banks to security became a matter of national concern. How did your office coordinate with other State and Federal offices in order to provide relief for the city? Were you able to do that?

Mr. CANGEMI. Yes. What we had is a centralized Office of Emergency Management and, although it was destroyed in 7 World

Trade Center, we actually physically located along a pier, and at that location we had authorities from other States essentially set up cubicles with work stations, computers, Internet access, wireless access. Cell phones were distributed at the site; developed identification cards for security. But at that one centralized Office for Emergency Management, there were work stations for our various representatives from the Red Cross, the Salvation Army, not-for-profits that were providing assistance, State officials, other governmental officials.

Physical proximity I guess was the answer. Representatives from each of those organizations were able to physically kind of co-locate and that greatly helped.

Senator INOUE. I can understand the interoperability of the system in the greater Washington area, but did you have some sort of connection with other States other than Virginia and Maryland and Washington, D.C.?

Mr. SOUDER. Unfortunately, we did not. We were able to meet our immediate needs by simply calling upon the immediate resources that all three major jurisdictions in this area provide, namely the District of Columbia as the hub, Northern Virginia, and suburban Maryland. Those folks from Northern Virginia and from Maryland respectively went out to their State level emergency management personnel for the assistance that they needed.

Of course, we had the good fortune, because FEMA is located here in our community, that they were quick to respond and assist as well. But even FEMA and Virginia Emergency Management and Maryland Emergency Management, because they are on divergent radio systems, are not able to communicate effectively with those that have already been there and really are seeking their assistance.

Senator INOUE. If 9-11 should occur now, can you communicate with them now?

Mr. SOUDER. We could only do so in the manner that we did on the 11th, which would be by sharing with them, if we had available, excess radios so that they could communicate with us. The good fortune that we had on September 11th is because several of those communities that I mentioned earlier that are going to become 800 megahertz users by the end of this calendar year, the portable radios that their firefighters and EMT's and law enforcement personnel are going to eventually be issued were in fact in those communities in boxes, yet to be issued, yet to be programmed. So we had the good fortune of having more than a thousand portable radios, as you might say, in the closet.

We were able to retrieve those radios quickly, program those radios, charge the batteries for those radios, which all took time, but nevertheless we could quickly do it over the course of about 4 hours, and then virtually hand them or distribute them out to those people that were coming to assist us, like the State level, like the military, and like the Federal assets as well.

Senator INOUE. Obviously, the tragedy of 9-11 can occur in any other major city. Have you been able, both of you, to share your experience and knowledge with other places?

Mr. CANGEMI. Yes. I have actually made a similar presentation to the National Association of Public Utility Commissioners, so that

was addressed at the State level. Each of the 50 States were represented at that hearing. I made a presentation in Florida. I have been contacted by the Clark County-Las Vegas emergency management officials. A colleague of mine at my agency has also been in contact with many other municipalities.

I think they are all interested in our MARC, Mutual Aid and Restoration Consortium, model, our Emergency Management Command Center model, and are interested in perhaps replicating it at their local level as well.

Mr. SOUDER. I have also had that good fortune of being invited to speak at a number of conferences on these very same issues. Although nothing that we did in Washington, in the metropolitan Washington area, was terribly unique, but it was done with cooperation and collaboration. I think when we have explained to our colleagues across the Nation that was really the foundation of what we did, it has kind of opened their eyes to perhaps a new business model for doing local government where the sharing of resources and the planning collectively can really work for the good of not only one agency, but an entire region.

Senator INOUE. In your initial discussions with your colleagues throughout the land, were you convinced that they were ready?

Mr. SOUDER. I think "ready" is probably a relative term. They might be ready as they are doing business today, but I think when they have realized how dramatically our world has changed since September 11th and the fact that there are threats and possibilities out there that heretofore we had not given a lot of thought to, combined with the fact that when hearing the way other communities deal with things both routinely as well as in a disaster, it has provided an opportunity for some new thought to be given as to the way that business is conducted, particularly in public safety communications and the way in which communities and regions respond to both routine as well as a major disaster, yes.

Senator INOUE. Are you convinced that other communities are trying to improve their facilities?

Mr. CANGEMI. I think that the other communities are greatly interested. I have been actually fielding dozens of calls and have shared a copy of our Mutual Aid and Restoration Consortium agreement with a number of other municipalities. It is not something that they actually were familiar with. They had not even really contemplated having a consortium of competitors working as cooperatively as we had contemplated back in 1992. So perhaps it has some steam and will be able to be replicated.

Senator INOUE. I have a few other questions, but let me yield to Senator Burns.

Senator BURNS. Thank you, Mr. Chairman.

Mr. Souder, could you give me an idea of Montgomery County's infrastructure? Do you have one central communications center that you dispatch and receive calls?

Mr. SOUDER. That is correct. In the business that is commonly referred to as a PSAP, a public safety answering point. In Montgomery County, as well as in most of the other communities throughout the metropolitan Washington area, they are served by one communications center that serves the entire community as well as all of its public safety resources.

Senator BURNS. Now, whenever a call comes in, an emergency call comes in, say it comes in from a—say you have a residence on fire, just a fire call, an ordinary fire call. Does your fire department—each fire department in the county—and there are individual, I would imagine, jurisdictions—do they operate on the same frequency or different frequencies?

Mr. SOUDER. They all operate on the same common radio system, as well as the same common radio frequencies within that system. The assignment of a given frequency is done at the PSAP or the dispatch center, so that the command and control of that event is really controlled at the PSAP and each unit and each event is given its separate channel or frequency to talk on.

Senator BURNS. Is the same true with your police?

Mr. SOUDER. Yes, it is.

Senator BURNS. Now, tell me, in our PSAP or whatever, you receive a call, you call that policeman in that jurisdiction. Then can you monitor their conversation between them and their headquarters, and do you do that?

Mr. SOUDER. Yes, we can, and yes, we do. We would be their headquarters, so we would be able to monitor the conversations that were taking place both between the unit and headquarters as well as between units and units.

Senator BURNS. I am thinking of New York and redundant systems. You mentioned your redundant systems. Tell me about—you say now you are going to have broadband wired redundant systems. How about wireless?

Mr. CANGEMI. As far as wireless goes, from a local perspective we have not actually had that much kind of interaction with the wireless folks because we do not have regulatory authority over the wireless industry. But one of the plans—what we were able to deploy in New York was wireless 128K modem access. There is a company called Metrocom that actually is in bankruptcy. I wrote a letter to the bankruptcy court following September 11th, which allowed them to actually restart the company again, to the detriment of some of the creditors, but I found that they were understanding.

What we do is we have our light poles in New York City have antennas on the light poles. That is an extraordinarily fast means of communicating wirelessly. We were able to actually use that. We have plans to reinvigorate a similar system in New York going forward.

Senator BURNS. Voice and data?

Mr. CANGEMI. It is not currently set up for voice. It is just data right now. But I think it is possible to actually have some voice on the network as well.

Senator BURNS. Mr. Souder, have you ever asked your vendors if the police wanted to communicate with fire—let us say under the circumstances of a deployment of police handling security, fire trying to deal with their situation. Yet they cannot talk to each other by radio because both of them are operating on different frequencies. Have vendors ever come up with a radio device that will switch frequencies on the individual radio?

Mr. SOUDER. Well, within the 800 megahertz type of radio system that is in use in our metropolitan area and many other areas

of the country, those systems would allow for the law enforcement personnel to communicate with the fire and rescue personnel on an as-needed basis on the same system and, when necessary, on the same channel. So that really is one of the tremendous advantages that are associated with the 800 megahertz trunking technology.

Senator BURNS. Tell me, in order to bring you up to speed how much more spectrum do you think you require out there to really be effective?

Mr. SOUDER. The APCO organization which Mr. Nash will represent at the next portion of this hearing will speak to that. I think one of the problems is that the spectrum that has been allocated recently by the Commission, that is commonly referred to as that which used to be assigned to television channels, is spectrum that unfortunately will not under the best of circumstances be available to public safety until December 31st of 2006. That is only initially, and by nature of some formulas that are associated with how and when that spectrum in reality will be available, predicated upon the amount of digital televisions that are in service in a given particular geographical area will influence that.

So we really need that spectrum, I believe, much sooner than the 31st of December in the year 2006. We need it today. But even if we got it then, I am not sure that would be really meaningful, in that because of the passage of that date, if there has not been that transition to digital television, what is in theory ours cannot be ours until that 85 percent saturation point of digital televisions has taken place in a given market area.

Senator BURNS. Thank you, Mr. Chairman.

Senator INOUE. Thank you.

Senator WYDEN.

Senator WYDEN. Thank you, Mr. Chairman.

Let me begin with you if I can, Mr. Cangemi. Am I pronouncing that right?

Mr. CANGEMI. Yes.

Senator WYDEN. Great. I think your testimony is especially important because it seems to me, and sort of the attitude I bring to this is, that New York City is arguably the most sophisticated place on the planet from a communications standpoint and yet we had what amounts to a total meltdown for a period of time. I was struck at my hearing where one of the fire chiefs who responded to the problem said that at one point his only means of communicating directions to firefighters on the front lines was handwritten notes delivered by runners on foot. So for a period of time there was just a complete meltdown.

As I have studied what has gone on in New York, it seems to me you did a lot of things very well in terms of coming back. Now the question is sort of where do we go from here. That is what I want to ask you some questions about.

Let me begin in terms of this concept of trying to utilize the many people in the private sector who would like the help, the companies with people and equipment, and ask you whether you think it would be useful to have a preexisting database, a database that would be created now and would be in place and updated, so as to have an ongoing list of available private sector technology and

communications resources that you could call on if you were faced with another attack like September 11th?

Mr. CANGEMI. Absolutely. Many of the participants on the MARC calls were those kinds of companies, folks that did not have any obligation to be participating on our calls and all they wanted to do was help and make their resources available. Large telecommunications equipment companies provided donations of equipment, donations of trailers to bring up telecommunications as quickly as possible. To have a database like that would actually be extraordinarily helpful going forward.

Senator WYDEN. Good. That is one thing we will include.

One other aspect of this. You know, this country has got a strategic petroleum reserve in order to have a measure of protection against a calamitous situation with respect to oil. It seems to me I think we would be well served by having what amounts to a strategic technology reserve in effect. It could be a virtual technology reserve where companies could pledge equipment and resources again if there was a problem.

Would that be useful to you?

Mr. CANGEMI. Absolutely. We had our own reserves for Y2K planning and there was a certain amount of generosity on behalf of the companies in the days following September 11th. But from a global perspective I think that would be helpful nationally.

Senator WYDEN. Mr. Souder, do you agree? I gather you already have some reserves with respect to radios and that kind of thing and that strikes me as plenty useful. There is a lot of interest in that at home in Oregon even for things like fighting forest fires. But my sense is that the private companies would be willing to do a whole lot more, and I gather you would be sympathetic to something like that as well?

Mr. SOUDER. Absolutely. I think, in credit to them—and I know it occurred in New York and it certainly occurred in our area—is that the response by the private sector to the needs of the public sector could not have been better. It was good fortune, though. Not that it would not have come forward, but everything was lined up right, if you will. It was a beautiful day, kind of a fall day, clear skies, middle of the day. There were not a lot of the things that could impair that, if you will.

But that was good fortune. Picture it happening in Oregon in the middle of a snowstorm in the middle of the winter and it may not come together quite as smoothly as that. So to have the kind of structured database of resources available clearly would ensure that it could come together regardless of what the circumstances were.

Senator WYDEN. The next area I would like to explore with you is that the key to making this work is to ensure that it is first responder-friendly, that all of these resources from the private sector really help the first responders. The last thing people from Intel, say, want to do is basically stand around and get in the way when people in New York and D.C. are trying to respond to these kinds of things.

Do you have any thoughts or suggestions with respect to how to make sure that this is first responder-friendly and that these re-

sources from the private sector complement the kind of work that your people are doing, Mr. Cangemi?

Mr. CANGEMI. I agree. There had been a proceeding in front of the FCC regarding wireless priority and a Federal agency had actually tried to establish a wireless priority, kind of creating these super-cell phones that would in the event of an emergency have access and everyone else would kind of fall down the priority list. I was amazed that New York City first responders were not included on that.

Senator WYDEN. Were not included?

Mr. CANGEMI. Were not. We submitted comments describing how as first responders we were there in the days following the World Trade Center and it took approximately a week before we saw a presence at the Federal level in terms of FERC, those kind of emergency responders. So we think it is a great idea. We just want to make sure that kind of priority access gets in the hands of the first responders proportionately.

Senator WYDEN. Mr. Souder?

Mr. SOUDER. I would agree with that comment also. We have reached out to our six major wireless carriers in the metropolitan area, wanting to meet with them and see if we cannot orchestrate a system whereby, should an event of this magnitude occur in the future and we have cellular gridlock again, that notwithstanding the efforts of the Senate and the House and the FCC along these lines, that we would having a working partner in the form of the carriers, so that they could do whatever they could do internally to their systems to kind of address the problem, if you will.

Mr. CANGEMI. Just a follow-up. We have actually already addressed that with a company that wants to bring up the wireless data network in New York City and they have assured us that as far as the modems that New York City emergency workers would have, we would be able to have priority access. So that is critical to us.

Senator WYDEN. Did you bump up against any obstacles in taking donations? I have heard reports that there are some legal constraints in terms of what you can take because of a suggestion that somehow, in some way, someone would enrich themselves or something like that. I have heard of credentialing questions or people, for example, who came to New York City and had difficulty getting credentialed.

Again so I am clear on this, Mr. Cangemi, I think you all did a lot of things very, very well. This is not in any way supposed to be some broadside. To the contrary, the question is trying to think down the road a little bit to deal with these questions for the future. I would be interested in your response on that.

Mr. CANGEMI. I am sorry? As far as the donations?

Senator WYDEN. Any obstacles with respect to what you could take and how you could use it, your thoughts on the credentialing issue, that general area.

Mr. CANGEMI. Honestly, Senator, in the days following September 11th I kind of put my General Counsel hat down and acted as a Deputy Commissioner and tried to get the job done. We had an open kind of system, so that all the calls and the donations and those kinds of offers were being made with their competitors hear-

ing it, so it kind of allayed some of the fears I may have had if there were any accusations of favoritism as a result of that.

We had this open system. There were 40 of the largest telecommunications providers communicating at the same time, with the opportunity to assist equally. Any offers that made sense to us were accepted and that offer was available to everybody.

As far as credentialing, I leave that to the emergency management folks to answer. They were at first very hesitant to credential certain representatives. I was able to provide them with a list of our MARC, Mutual Aid Restoration Consortium, participants and their respective companies, and that helped with credentialing of at least the companies that participated in our conference calls.

Senator WYDEN. I know my time is up. Thank you, Mr. Chairman.

Senator INOUE. Senator Burns.

Senator BURNS. I have no other questions.

Senator INOUE. I would just like to ask one question. In every community there are radio stations and TV stations that have been designated for emergency signals. Did that system work on that day?

Mr. CANGEMI. Senator, I actually saw a news story in the New York Times about how that system was not deployed following September 11th, how there was kind of this actual—there were personnel, staffed 24 by 7, who were supposed to do that.

The main antenna that serves broadcast in New York City was on top of the World Trade Center. The folks who were only served by that antenna did not receive any kinds of television type motivation. As far as cable television goes, the system in place seemed somewhat antiquated because of the news coverage that existed on a multitude of channels. So while it was not employed, it did not seem as if there was a lack of information, at least to the customers in the New York City area that had web access or cable television access in the days following September 11th.

Senator INOUE. Mr. Souder?

Mr. SOUDER. Although I do not have direct knowledge of it, my understanding is that in this area the news media was very effective in broadcasting the events that were occurring at the Pentagon and some of the traffic issues that were associated with that. But I am not sure that the Emergency Broadcast System per se actually was activated, and my understanding is that is an issue that is being looked at this time.

Senator INOUE. Gentlemen, on behalf of the Committee I thank you very much.

Mr. SOUDER. Thank you very much.

Mr. CANGEMI. Thank you, sir.

Senator INOUE. Now may I call upon the Counsel of ComCARE Alliance, Mr. Christopher A. McLean; the President of the Association of Public Safety Communications Officials International, Mr. Glen Nash; the Group President for New York and Connecticut of Verizon, Mr. Paul Crotty; the Vice President of Operations, New York, New Jersey, and Connecticut, AT&T, Ms. Gloria Harris; and the Chairman, CEO, and President of Time Warner Telecom, Ms. Larissa Herda.

May I first call upon Mr. McLean.

**STATEMENT OF CHRISTOPHER A. McLEAN,
COUNSEL, COMCARE ALLIANCE**

Mr. McLEAN. Thank you. Thank you very much, Mr. Chairman. If I may be indulged in a point of personal privilege, I want to say as a former staffer to Senator Jim Exon, it is indeed a very deep personal and professional honor to appear before this Committee.

The ComCARE Alliance is a not-for-profit coalition of over 75 organizations in the medical, emergency response, telecommunications, transportation, and technology sectors, dedicated to advancing policy and technologies to improve emergency communications in individual and mass events.

The war on terrorism will be won or lost on information. Emergency responders on the front lines of homeland security need information to do their jobs. It is their most important tool. Every day we send first responders into harm's way without the information tools they need to save our lives or protect their own. Without change, the jobs of our heroic emergency responders will get even more difficult.

In general, the emergency communications network of America is voicecentric, with minimal data capabilities. Emergency calls are being dropped, operators are being overwhelmed, responses are delayed for lack of location information, communications systems can quickly become gridlocked, there is little ability to share data among multiple emergency response agencies or to communicate securely across jurisdictional and agency lines.

What is needed is a coordinated and integrated approach to upgrading all emergency communications, and this Committee gave a very good blueprint for that pathway in enacting the Wireless Communications and Public Safety Act of 1999.

The E-Safety program was developed with the help and guidance of experts in the field and was adopted by the ComCARE Alliance board of directors. Some of those experts include Jenny Henson from the State of Montana, the 9-1-1 administrator, and Gary Haycox of Intel from the State of Oregon.

The E-Safety program is designed to address the Nation's need in mass emergencies in a way that will significantly improve our ability to handle thousands of daily individual emergencies as well. The E-Safety program has eight essential elements:

Point one, we need to increase the capacity and reliability of America's communications network. Emergency response starts with a call for help from a citizen and every effort must be made to ensure that there is sufficient fixed and wireless bandwidth deployed to be able to handle call and data volume in times of emergency. Being connected saves lives. The availability of robust wireless, wireline, and satellite networks enhances public safety and security.

Point two, we need to deploy modern end-to-end emergency communications systems. Every emergency—every emergency agency should have at least one broadband connection and at least one intelligent work station.

Point number three, location technologies need to be deployed. Knowing the location of an emergency is critical to speeding response. If you were to make a call to 9-1-1 from your home phone in most parts of this country, the emergency responder would have

your street address on their screens in an instant and help can be dispatched even if you are unable to talk. They do not have that capability when you call from a large complex like the Capitol because the call goes through a PBX system, or from a wireless phone.

Where location is being deployed is in the car. Telematics leaders like Onstar and ATX are making Americans safer by delivering location safety products, and the Congress should encourage those types of activities.

Point number four, there needs to be support for State planning and deployment of integrated systems in model States. Leading States are ready to bring together all stakeholders, and grants should be made available to help create model deployments in these leading States. Places like Montana where Senator Burns chaired an E-Safety summit are ready to lead the way and to bring modern emergency communications tools to their everyday response to emergencies.

Point number five, we need to have two basic tools for all emergency agencies to move into the E-Safety realm: a national emergency electronic registry and event mapping capability. There is no comprehensive electronic directory of all emergency response and public health agencies, nor is there a directory of the type mentioned by Senator Wyden. The national nonprofit registry being developed by the ComCARE Alliance could help fill that gap.

We also need to encourage the broad use of shared electronic mapping of emergency event information. An emergency event web site could help solve the PSAP readiness riddle for enhanced 9-1-1 capabilities for wireless communications.

Point number six, we need to increase emergency response training. Wherever ComCARE goes we hear a common theme: Emergency response professionals want and need more training, and in times of emergency the public needs reliable information and instructions on how to move from danger to safety. Fortunately, America has a time-tested system to alert the public to weather dangers through the NOAA Weather Radio Network. Mr. Chairman, no one has done more for NOAA than you and the members of this Committee.

I am especially proud of my former agency, the Rural Utilities Service, for its leadership and efforts to close the NOAA Weather Radio gaps in rural America. What is needed now is for NOAA and the National Weather Service to continue and rapidly expedite their work to make the weather radio system a true all-hazards warning system.

Point number seven, we need to develop research and new safety applications. Congress should encourage major public and private efforts to develop critical civil defense and emergency applications which can use the basic E-Safety platform.

Point number eight, we need to support a national education and outreach effort. All the key members of the emergency response community, from first responders to 9-1-1 operators to the folks in the hospital and emergency rooms, need to be involved in understanding what together they can do with new technologies.

This is a very unique and important moment to form an integrated approach to emergency communications and response. That

approach was very clearly put forward by this Committee in the Wireless Communications Public Safety Act of 1999. Mr. Chairman, this Committee has done so much to advance emergency preparedness and response. The E-Safety program seeks to build on that solid record of success, and we welcome at the ComCARE Alliance the opportunity to work with the Committee to help make America safer.

Thank you very much, Mr. Chairman.

[The prepared statement of Mr. McLean follows:]

PREPARED STATEMENT OF CHRISTOPHER A. McLEAN, COUNSEL, COMCARE ALLIANCE

The E-Safety Program

Mr. Chairman and members of the Committee, I am Christopher A. McLean, counsel to the ComCARE Alliance. As a former staffer for Senator Jim Exon, it is a deep personal and professional honor to appear before this Committee.

ComCARE stands for Communications for Coordinated Assistance and Response to Emergencies. The ComCARE Alliance is a not-for-profit coalition of over 75 organizations in the medical, emergency response, telecommunications, transportation and technology sectors dedicated to advancing policy and technologies to improve emergency response in individual and mass events.

The ComCARE Alliance salutes all the American heroes in public safety who daily put their lives on the line for their communities as well as those who work with little recognition and fanfare to be the information bridges between those agencies, and between the public and public safety.

Our nation is engaged in a war unlike any other. In this war, America's greatest civil defense weapons are information and the ability to communicate.

The war on terrorism will be won or lost on information. It was one piece of information relayed to passengers in a plane over Pennsylvania on September 11th which brought heroic action to save the lives of many, many people in the nation's Capitol.

Police, fire, medical, public health and other emergency responders on the front lines of homeland security need information to do their jobs. It is their most important tool.

Indeed, every American has a role to play in making America safer. The vigilance of individual citizens and the emergency communications systems of the nation are valuable defensive weapons.

We would not send soldiers into battle without being well armed and well protected. Unfortunately, every day, we send first responders into harm's way without the information tools they need to save our lives and protect their own.

The emergency communications systems in many parts of the country are antiquated and, in some rural communities, they are struggling without even basic 9-1-1 systems.

Without change, the jobs of our heroic emergency responders get even more difficult.

In general, the emergency communications network is voice centric. It does not often utilize modern communications or information management tools which are so common now in industry. There are too often large disparities between the information capabilities of emergency agencies in the same jurisdiction, and between well funded urban and suburban communities and rural areas. Every day in large and small cities around the nation, emergency calls are being dropped, 9-1-1 operators are being overwhelmed with multiple calls, and responses are delayed for lack of location information. In mass emergencies, wireless and wireline communications systems can quickly become grid-locked. At the scene of an emergency, there is very little ability to share data among multiple emergency response and public health agencies, or to communicate securely across jurisdictional and agency lines in an emergency or in anticipation of an emergency.

What is needed is a coordinated and integrated approach to upgrading all emergency communications. We need to evolve current voice grade systems and civilian network capacity into modern, robust, networks capable of improving response to mass disasters and every day emergencies.

The ComCARE Alliance has been working in the field of emergency communications for more than four years. Immediately following the September 11th attacks, the Alliance convened a working group of our members to consider the lessons learned from September 11th and lay out an action agenda for a quick start pro-

gram to enhance our emergency communications infrastructure. The E-Safety Program is the result of those efforts. It was developed with the help and guidance of experts in the field and adopted by the ComCARE Alliance Board of Directors.

The E-Safety Program proposes to enhance homeland security by helping bring 21st century capabilities, commonly used in e-Business today, to emergency response, deploying integrated, interoperable and interconnected wireline and wireless systems and applications. The E-Safety program is designed to address the nation's need in a mass emergency in a way that will significantly improve our ability to handle thousands of daily individual emergencies as well.

The E-SAFETY PROGRAM has eight essential elements. In short, they are:

- Increase the Capacity and Reliability of America's Wired and Wireless Communications Networks;
- Deploy Modern End-to-End Emergency Communications Systems;
- Deploy Enhanced 9-1-1 for Wireline, Wireless and PBX; Deploy Telematics for automobiles;
- Support State Planning and Deployment of Integrated Emergency Communications Systems in Model States;
- Provide the two basic E-Safety tools to All Emergency Agencies:
- National Emergency Electronic Registry; and
- Event Mapping Capability.
- Augment and Increase Emergency Response Training;
- Make a Commitment to Research, Develop and Deploy New Safety Applications and Devices;
- Support National Education and Outreach, Bringing Together All the Key Emergency Stakeholder Communities

I am pleased to discuss the specifics of each.

Point 1. Increase the Capacity and Reliability of America's Communications Networks.

Every effort must be made to ensure that sufficient fixed and wireless bandwidth is deployed to handle call and data volume in times of emergency. Enhancing the capacity, capability and reliability of our nation's essential telecommunications networks should be a matter of national security.

Imagine if a citizen needed to communicate information about subsequent terrorist attacks at twelve noon of September 11th. In all likelihood, that call would not go through.

Today, the wireless phone has become an indispensable safety device. Consumers carry wireless phone for convenience of conversation, but most often, "just in case of an emergency." On September 11th and increasingly in day-to-day life, our wireless networks reach their capacity. Enhancing that capacity through sound spectrum policy, new technology and cell site policy will enhance public safety. We need to ensure that the wireless safety net stretches broadly and with as few holes as possible.

In the war on terrorism, it could be a vigilant citizen on a cell phone or in a telematics equipped vehicle who observes and reports a hijacked truck, suspicious activity at an airport, or terrorist or criminal activity. And similarly, we must provide sufficient spectrum for public safety agencies' own use.

Providing adequate spectrum and cell site locations to meet needs in times of mass emergency also works to ensure that the phone works in instances of a crime, a crash or a medical emergency. Being connected saves lives. Now more than ever, we cannot afford to let wireless dead zones become deadly zones.

All carriers should be encouraged to invest in their networks. The availability of robust wireless, wireline and satellite networks enhance public safety and security.

Point 2. Deploy Modern End-to-End Emergency Communications Systems.

We need to empower and tie all emergency response and public health agencies together with broadband connections and basic modern information technology. Every emergency response and public health agency such as police, fire, 9-1-1, hospital and health care facilities should have at least one broadband connection and one intelligent work station.

What worked on September 11th were broadband internet connections and wireless IP connections. Today many emergency responders do not have basic information infrastructure.

For example, one of our members, the American Public Health Association, reported that only about one half their members had broadband connections and about 10% did not even have e-mail.

High speed networks would connect responders to the tools of next generation emergency response such as a national emergency electronic directory, data sharing

systems, incident mapping, and other applications. Responders need the ability to send, receive and move real time emergency information among and between multiple agencies.

Point 3. Deploy Enhanced 9-1-1: Wireline, Wireless and PBX; Deploy Telematics

Knowing location is critical to emergency response. The most effective and efficient methods of Enhanced 9-1-1 deployment must be used, including overall state planning and organization. The deployment of telematics safety systems in cars should also be strongly encouraged.

If you were to make a call to 9-1-1 from your home phone, in most parts of this country, the emergency responder would have your street address their screen automatically. Help can be dispatched, even if you do not talk.

If you were to call from this room, the 9-1-1 reported address would be "Capitol complex." Location information speeds response. It is vitally important that the federal government, at least, ensure that its phones are locatable and encourage the private sector to work with emergency responders to find solutions. An excellent example of public/private partnership is in Washington State where Bob Oening, State 9-1-1 Administrator worked with Boeing to provide locations for phones on its vast Washington State network.

On the wireless side, today, wireless calls account for nearly 40% of 9-1-1 calls in some communities. Today, wireless phones are not locatable, although commercial technologies to do so are available. Make that same 9-1-1 call from your cell phone from the plaza in front of the Capitol, and the dispatcher will have no idea where you are. Indeed, the call could be answered in Virginia. This Committee has done a great deal to raise the profile of this important issue.

In the car, telematics is one of the most important safety features to be developed in recent years. By providing a hands free communications link, navigation, automatic crash notification and a mayday alert, powered by telecommunications and location technology, the telematics leaders in the auto industry are making Americans safer by delivering location and safety products. Those efforts should be encouraged.

Point 4. Support State Planning and Deployment of Integrated Systems in Model States.

Leading states are ready to bring together all stakeholders, plan sophisticated, integrated emergency and transportation communications and information systems, and then deploy them. New information technologies hold great promise in helping bridge the gap between urban and rural response capabilities.

Grants should be made available to create models of deployment in these leading states for other states to emulate, and to encourage state emergency communications planning.

This Committee understands well the importance of coordinated state, federal, local and private sector planning. Thanks to the leadership of members of this Committee, the Congress enacted legislation which includes the clear blueprint for action.

In enacting the Wireless Communications and Public Safety Act of 1999 (WiCAPs '99) the Congress called for a coordinated, end to end response to emergency communications planning.

Working together, communities are stronger than working separately. Several States have taken leadership role in beginning to give life to the vision of WiCAPs '99. ComCARE is proud to be working with these states to advance the vision of an integrated approach to emergency communications planning.

Just days before September 11, Senator Burns convened a historic public safety summit in Helena, Montana. The ComCARE Alliance was honored to participate. By bringing people together, and continuing a formal dialogue, participants are discovering that they have common needs, new opportunities to share and leverage resources and the support of the State's political leadership to get the job done. We look forward to continuing to work with the public safety community in Montana.

In Virginia, the Virginia Department of Transportation is funding a ground breaking effort in the Shenandoah Valley to create a 21st Century emergency communications capability. Thanks to the leadership of Congressmen Wolf, Goodlatte and Boucher the Shenandoah Valley is quickly becoming a test bed for new thinking in emergency communications.

In Washington State under the leadership of Senators Murray and Cantwell and with the support of the Washington State Center for the Digital Bridge, a Washington State E-Safety Summit is planned for this March 26th.

And in Oregon, Senator Wyden's Net Guard proposal has inspired the public safety and technology communities in Oregon to begin a dialogue on next generation response technologies.

Through these efforts, communities learn that they are not alone. They see opportunities to leverage existing funding sources and technology projects. The private sector discovers that there are innovation solutions for public/private partnership and resources well spent can solve multiple problems.

Point 5. Provide Two Basic Tools to All Emergency Agencies: National Emergency Electronic Registry and Event Mapping Capability.

There is no comprehensive, electronic directory of all emergency response and public health agencies. Therefore neither the President nor any other appropriate entity has the ability to send emergency warnings or data to all or some emergency responders or public information outlets in a particular area. The national non-profit registry being developed by ComCARE will fill that gap.

We also need to encourage broad use of shared electronic mapping of emergency event information. Emergency data and information can be sent to a shared map resource by emergency managers, telematics companies, wireless carriers, commercial transportation and others, and displayed/shared by all relevant emergency responders. These enabling technologies, combined with broadband connections to a safety network create a basic

E-Safety platform on which a wide variety of other safety applications can operate.

Point 6. Augment and Increase Emergency Response Training

New threats and new technologies require new training. There is a continuous need to ensure that new employees and volunteers are fully prepared for the challenges that face our nation. Fortunately, new communications technologies can make training more efficient. The same broadband platform for emergency response can be used for a host to digital training uses in times of peace and calm.

Where ever ComCARE goes, we hears a common theme. The hard working professionals in the emergency response field want more training. We especially need to share the lessons of September 11th and the anthrax attack.

The public also needs to be informed of their role in the war on terrorism. Public information is a vital government role.

In times of emergency, the public needs reliable information and instructions on how to move from danger to safety. Fortunately, America has a time tested system to alert the public to weather danger through NOAA weather radio network. The ComCARE Alliance applauds the Committee for its work and support for the NOAA all hazards warning network initiative. NOAA Weather Radio saves lives and it is the nation's largest most expansive radio network. It is an important backbone network for emergency warnings. I am especially proud of my former agency, the Rural Utilities Service for its leadership in efforts to close the NOAA weather radio gaps in rural America. In the Senate farm bill, the stage is being set to finish the job.

NOAA and the National Weather Service must continue and expedite its work to make the Weather Radio System a true all hazards warning system.

Point 7. Make a Commitment to Research, Develop and Deploy New Safety Applications and Devices

We must encourage major public and private efforts to develop critical civil defense and emergency applications which can use the basic E-Safety platform. This requires a significant university-based, emergency response research capability; rapid, industry-based open standards development efforts; and major public and private investments in new safety applications and devices.

Point 8. Support National Education and Outreach, Bringing Together All the Key Emergency Stakeholder Communities

We need to involve all the key members of the emergency response community in understanding—together—what is possible with the new technologies, and in planning, deploying and creating new operations protocols based on them. ComCARE and its non-profit membership associations like Emergency Nurses Association, National Emergency Number Association, American Public Health Association and the American College of Emergency Physicians should be given the resources to hold national, state and local conferences, and to run communications programs with agency and private sector partners, focused on best practices and new technologies. They are ready to step up to the plate and help bring emergency communications and response into the 21st Century.

To achieve the E-Safety program will require some new legislation and appropriations, but significant elements of the E-Safety program can be accomplished through a coordinated approach to existing programs and homeland security and through cooperation with the private sector. Billions of dollars have already been appropriated. The President has appointed a respected leader to head the Office of Homeland Se-

curity. This is a unique and important moment to forge an integrated approach to emergency communications and response. That approach was very clearly put forward by this Committee in WiCAPs '99. It is fully consistent with the Administration's approach to federalism and homeland defense. This is a moment and an opportunity which should not be lost.

Mr. Chairman, thank you again for inviting ComCARE to be represented at today's hearings. The individual members of this Committee and the Committee as a whole have done so much to advance emergency preparedness and response. The E-Safety program seeks to build on that solid record of success and we welcome the opportunity to work with the Committee to find ways to make America Safer.

Thank you Mr. Chairman.

Senator INOUE. Thank you very much, sir.
Then I will call on Mr. Nash. Mr. Nash.

**STATEMENT OF GLEN NASH, PRESIDENT, ASSOCIATION OF
PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-
INTERNATIONAL, INC.**

Mr. NASH. Thank you, Mr. Chairman. My name is Glen Nash. I am an engineer with over 29 years experience in the design of public safety communications systems and I am the President of the Association of Public-Safety Communications Officials-International, more commonly known as APCO.

APCO is the Nation's oldest and largest public safety communications organization. The majority of APCO's 15,000-plus members are State or local governmental employees who manage and operate the communications systems used by police, fire, emergency medical, disaster relief, and other public safety agencies.

The events of September 11th forced all of us to examine the vital role played by public safety agencies. These first responders literally are the front line troops, not only in the domestic war on terrorism, but also in the day to day reality of living in a less than perfect society.

To do their jobs effectively, public safety agencies need a variety of tools. At or near the top of the list of those tools lies effective radio communications. Public safety agencies use radio communications for command and control and to provide vital information and other resources that enable field personnel to do their jobs better. Additionally, effective communications between and amongst on-scene police officers, firefighters, EMS personnel, and other first responders is critical.

To achieve these goals, there are two intertwined communications issues that need to be addressed on behalf of our public safety agencies. First is spectrum capacity and second is interoperability. Public safety agencies in many areas face dangerous congestion on existing channels due to limited spectrum. This lack of spectrum also makes it impossible for many public safety agencies to implement the technologies that would make their field operations more effective. Furthermore, it impacts the ability of different agencies to communicate with each other, as they often are forced to operate on separate incompatible frequency bands.

In 1996 it was my pleasure to serve on the Public Safety Wireless Advisory Committee that documented the spectrum and interoperability problems. The Committee identified the need for 97.5 megahertz of new spectrum, including 25 megahertz needed within 5 years. Unfortunately, on September 11th, 2001, exactly 5 years

after the PSWAC report was released, no new spectrum had been made available nationwide for public safety use.

Yes, the 1997 Balanced Budget Act required the FCC to reallocate 24 megahertz of spectrum from television channels 60 to 69 for public safety use. The FCC has complied with that requirement by reallocating specific TV channels for public safety use in what is now called the 700 megahertz band. However, the act also stipulates that incumbent broadcasters can continue to operate in this band until December 31st, 2006, or until at least 85 percent of the households in the relevant market area have access to digital television, whichever is later.

That 85 percent provision creates uncertainty as to when the spectrum will ever become available. This makes it impossible for most State and local governments to plan, fund, or begin to design systems utilizing this new spectrum. Therefore, we urge Congress to establish a firm date for the availability of this spectrum for public safety use. We are joined in this effort by the International Association of Chiefs of Police, the International Association of Fire Chiefs, the National League of Cities, the National Association of Counties, and many other organizations who agree that Congress needs to revisit this issue.

While making the 700 megahertz band available for public safety use will help address the lack of adequate spectrum, it is not a panacea for resolving public safety's interoperability problem. Currently public safety agencies operate in ten different frequency bands, many of which are incompatible with each other. The obvious solution is to put all public safety agencies into a single radio band. However, no single block of radio spectrum has yet been identified which is capable of satisfying the entire public safety requirement for communications. Furthermore, moving all existing public safety users to a new band would impose tremendous costs upon State and local governments.

Therefore, we encourage Congress, the NTIA, and the FCC to consider making available frequency bands that are immediately adjacent to existing public safety spectrum allocations. As I discussed earlier, Congress attempted to do this in 1997 when it required the FCC to make available spectrum in the 700 megahertz band, which is immediately adjacent to existing public safety spectrum at 800 megahertz. However, this 700 megahertz spectrum is not currently available in many areas of the country. We need to have a firm date for the availability of this spectrum to support our Nation's police, fire, and emergency medical personnel.

Senator Burns, I would like to expand upon a question that you asked of Mr. Souder regarding whether agencies on different frequencies are able to talk with each other. The answer to that question really is it depends. First off, as I indicated earlier, public safety agencies operate on ten different frequency bands, many of which are incompatible with each other. In some areas of the country agencies have been able to congregate together, as they have done here in the Washington metro area, to operate in one of those bands or at least in immediately adjacent bands, which would allow for some compatibility. If this has occurred, it is technically possible for them to intercommunicate.

However, there is a second problem that comes into that. It involves the issue of prior planning and it really requires the agencies to have sat down prior to an event that they do not know is coming and they do not know the magnitude of what it is going to be and to have laid out a plan of how they would intercommunicate.

Over the years we have had many incidents that I have gone back at and looked at as an after-action report where the complaint has been made that the agencies were unable to communicate with each other. As we have looked at their radios, they in fact had common radio channels. They were able to communicate. They just did not know it. They had not done the preplanning that they really needed to do and, as Mr. Souder indicated, a critical part of this is for the agencies involved to get together and discuss how they would intercommunicate and what they would do when the event happens that they do not expect.

If, on the other hand, they are operating on totally different frequency bands, technically it is not technically possible for them to intercommunicate, at least directly over the radio, and we have to work at developing other plans and alternatives. That really becomes the problem even if we develop regional coordination systems, as was done in the D.C. metro area here. As the event grows and we reach further and further out for assistance, we are bringing in people who are not a part of that original plan and it becomes more likely that they are operating in a different frequency band and therefore will be unable to communicate directly when they arrive on scene.

With that, in closing I want to thank you, Mr. Chairman and the Members of the Subcommittee, for conducting these important hearings and for providing me an opportunity to discuss the critical communications problems facing public safety agencies in these difficult times. APCO stands ready to work with Congress, the FCC, and other interested parties in resolving these issues as quickly and as efficiently as possible.

[The prepared statement of Mr. Nash follows:]

PREPARED STATEMENT OF GLEN NASH, PRESIDENT, ASSOCIATION OF PUBLIC-SAFETY COMMUNICATIONS OFFICIALS-INTERNATIONAL, INC.

Thank you, Mr. Chairman

My name is Glen Nash. I am the President of the Association of Public-Safety Communications Officials-International, Inc. (APCO), and I am here today on APCO's behalf. I have over 29 years experience in the design, installation and maintenance of public safety communications systems and currently serve as Senior Telecommunications Engineer with the State of California Department of General Services. Please note, however, that I am here today on APCO's behalf, and not in any official capacity for the State of California. I also currently serve as Chair of the Technology Subcommittee of the FCC's Public Safety National Coordination Committee (NCC), and I was an active participant in the joint FCC/NTIA Public Safety Wireless Advisory Committee (PSWAC).

APCO, founded in 1935, is the nation's oldest and largest public safety communications organization. APCO has over 15,000 members, most of whom are state or local government employees who manage or operate communications systems for police, fire, emergency medical, disaster relief, and other public safety agencies. APCO is certified by the FCC as a frequency coordinator for public safety mobile radio channels, and has long played a major role in public safety radio spectrum and wireless E9-1-1 issues before the Commission.

The events of September 11 have forced all of us to re-examine our nation's priorities, especially those related to our police, fire, EMS and other agencies charged

with the protection of life, health, and property. These “first responders” literally are the frontline troops not only in the domestic war on terrorism, but also in the day-to-day reality of living in a less than perfect society.

Today, more than ever, our nation’s public safety agencies must have the tools they need to perform their critical tasks. Communications is at or near the top of the list of those essential tools. Public safety communications, in turn, depends upon an adequate supply of appropriate radio spectrum dedicated for public safety use.

Public safety agencies use radio communications not only to dispatch personnel to the scene of an incident, but also as a link between field personnel and a resource center so that they can request additional assistance and/or information to properly handle the incident. Of particular importance is on-scene portable radio communication between various public safety personnel responding at the scene of a crime-in-progress, fire, flood, explosion, vehicle accident, or other emergency. This is true whether we are talking about the events such as those of September 11; emergencies associated with floods, earthquakes and weather-related emergencies; or day-to-day responses to crime, fire, accidents and medical emergencies. Now, with new Homeland Security responsibilities being placed upon state and local public safety agencies, the need for effective radio communications is heightened even more.

Unfortunately, for far too many years, public safety agencies across the nation have faced a severe shortage of radio spectrum available for their communications systems. These shortages were documented in 1996 by the Public Safety Wireless Advisory Committee (PSWAC), a blue-ribbon committee created by NTIA and the FCC. The PSWAC Report, which was adopted on September 11, 1996, determined that public safety users would require an additional 97.5 MHz of radio spectrum by 2010, and would need approximately 24 MHz within five years of the Report. Unfortunately, exactly five years later, on September 11, 2001, that 24 MHz was still not available for nationwide public safety use, for reasons that I will discuss in a moment.

The lack of sufficient radio spectrum for public safety has several significant consequences. In many metropolitan and other densely populated areas, public safety agencies face dangerous congestion on their radio systems. In some instances, public safety agencies operate with hundreds of users per channel, far more than is safe under “normal” day-to-day circumstances, let alone major emergencies. Demand for channel capacity has been increasing with population growth and density. Now, with new Homeland Security responsibilities being placed on public safety personnel, there will be even greater demand for public safety spectrum.

Inadequate spectrum also prevents public safety agencies from implementing new communications tools, such as wide area mobile data systems that can provide law enforcement officers, firefighters, and EMS technicians with a wealth of critical on-scene data. This includes not only high speed text delivery (such as criminal background information), but also, with sufficient spectrum, high resolution images such as mug shots, fingerprints, and building diagrams. While the FCC recently allocated spectrum in the 4.9 GHz band for certain public safety data and video functions, use of that band will be limited to relatively short distance transmissions. The 4.9 GHz band is not expected to provide a spectrum home for wide-area, mobile data systems.

The lack of spectrum also has a direct and significant impact on interoperability. All too often, public safety personnel from different agencies responding to the same emergency cannot communicate with each other, because they operate on incompatible, non-interoperable radio systems. The lack of interoperability is generally the result of different agencies being forced to operate on different radio frequency bands. The most effective way to address that problem is to migrate agencies in the same geographic area to common, or at least compatible, radio frequency bands. Unfortunately, that’s not possible in many areas as there is not enough spectrum in any one band to accommodate all, or even most, of the public safety users in the region. New allocations, especially if adjacent to an existing public safety spectrum allocation, would greatly enhance interoperability with existing users, while at the same time providing capacity for new, multi-agency, multi-jurisdictional radio operations.

Congress tried to address some of these issues in 1997, when it required the FCC to allocate 24 MHz of spectrum for public safety purposes from the 746–806 MHz band (TV channel 60–69). This was consistent with the 1996 recommendations of the Public Safety Wireless Advisory Committee. The FCC then did its part. It reallocated TV channels 63, 64, 68, and 69, for public safety and adopted rules to promote interoperability among all users of the band and the adjacent 800 MHz public safety bands. Indeed, the Commission allocated approximately 10% of the new band for nationwide public safety interoperability, and required that all radios in the new band

be capable of operating on the interoperability channels. The Commission also adopted a digital interoperability standard (Project 25) for the band, to ensure that digital equipment from different manufactures would still be interoperable.

However, in most of the nation's largest metropolitan areas, the new spectrum allocated for public safety was not available on September 11, and will not be available until TV broadcasters on channels 63, 64, 68, and 69 (and in many cases the adjacent channels), release those channels as part of the digital television (DTV) transition. The problem facing public safety is not only that the spectrum is not currently available nationwide, but also that there is no firm date for when the spectrum will become available. The 1997 Balanced Budget Act, which required the FCC to allocate spectrum for public safety, allows incumbent broadcasters to continue operation on TV channels 60–69 until December 31, 2006, *or* until some uncertain, future date when at least 85% of the households in the relevant market have access to DTV signals.

That 85% provision creates uncertainty as to when (or if) the spectrum will become available, and makes it impossible for most state and local governments to plan, fund, or construct systems using the spectrum allocated for their public safety operations. For example, the State of California has a tremendous need to upgrade the radio systems for its own agencies, but we cannot build a statewide system that does not include the Los Angeles and San Francisco Bay areas. Unfortunately, those are among the metropolitan areas where TV stations block use of the newly allocated public safety spectrum. Many other large public safety agencies across the country face the same dilemma.

APCO has therefore joined with the International Association of Chiefs of Police, the International Association of Fire Chiefs, the National League of Cities, the National Association of Counties, the U.S. Conference of Mayors, and other organizations to urge that Congress establish an early and firm date for the newly allocated public safety spectrum to become available for actual operations.

There are also important steps that the FCC needs to take. For example, we remain deeply concerned about the rules adopted to protect future public safety users of the new spectrum from interference caused by new commercial mobile radio services in the same band. These are commercial users who would receive licenses pursuant to the 700 MHz band auctions currently scheduled by the FCC. We do not believe that the interference provisions are adequate, based upon studies conducted by the Telecommunications Industry Association, and have petitioned the FCC to reconsider its rules.

The interference that we fear in the 700 MHz band is similar in some respects to current interference problems that many public safety agencies already face in the nearby 800 MHz band. The FCC is about to initiate a proceeding on that issue, which includes a proposal that would also provide additional spectrum relief for public safety agencies in that band.

Finally, I want to note that many public safety agencies will continue to operate in the UHF (450–470 MHz, plus, in some areas, portions of 470–512 MHz) and the VHF High Band (150–170 MHz) for the foreseeable future. Indeed, due to the low cost of equipment and good propagation characteristics, the VHF High Band is the most heavily used public safety frequency band. However, that band is extremely overcrowded and is in desperate need of “breathing” room to relieve congestion and facilitate wide-area interoperability plans. In that regard, we were pleased that Congress required the Department of Defense to study the potential for sharing of its nearby 138–144 MHz band, which we understand is lightly used in at least some portions of the nation. DOD has submitted a classified study to the Congress on this issue, and we look forward to learning more about the results of that study, and moving as quickly as possible towards actual sharing of the band with state and local government public safety agencies wherever feasible.

In closing, I want to thank you Mr. Chairman and members of your Subcommittee for conducting these important hearings, and for providing me an opportunity to discuss the critical communications problems facing public safety agencies in these difficult times. APCO stands ready to work with the Congress, the FCC, and other interested parties in resolving these issues as quickly and efficiently as possible.

Senator INOUE. Thank you very much, Mr. Nash.
May I now recognize Mr. Crotty.

STATEMENT OF PAUL CROTTY, GROUP PRESIDENT FOR NEW YORK AND CONNECTICUT, VERIZON, INC.

Mr. CROTTY. Thank you, Mr. Chairman, Senator Burns.

My name is Paul Crotty. I am Verizon's Group President, New York and Connecticut, and I am pleased to be here today to discuss our experiences after the terrorist attack in September.

On September 11th I stood at the corner of Veasey and West Street amidst the debris of 1 and 2 World Trade Center, which had collapsed by 10:00 o'clock in the morning. I saw our brave firefighters, police officers, and emergency medical technicians carrying on heroically amid utter destruction. I thought of our 1600 employees at 140 West Street and 500 employees at 2 World Trade Center and prayed that they had escaped. We lost two employees at the World Trade Center plus another employee at the Pentagon.

As horrific as that scene was, Verizon's building at 140 West Street was still functioning. What happened at 5:00 p.m. changed that. 7 World Trade Center twisted on its frame and collapsed, and as it fell number 7 ripped out a large portion of the east-facing wall of our building and then collapsed into our cable vault.

Our outside plant in Manhattan is below ground and in lower Manhattan "below ground" means below sea level. The pulverized cement and fiberglass dirt and other airborne debris blew into our equipment floors, covering our sophisticated electronic equipment with up to five inches of soot-like material. 7 World Trade Center's collapse into and through our cable vault cut up our outside cable plant like so many strings of spaghetti.

Our sub-basements were flooded by ruptured water mains. Even after the water mains were secured, our basements continued to flood with the runoff from water used to fight the fire at 7 World Trade Center, which burned steadily for 2 weeks and intermittently for another 6 weeks after that.

We have now restored service in lower Manhattan. We are in the process of replacing equipment at 140 West Street and rebuilding our outside plant.

I have already mentioned our brave uniformed forces, but I would be remiss if I did not also say something about Mayor Giuliani and Governor Pataki. They were both outstanding in every way. Their presence and quiet leadership kept us going. They confronted danger and uncertainty with a calming and reassuring strength.

Mr. Chairman, I appreciate your visit and the visit of other members of your Committee. It was very important to keep the spirits up and to keep us involved knowing that our efforts at Ground Zero were supported by the ranking members of the Congress and indeed by all citizens of the United States.

Our building at 140 West Street contained four switches which had the capacity to serve a city the size of Cincinnati. The damage to our building was severe. Altogether we lost ten cellular towers along with 300,000 voice lines and 3.6 million data circuits affecting 14,000 businesses and 20,000 residential customers.

Although this was a disaster at a particular point in our network, the network itself continued to function. Many customers reacted to the tragedy by telephoning their families to let loved ones know they were safe. That made call volumes spike up to 100 percent higher than on a normal day for both wireless and wireline telephones. We worked with other carriers and we processed these volumes.

Verizon had the process and people in place to deal with the restoration job of this magnitude. We approached this in an organized fashion. Our first priority was to restore service immediately for emergency services—police, fire, medical, governmental agencies. To accomplish this, we harnessed our emergency preparation planning, we quickly mobilized a team and set our plan in motion. We were able to take advantage of redundancy that was built into the network to accomplish immediate restoration of critical functions.

Mr. Cangemi has already mentioned the Office of Emergency Management, which moved. It had its office at 7 World Trade Center. When 7 World Trade Center collapsed, it was relocated first to the police academy and then to Pier 92 on the west side of Manhattan.

Within 36 hours we had installed over 500 voice lines in 15 T-1's, so that when the Mayor put the Emergency Management Center back in operation it had representatives from every city, State and Federal agency that was involved in responding to the disaster, along with other agencies such as the Red Cross and Salvation Army not-for-profits, which were also emergency responders.

The city's 9-1-1 system had designed redundancy and automatic backup. It never failed. Not a single call was missed on September 11th. In addition, our optical network rerouted 90,000 data circuits immediately.

Our second priority was to do the work necessary for the New York Stock Exchange and the Mercantile Exchange to reopen on September 17. In the weeks following we restored the American Stock Exchange. When the New York Stock Exchange opened on Monday, September 17, it handled over 2 billion shares, a record number.

To make this happen we had to do a number of things. First of all, as I indicated, Con Edison lost power. 7 World Trade Center also contained two sub-stations for Con Edison, and when 7 World Trade Center collapsed we lost power throughout lower Manhattan. Therefore the power for our Broad Street station was provided by standby diesel power for a period of up to 12 days.

Verizon also rerouted or rebuilt high-capacity data circuits that passed through West Street. We provisioned 1.5 million lines and 2 million data circuits in 6 days and we ported more than 150,000 telephone numbers that had been assigned to our equipment in West Street facilities to equipment in other locations. We acted as systems integrators and project leader for coordinating efforts of suppliers, other carriers, major stock exchange and Security Industry Automation Corporation customers. We again would like to publicly thank the many carriers and equipment makers who went out of their way to share resources in that time of crisis.

I also want to mention the extra work of Verizon's men and women, what worked 24 hours a day, 7 days a week, for months at a time. One of our major problems with our work force was convincing them that they had to go home at the end of the shift. We had tremendous cooperation from our collective bargaining representative, the Communications Workers of America.

The end result was that Verizon got a huge amount of capacity to many customers and got it there quickly.

Our third priority was to restore services to all affected residential and business customers. Wireless technology played an important part in that story. We deployed seven “cells on wheels” and 16 temporary cell sites almost immediately after September 11th. That allowed us to replace wireless service that was disrupted by damaged cell sites. Within 1 week we had 150 percent of the capacity in lower Manhattan that we had on September 10th.

We provided customers with alternatives to their regular service through mega-call forwarding. We made our 4,000 pay phones on the streets of Manhattan free for over a week and we brought in extra pay phones which provided free pay phone service in the affected area in lower Manhattan. We provided over 5,000 wireless phones for small business customers. We provided the Secret Service and other Federal agencies with wireless devices to help offset equipment loss when their offices in the World Trade Center were destroyed.

Our business solutions group visited 900 small businesses a day and our emergency office in New York City’s business recovery center was taking orders from 400 walk-in customers a day. We worked one on one with large business customers, including our wholesale customers, and with 40 carriers which connected through Verizon’s facilities, to help them restore services. We opened a special office in Chinatown to help residence customers.

The good news is that we were able to get our customers back into service quickly, in many cases through gerry-rigged arrangements. Much of this work will have to be redone now as debris is cleared from manholes and we can get into our underground facilities.

While this was going on in New York, we had the similar attack at the Pentagon. We also had major efforts there. At the Pentagon we had about 40 people who operate the communications system pursuant to a contract with the Federal Government, a system that never went down, not even for a minute. The people there were not evacuated as the situation did not warrant it, and in fact two of our employees, by reporting to the Defense Secretary’s office on the position of the fire relative to a critical telecommunications switch, were responsible for saving it. We set up mobile wireless cell sites in Arlington.

Finally, at the plane crash site in western Pennsylvania we provided the additional wireline and wireless capacity needed by the emergency response personnel at that site.

As to lessons learned, what did we learn from all this? Well, first we learned about the resiliency of our telephone network, Verizon’s and those of other provider. They all proved their worth. While call volume spikes caused temporary difficulties, by the close of business on September 11th those difficulties were largely under control. Diversity of routes, redundancy of facilities, and experience with recoveries were keys to putting the right resources at the right place to resolve a very complex problem.

The economy remains the biggest uncertainty in the aftermath of September 11th. We were already feeling the effects of the economic slowdown before this. We need to look for prudent ways to stimulate investment, innovation, and consumer confidence. This is

particularly so in lower Manhattan. We are rebuilding our network and we must have users to make our investment worthwhile.

We also came away from September 11th and the recovery efforts with new clarity on the larger issues facing the communications industry. First, true competition comes from diverse technologies, whether it is wireline, wireless, cable, or the Internet. With regard to telecommunications, facilities-based competition demonstrated that it is the real competitive alternative, not resale of pieces of the existing network.

The fact the service restoration in lower Manhattan occurred as quickly as it did demonstrates the value of large-scale facilities-based local networks. Scale and scope matter. Verizon's ability to draw on the resources of a national company was invaluable. The value of large facilities-based competitors is evident. They tend to have the scale and experience to help the Nation recover quickly.

Fiber, broadband, and diverse technology are crucial because they improve survivability. Fiber and broadband to large business customers works and has never been more important. Also, fast Internet access was vital to consumers. Broadband service to the home helped keep America connected and productive. In the crisis people were able to choose from several technologies to handle their communications. If wireless did not work, often email and Instant Messaging did, and if wireline did not work then often wireless would. When it was impossible for people to drive to their place of work, they could telecommunicate over broadband networks. New high-speed information technology—our national strength.

With regard to security issues, Verizon gets plenty of practice in system recovery efforts. We have more than 1,000 recovery efforts every year of various scale, manmade and natural, from airplane crashes to ice storms, major floods, hurricanes, and tornadoes, to trucks hitting telephone poles and people digging up and cutting our underground plant. Our experience with these situations helped make the September 11th recovery run effectively.

But we had never experienced anything like this, which seemed to be a witch's brew of every disaster known and unknown, and they occurred in three separate places simultaneously.

What have we learned? There are two major lessons. First, we need to take a fresh look at security of telecommunications networks, and we are already well along with that process.

Second, the country needs to develop national policies related to access to critical network assets, cybersecurity, and the redundancy and diversity of networks. At Verizon we have a regular aggressive schedule of security audits and continual discussions with the security community about new threats. These practices have been the cornerstone of our regular cycle of security improvement and testing.

We share information with and work closely with the national security and emergency preparedness agencies at the Federal, State, and local levels. We have complied with the FCC's telecommunications service priority guidelines. Agencies such as New York City's Mutual Aid and Restoration Consortium, the FBI's National Information Protection Center, the National Communications System, and the National Security Telecommunications Advisory Committee are illustrative of the agencies that we work with. Many of

those discussions are very candid and involve vulnerability assessments and plans.

Of course, we continue to work with both the FCC and our New York State regulatory agency, the Public Service Commission.

Since September 11th Verizon has additional efforts under way to further improve the security, survivability, and rapid recovery of our networks. We have undertaken a review of which assets need additional hardening. That means a physical inventory of our 5100 central offices and hundreds of key buildings, with rankings for significance and thus priority attention for hardening. Mostly this means beefing up physical security, such as perimeter and entryway, some better monitoring, in a few cases interior partitioning.

We have heightened attention to prevent and discover unauthorized cyber-intrusion. We caught and were the first to report a major computer virus to the National Information Protection Center right after September 11th. We continue our regular security audits that Verizon conducted even before September 11th and we promptly address any findings of noncompliance or design weakness.

I thank the Committee and you, Mr. Chairman, for your attention to critical infrastructure matters, and I will try to answer any questions you may have further along in the program. Thank you.

[The prepared statement of Mr. Crotty follows:]

PREPARED STATEMENT OF PAUL CROTTY, GROUP PRESIDENT FOR NEW YORK AND CONNECTICUT VERIZON, INC.

Mr. Chairman, my name is Paul Crotty, and I am Group President New York/Connecticut. I am pleased to be here today to discuss our experiences after the terrorist attack in September.

On September 11, I stood at the corner of Vesey and West amidst the debris of 1 and 2 World Trade Center which had collapsed by 10 am. I saw our braver fire fighters and police officers and emergency medical technicians carrying on heroically amid utter devastation. I thought of our 1600 employees at 140 West Street and 500 employees at 2 World Trade Center and prayed that they had escaped. We lost 2 employees at the World Trade Center, plus another employee at the Pentagon.

As horrific as that scene was, Verizon's building at 140 West St. was still functioning. What happened at 5pm changed that. 7 World Trade Center* twisted on its frame and collapsed. As it fell, it ripped out large portions of the east facing wall and then collapsed into our cable vault. Our outside plant in Manhattan is below ground and in lower Manhattan, below ground means below sea level. The pulverized cement and fiberglass, dirt and other airborne debris blew onto our equipment floors covering our sophisticated electronic equipment with up to 5 inches of soot-like material. And 7 World Trade Center's collapse into and through our cable vaults cut up our outside plant like so many strings of spaghetti.

Our sub basements were flooded by ruptured water mains. Even after the water mains were secured, our basements continued to flood with the run off from the water used to fight the fire at 7 World Trade Center which burned steadily for 2 weeks and intermittently for another 6 weeks after that.

I have mentioned our brave uniformed faces. I would be remiss if I did not also say something about Mayor Giuliani and Governor Pataki. They were both outstanding in every way. Their presence and quiet leadership kept us going. They confronted danger and uncertainty with a calming and reassuring strength.

Synopsis of Events

Lower Manhattan. Our building at 140 West Street contained 4 switches which had the capacity to serve a city the size of Cincinnati. The damage to our building

*7 World Trade Center also housed 2 Con Edison substations. When the substations were lost, lower Manhattan lost its power. Even today, lower Manhattan is powered by a 13,000 volt "extension cord" which runs on the sidewalks and streets of lower Manhattan.

was severe. Altogether, we lost ten cellular towers, along with 300,000 voice lines and 3.6 million data circuits—affecting 14,000 businesses and 20,000 residential customers.

Although this was a disaster at a particular point in our network, the network itself continued to function. Many customers reacted to the tragedy by telephoning their families, to let loved ones know they were safe. That made call volumes spike 100% higher than a normal day, for both wireless and wireline telephones. We worked with other carriers and processed these volumes. Verizon had the process and people in place to deal with restoration job of this magnitude. We approached it in organized focused way:

Our first priority was to restore service immediately for emergency services—police, fire, medical, government agencies. To accomplish this, we harnessed our emergency preparation planning—we quickly mobilized a team and set our plan in motion. We were able to take advantage of redundancy that was built into the network to accomplish immediate restoration of critical functions.

The City's 911 system, which had designed redundancy and automatic backup never failed—not a single call was missed. In addition, our optical network re-routed 90,000 data circuits immediately.

Our second priority was to do the work necessary for the New York Stock Exchange and the Mercantile Exchange to reopen on September 17. In the weeks following, we restored the American Stock Exchange. When the NY Stock Exchange opened, it handled over 2 billion shares, a record number. To make that happen:

- As I indicated Con Ed lost power and we operated on standby diesel power for 12 days at our Broad Street facility.
- Verizon rerouted or rebuilt high capacity data circuits that passed through West Street.
- Verizon provisioned 1.5 million lines and 2 million data circuits in six days.
- We ported more than 150,000 telephone numbers that had been assigned to equipment in our West Street facility to equipment in other locations and
- We acted as systems integrator and project leader for coordinating efforts of suppliers, other carriers and major NYSE and Securities Industry Automation Corporation (“SAIC”) customers. We again publicly thank the many carriers and equipment makers who went out of their way to share resources in that time of crisis.

The end result was that Verizon got a huge amount of capacity to many customers—and got it to them quickly.

Our third priority was to restore service to all affected residential and business customers. Wireless technology played an important part in that story

We deployed seven “cells on wheels” and 16 temporary cell sites almost immediately on 9/11. This allowed us to replace wireless service that was disrupted by damaged cell sites. Within one week we had 150% of the capacity in Lower Manhattan we had on September 10.

We provided customers with alternatives to their regular service through mega call forwarding, 4000 free payphones and 5000 wireless phones for small business customers. We provided the Secret Service with 300 wireless devices to help offset equipment lost when their office in the World Trade Center was destroyed. Our Business Solutions Group was visiting 900 small businesses a day, and our emergency office in NYC's Business Recovery Center was taking orders from 400 walk in business customers a day. We worked one-on-one with large business customers, including our wholesale customers and with 40 other carriers which connect through Verizon facilities to help them restore services. And we opened a special office in Chinatown to help residence customers.

The good news is that we were able to get our customers back into service quickly—in many cases, through jerry-rigged arrangements. Much of this work will have to be re-done as debris is cleared from manholes and we can get to underground facilities.

Pentagon. While all this was going on in New York, there were also major efforts in Northern Virginia. At the Pentagon, we had about 40 people who operate the communications system—a system, by the way, that never went down, not even for a minute. The people there were not evacuated, as the situation didn't warrant it; and in fact, two of our employees, by reporting to the Defense Secretary's office on the position of the fire relative to a crucial telecommunications switch, were responsible for saving it. Verizon provides service to the Department of Defense under WITS 2001 contract.

We set up mobile wireless cell sites in Arlington. Finally at the plane crash site in Western Pennsylvania we provided the additional wireline and wireless capacity needed by emergency response personnel at those sites.

Lessons Learned

What did we learn from all this?

First, the resiliency of telephone networks—Verizon’s and those of other providers—proved their worth. While call volume spikes caused transitory difficulties, by close of business on September 11, those difficulties were largely under control. Diversity of routes, redundancy of facilities and experience with recoveries were the key to putting the right resources at the right places in a complex problem.

The economy remains the biggest uncertainty in the aftermath of Sept. 11. We were already feeling effects of economic slowdown before this. We need to look for prudent ways to stimulate investment, innovation and consumer confidence. This is particularly so in lower Manhattan. We are rebuilding our network and we must have users to make our investment worthwhile.

We also came away from 9/11 and the recovery efforts with new clarity on larger issues facing the communications industry.

True competition comes from diverse technologies (wired, wireless, cable, Internet). With regard to telecommunications, facilities based competition demonstrated that it is the real competitive alternative, not re-sale of pieces of an existing network. The fact that service restoration in lower Manhattan occurred as quickly as it did demonstrates the value of large- scale facilities-based local networks.

Scale and scope matter. Verizon’s ability to draw on resources of a national company was invaluable. The value of large facilities- based competitors is evident—they tend to have the scale and experience to help the nation recovery quickly.

Fiber, broadband, and diverse technology are crucial because they improve survivability. Fiber/broadband to large business customerworks and has never been more important. Also, fast Internet access was vital to consumers; broadband service to the home helped keep America connected and productive. In the crisis, people were able to choose from several technologies to handle their communications—if wireless didn’t work, often e-mail and Instant Messaging did, if wireline didn’t work, often wireless did. When it was impossible for people to drive to their place of work, they could telecommute over broadband. New, high speed communications technologies are a national strength.

Security Issues

Verizon gets plenty of practice in system recovery efforts. We have more than 1000 recovery efforts every year of various scales man-made and natural: from airplane crashes to ice storms, major floods, hurricanes and tornadoes, to trucks hitting telephone poles and to people digging up or cutting our underground plant. Our experience with these situations helped make the 9/11 recovery run effectively.

But we have never experienced anything like this which seemed to be a witches brew of every disaster known—and unknown. And they occurred in 3 separate places, simultaneously. What have we learned? Two major lessons: First, we need to take a fresh look at security of telecommunications networks—and we’re already well along on that. Second, the country needs to develop national policies related to access to critical network assets, cybersecurity, and the redundancy and diversity of networks.

At Verizon, we have a regular, aggressive schedule of security audits, and continual discussion with the security community about new threats. These practices had been the cornerstone for our regular cycles of security improvement and testing.

We share information with and work closely with National Security and Emergency Preparedness agencies—at the federal, state and local levels. Agencies such as NYC’s Mutual Aid and Restoration committee, the FBI’s National Information Protection Center, the National Communications System, and the National Security Telecommunications Advisory Committee are illustrative. Many of those discussions are very candid and involve vulnerability assessments and plans.

Since 9/11, Verizon has additional efforts underway to further improve the security, survivability and rapid recovery of our networks.

We have undertaken a review of which assets need additional hardening. This means a physical inventory of all 5100 central offices and hundreds of key buildings, with ranking for significance—and thus priority attention for hardening. Mostly this means beefing up physical security—such as perimeter and entryways, some better monitoring, and in a few cases interior partitioning.

We have heightened attention to prevent and discover unauthorized cyber-intrusion. We caught and were the first to report a major computer virus to National Information Protection Center right after 9/11.

We continue our regular, aggressive security audits that Verizon conducted even before 9/11. And we promptly address any findings of non-compliance or design weakness.

I thank the Committee for its attention to critical infrastructure matters, and I will try to answer any questions that you have.

Senator INOUE. Thank you very much, Mr. Crotty.
May I now recognize Ms. Harris.

**STATEMENT OF GLORIA HARRIS, VICE PRESIDENT OF
OPERATIONS—NEW YORK, NEW JERSEY AND CONNECTICUT,
AT&T WIRELESS**

Ms. HARRIS. Mr. Chairman, Members of the Committee: Thank you for the opportunity to appear before you today. I am Gloria Harris, Vice President, Field Operations, New York, New Jersey, and Connecticut, of AT&T Wireless. Today my testimony will focus on how AT&T Wireless responded to the events of September 11th as well as the steps we are taking in the aftermath of 9-11 to enhance our emergency response procedures and to make our wireless network as strong as it can possibly be.

The horrific events of September 11th had a profound effect on our Nation's critical telecommunications infrastructure. AT&T Wireless' network was pushed to its limits both in New York and Washington, D.C. I am proud to say, however, that our robust system withstood the assault, thanks in great part to our dedicated employees who worked around the clock and who also refused to go home, and followed our established emergency procedures.

Problems for our network began almost immediately after the first plane hit the World Trade Center. Although our facilities sustained no direct damage at that time, thousands and thousands of AT&T Wireless subscribers in New York and Washington who under normal circumstances would not be using their wireless service at all simultaneously picked up their phones and began to dial—some to contact loved ones, some to call for help, and some to say goodbye.

We also began handing out wireless handsets to emergency workers at Ground Zero in lower Manhattan, all of whom started placing calls immediately to coordinate rescue and recovery efforts.

Traffic on our network in Manhattan increased by as much as 150 percent from the same day the previous week, and in certain areas of the city there were 360 percent more call attempts than AWS usually experiences.

Around 4:00 in that afternoon, the burden to our network increased dramatically as a result of the complete destruction of Verizon's major switching office, which was directly across the street from World Trade Center. Not only did that Verizon switch serve 45 of our cell sites, the landline customers in the affected area had nowhere to turn for service but to their wireless carriers.

Just minutes after the north tower was hit, we activated our highest level of disaster response with national, regional, and local coordination on a 24 by 7 basis. As part of these activities, we established a 96-port conference bridge which remained open day and night for weeks after September 11th. Although intended to manage internal resources, that bridge soon became an essential mechanism for communication among dozens of different agencies. Police, fire, and other emergency responders regularly dialed in order to distribute and obtain information about rescue and recovery ac-

tivities and public safety dispatchers used the conference facilities to request our assistance in tracking callers to 9-1-1.

Obstacles encountered in trying to restore wireless service in the New York area were enormous and, surprisingly, had much to do more with bureaucratic hassles than with technical problems. First we discovered that bringing equipment into Manhattan on September 11th and ensuing days would be a significant challenge because all bridges into the city were closed and all flights had been grounded.

Even after equipment arrived at its destinations, however, we had serious problems in getting our "Cells on Wheels," our COW's, as we call them, permitted and parked in locations that had line of sight to our network. While New York authorities were quite cooperative, certain other nearby localities wanted us to go through full-fledged zoning proceedings, which normally could take weeks or even months, before we could site and activate these temporary facilities.

But perhaps the biggest obstacle to our recovery activities was in our attempt to obtain and retain access to Ground Zero for our employees, contractors, and vendor employees. This seemed to be primarily an issue of too little coordination among dozens of agencies. While the police department might let us bring our equipment into the area in the morning, a few hours later the fire marshal would deny access to the same equipment or require another burdensome round of paperwork.

The final hurdle we faced was the lack of sufficient spectrum to support our recovery operations and the increased call burden. Because many customers in Manhattan had no wireline service and because rescue workers were using AT&T Wireless phones for Ground Zero communications, our network remained severely overloaded for weeks.

Accordingly, on September 12th we went to the FCC and, with the cooperation of NextWave Communications, we requested a special temporary authorization to use NextWave's unused spectrum in the New York market. The FCC responded immediately and that very day we had approval to use those bands.

By September 27th, through the addition of these channels as well as the deployment of COW's and the expedited construction of new sites, we had added enough capacity in Manhattan to permit almost 5,000 additional simultaneous calls. By the following day, we had permanently restored all but three of the recoverable sites.

While our primary focus during the days surrounding September 11th was on averting a network disaster and continuing to maintain critical wireless service to public safety and commercial users, we were also heavily involved in supporting the ongoing search and recovery efforts at Ground Zero and the Pentagon in other ways. Immediately after September 11th, for example, we activated, registered, and handed out more than 5,000 wireless phones to approximately 50 organizations, including the Red Cross, FEMA, the Department of Transportation, and the City of New York.

In addition, together with the Wireless Emergency Response Team, a newly formed coalition of wireless and wireline telecommunications carriers and infrastructure providers, we equipped three-person teams with spectrum analyzers, directional antennas,

and portable generators and sent them out to search for signals emanating from cell phones at Ground Zero.

We also used customer records to identify all the calls placed to 9-1-1 from the World Trade Center and the Pentagon and, at FEMA's behest, called those numbers to determine if the callers needed further assistance. While no survivors were located in either location, we contacted many people who were thought to be missing and helped to bring closure to family members who lost their loved ones on September 11th.

So the question now is where do we go from here? What have we learned from September 11th that could make our network stronger and ensure uninterrupted service during emergencies for both public safety personnel and our customers? Since September 11th AWS has taken a number of steps internally to ensure that we can respond effectively to a disaster on a nationwide level and across all critical units of our company. In addition, in light of the finite capacity of all telecommunications networks, we have been working to come up with a practical solution to ensure those with the greatest need are able to place and receive calls.

Emergency agencies' need to communicate is obviously critical, but 9-11 taught us that the ability of our existing customers to place calls is no less important. Indeed, it was a wireless call that gave passengers on a plane likely bound for the White House or the building we are standing in right now the information they needed to avert an even larger disaster.

Accordingly, we have been working cooperatively with the members of the wireless community and the national communications system to develop a plan that will give priority access to certain emergency personnel in times of severe network congestion, while at the same time reserving capacity for customers. We think that the wireless priority access plan currently being discussed goes a long way towards ensuring that the facilities we have are used in the most efficient and effective manner possible.

Now I will spend just a few minutes suggesting how you, Congress, can help us in our efforts to strengthen our network. First, as I indicated earlier, one of the most significant problems we faced in attempting to restore service to customers and emergency workers after September 11th was coordinating with the dozens of Federal, State, and local agencies and offices to bring the necessary equipment to the affected areas, to obtain permits to site those temporary facilities, and to ensure that our employees had continual access to the equipment once it was in place.

One suggestion I have to ensure smoother sailing in the future would be to empower FEMA or another Federal agency to oversee issues involving the access of essential companies, such as telecommunications providers like AT&T Wireless, to disaster areas. Should we ever face a similar circumstance—and I pray that we do not—the agency could distribute universal badges which the companies could then hand out to their employees as necessary.

The next major action Congress could take to help ensure the development of a comprehensive wireless network is to assist us in our efforts to obtain more spectrum. AT&T Wireless is in the enviable position of having enough spectrum to provide services to our customers' demand through the first part of this decade. As we

begin to roll out advanced technologies on a wider scale, we will require additional bandwidth to provide the types of services our subscribers tell us they want and at the same time to be able to assist public safety agencies with their needs.

Much of the globally harmonized spectrum that wireless carriers need is woefully underutilized today by existing licensees in those bands and should be reallocated promptly.

Today, based on the lessons learned from 9–11, we have begun to take the necessary steps to ensure that our network and service to our customers and emergency personnel remain strong for years to come. We hope that we can count on you to also take actions that will safeguard the wireless industry's continued effort to serve the public, both in times of disaster and in times of peace.

Thank you for this opportunity to share our findings today.

[The prepared statement of Ms. Harris follows:]

PREPARED STATEMENT OF GLORIA HARRIS, VICE PRESIDENT OF OPERATIONS—
NEW YORK, NEW JERSEY AND CONNECTICUT, AT&T WIRELESS

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to appear before you today to discuss how the wireless industry's ubiquitous and robust telecommunications networks enhance public safety, assist emergency personnel, and permit crucial contact among families and friends on both a daily basis and in times of crisis. I am Gloria Harris, Vice President, Field Operations—Tristate Area, of AT&T Wireless Services, Inc. ("AWS"). Today, my testimony will focus on how AWS responded to the events of September 11, 2001, including how we used our existing procedures and outstanding personnel to avert a potential network disaster. Even as cell sites across New York City failed due to a wireline switch outage, and thousands upon thousands of callers turned on their wireless phones at the same time, I am proud to say that our network remained solid. I will also tell you about the steps AWS is taking in the aftermath of 9–11 to enhance our emergency response procedures and to make our wireless network as strong as it can possibly be.

I. HOW WE RESPONDED.

Impact on the Wireless Network. At 8:45 a.m. on September 11, 2001, American Airlines Flight 11 crashed into the North Tower of New York's World Trade Center complex. This unspeakable terrorist act was just the beginning of what would soon become this century's most horrific national tragedy. It also put an enormous strain on our nation's telecommunications networks, including AWS's wireless systems, which were crucial not only to the rescue, recovery, and law enforcement efforts that were immediately launched, but to the ability of American citizens to reach loved ones in a time of crisis.

Between 9:00 and 10:30 a.m. on September 11, additional planes were piloted into the South Tower of the World Trade Center and the Pentagon, another plane crashed in Shanksville, Pennsylvania, and both World Trade Center towers collapsed. By mid-afternoon, there were power outages throughout lower Manhattan and six AWS cell sites were out of service.

To complicate matters, thousands and thousands of AWS subscribers in New York and Washington, who, under normal circumstances, would not be using their wireless service at all, simultaneously picked up their phones and began to dial—some to contact loved ones, some to call for help, and some to say goodbye. In addition, AWS handed out wireless handsets to emergency workers at Ground Zero in lower Manhattan, all of whom started placing calls immediately to coordinate rescue and recovery efforts. Traffic on our network in Manhattan increased by as much as 150 percent from the same day the previous week, and in certain areas of the city there were 360 percent more attempts to make calls than AWS usually experienced. Our systems in Washington, D.C. and Pittsburgh were being used up to and beyond capacity as well.

Around 4:00 p.m., the burden to AWS's network increased dramatically as a result of the complete destruction of Verizon's major switching office, which was directly across the street from the World Trade Center. Not only did that Verizon switch serve 45 AWS cell sites—most of which were in lower Manhattan—the landline customers in the affected areas had nowhere to turn for service but to their wireless

carriers. Verizon obviously was intent on restoring service for its own customers and consequently was unable to reroute AWS's traffic from the impaired cell sites. By the evening of September 11, 47 AWS cell sites were out of service, one cell site had been completely destroyed, all of lower Manhattan had sustained a complete commercial power failure, and wireless call volumes remained extremely high in light of the failure of the wireline network.

What We Did. Notwithstanding the incredible strain of increased call volumes and impaired cell sites, AWS's wireless network in New York and everywhere else remained strong. This is due in large part to our ability to draw upon the lessons learned and the procedures developed from many years of responding to hurricanes, tornados, and floods, as well as planned day-long disaster simulations. Specifically, in every market in the United States in which it provides service, AWS has a disaster field office. When not needed, these offices serve as conference rooms or storage areas, but they are equipped with redundant telephone lines, back-up power sources, food and medical supplies, and manuals outlining the steps to be taken in disaster situations. Each of our disaster field offices reports to one of our eight regional Emergency Operations Centers, whose activities are coordinated by AWS's National Emergency Operations Center in Bothell, Washington. Clearly, no established procedures could have prepared us for the events of September 11, but they did enable AWS to avert a potentially catastrophic network failure.

Just minutes after the North Tower was hit, AWS activated its highest level of disaster response. AWS's National Emergency Operations Center coordinated efforts at the national, regional, and local levels by identifying all available personnel and equipment to support recovery and repair activities in New York and Washington, D.C. We also set up a regional staging ground in Paramus, New Jersey, and used that location for the delivery of portable generators, network equipment, and "Cells on Wheels"—or "COWs"—from across the country. Many of our Manhattan employees were asked to report to a central disaster field office, where they were accounted for and where they began preparing for cell site recovery.

In addition, on September 11, AWS established a 96-port conference bridge to manage technical resources among our national and regional operational centers and the affected disaster field offices. That bridge, however, which remained open day and night for weeks after September 11, was not used solely by AWS personnel. Rather, police, fire, and other emergency responders regularly dialed in to the bridge in order to distribute and obtain information about rescue and recovery activities. Similarly, public safety dispatchers used the conference facilities to request AWS's assistance in tracking callers to 911. As it turned out, AWS's conference bridge was an essential mechanism for communication among dozens of different agencies, as well as a way for AWS to coordinate its own internal recovery efforts.

AWS's primary activity on September 11 and the following days was to assess the extent of the impairment to our service in New York and Washington, D.C. and to prioritize service restoration efforts. Since we could not rely on Verizon to install new facilities for us or to reroute traffic from its destroyed lower Manhattan switch, we had to figure out alternate ways to provide service in the areas around the impaired cell sites. Initially, this was accomplished by the mobilization of COWs or by adding additional equipment and capacity to nearby cell sites.

Bringing equipment into Manhattan on September 11 and the ensuing days, was a significant challenge because all bridges into the city were closed and all flights had been grounded. Accordingly, we worked with the New York City Office of Emergency Management and the Mayor's office to obtain permits or waivers to carry our equipment over the closed infrastructure and to secure escorts for the trucks.

We also faced serious obstacles in getting the COWs permitted and parked in locations that had a line-of-site to our network. While New York authorities were quite cooperative, certain other nearby localities wanted us to go through full fledged zoning proceedings, which normally could take weeks or even months, before we could site and activate these temporary facilities. AWS personnel, however, worked around the clock to obtain approvals from local authorities, establish microwave links, and test the temporary facilities. Within 21 hours after deployment, AWS activated its first COW in Liberty State Park in Jersey City, New Jersey. Shortly thereafter, a second COW was sent to Brooklyn to further support Manhattan's network capacity. And, at the Pentagon's request, we deployed a third COW to the Pentagon. Ultimately, AWS activated a total of 17 COWs: 15 in New York, one in Washington, D.C., and one in Pennsylvania. In addition, AWS deployed 12 portable generators to support the cell sites without commercial power.

Over the next several days, AWS brought 26 technicians from other AWS markets across the country to assist in New York, where the network was the most impacted. The technicians worked to integrate COWs into the permanent infrastructure, repaired AWS's damaged equipment, implemented a solution to permit law en-

forcement wiretapping, and recovered court-ordered surveillance systems used by law enforcement agencies. In addition, at the request of the New York Police Department, network engineers initiated, coordinated, and implemented the addition of over 6,000 emergency voice mail message hours in Queens, Manhattan, and Rochelle Park, thereby increasing the number of voice mail messages allowed in subscribers' mailboxes.

Perhaps the biggest obstacle to our recovery activities was in our attempts to obtain—and retain—access to Ground Zero for our employees, contractors, and vendor employees. This seemed to be primarily an issue of too little coordination among dozens of state and local agencies. While the police department might let us bring our equipment into the area in the morning, a few hours later, the fire marshal would deny access to that same equipment or require another burdensome round of paperwork. Verizon and Con Edison apparently did not encounter these difficulties because they were considered utilities, while AWS was not.

On September 11, the most immediate danger to our network was the enormous increase in calls being placed by our customers and emergency workers. During the peak of the crisis, we instituted load shedding procedures by deactivating non-essential features on a number of switches, such as Caller ID, performance measurement capability, and fraud detection, to avoid a complete crash of our New York system. The result was similar to that achieved by shutting windows on a personal computer—it helped provide more capacity for traffic routing. While there nevertheless were periods during the day in which accessing our network required multiple attempts, the system remained solid.

It quickly became clear to AWS, however, that it required additional spectrum to support recovery operations and the increased call burden. Accordingly, on September 12, AWS, with the cooperation of NextWave Communications, obtained a special temporary authorization from the Federal Communications Commission, which allowed it to access 10 MHz of unused spectrum licensed to NextWave in the New York market. By September 27, through the addition of these channels, as well as the deployment of COWs and other temporary equipment, and the expedited construction of new sites, AWS had added enough capacity in Manhattan to permit almost 5,000 additional simultaneous calls. It also added 630 new voice paths in Washington, D.C. by September 14, and 158 voice paths in Pennsylvania by September 12. These new channels provided the necessary capacity to compensate for the site losses at Ground Zero and to accommodate the additional call volume around the White House, the Pentagon, and the crash site in Shanksville, Pennsylvania.

At the same time as it was activating COWs and adding equipment at adjacent cell sites in the affected areas, AWS was performing surveys of all 47 lost cell sites to determine how service could best be restored on a permanent basis. By September 28, AWS had restored all but three of the recoverable cell sites using microwave facilities or AWS's own backhaul facilities, as well as working with Verizon to reroute traffic.

AWS's rescue efforts. While AWS's primary focus during the days surrounding September 11 was on averting a network disaster and continuing to maintain much needed wireless service to public safety and commercial users, it also supported the ongoing search and recovery efforts at Ground Zero and the Pentagon in other ways. Immediately after September 11, for example, AWS activated, registered, and handed out more than 5,000 wireless phones to approximately 50 organizations, including the Red Cross, the Federal Emergency Management Agency ("FEMA"), the Department of Transportation, and the City of New York. With these phones, AWS donated over 1.3 million minutes of airtime usage. In addition, AWS waived all airtime charges for calls made and received on September 11 by east coast customers between Massachusetts and Virginia. AWS employees also worked around the clock at phone distribution and recharging centers located near the disaster areas. Similarly, AWS coordinated the delivery of safety kits, radios, goggles, breathing filters, gloves and radio equipment to the impacted areas to sustain its own efforts and to support local emergency response teams in their recovery efforts.

To aid in the various search and rescue efforts, AWS joined the Wireless Emergency Response Team ("WERT"), a coalition of wireless and wireline telecommunications carriers and infrastructure and equipment providers. AWS allocated channels for the WERT activities and donated spectrum analyzers to support recovery missions. Both in conjunction with WERT and on its own initiative, AWS also established three-person teams of AWS technicians to assist emergency response personnel in searching for possible survivors in the World Trade Center rubble. Each team, equipped with a spectrum analyzer, a directional antenna, and a portable generator, was sent out to search for signals emanating from cell phones at Ground

Zero. Tragically, these teams found no survivors—only phones that had been left on by WTC workers.

In addition, AWS assisted FEMA in its efforts to locate those lost in the World Trade Center and the Pentagon by providing them with customer information that detailed which customers had placed calls from inside the Towers, the Pentagon, and nearby buildings. We identified all the calls placed to 911 from those locations and proceeded to call back each calling party to determine if they needed further assistance. While no survivors were located in either location, AWS contacted many people who were thought to be missing and helped bring closure to family members who lost their loved ones on September 11.

AWS also supported law enforcement personnel and kept rescue teams from danger by discrediting false reports. In addition, AWS provided U.S. Marshals with network information and frequencies for the equipment used to help locate cellular calls. In conjunction with these efforts, AWS provided guidance to 911call centers by giving recommendations for trapped survivors' cell phone usage to conserve battery power and maintain the best possible signal.

II. WHERE DO WE GO FROM HERE?

As the foregoing shows, given its existing procedures, training, and outstanding personnel, AWS was in a very good position to respond to the 9–11 crisis from a network operations standpoint. Despite the loss of 47 cell sites, largely due to the destruction of Verizon's wireline switch at Ground Zero and an incredible increase in calls on September 11 and the following days, AWS kept its network up and running, obtained additional spectrum, added temporary cell sites, and addressed urgent requests for service, equipment, and facilities from displaced residential and business customers, as well emergency response agencies and utility workers.

9–11 also taught AWS, however, that there are many ways in which it could improve its emergency procedures and be better prepared for disasters of any sort that impact the nation's vital telecommunications infrastructure. Therefore, as soon as the initial crisis had subsided in the days following September 11, AWS personnel from all areas of the company got together to brainstorm about what had gone wrong, what had gone right, and what it should do from that day forward to make use of the lessons learned from 9–11.

AWS Crisis Management Team. Although, as described above, AWS had in place on September 11 a multi-level disaster response team that was able to deploy quickly and respond efficiently to dozens of network outages and other problems, we came to the conclusion that our existing procedures were focused too heavily on just the operational part of our business. For that reason, we have now created a Crisis Management Team that operates at the highest levels and covers all functions of the company. This team has representatives in every AWS market, company vice presidents at the regional level, and AWS's Chief Operating Officer at the head. Personnel from customer service; environmental, health and safety; financial; human resources; legal; marketing; real estate; insurance, as well as network operations and every other corporate unit of AWS participate in this group and bring their particular expertise and interests to the table. Already, we have established business recovery plans for each critical unit of the company. We believe that our Crisis Management Team will help ensure that AWS can respond effectively to a disaster on a nationwide and *business-wide* level.

Priority Access. One thing 9–11 made abundantly clear is that wireless phones are crucial to the nation's ability to communicate during a disaster. Wireless service allowed people trapped in buildings to call for help and, in some cases, to call their loved ones for the last time, allowed passengers on a plane likely bound for the White House—or the building we are in right now—to obtain information in time to avert an even larger disaster, and allowed residents of New York, Washington, D.C., and across the nation to let their sons, daughters, husbands, and wives know they were safe. Wireless phones also were essential for firefighters, police, and other emergency response personnel in those cities to coordinate their rescue efforts, and for utility workers to coordinate their repair and salvage efforts.

In light of the limited capacity of any telecommunications system, it is necessary for carriers to balance competing demands for network time. Emergency agencies' need to communicate during a crisis obviously is crucial, but, as we discovered on September 11, the ability of AWS's existing customers—workers, parents, airline passengers—to speak to each other and to call for help was no less important. Accordingly, since September 11, AWS has been working to come up with a practical solution to ensuring that those with the greatest need are able to place and receive calls. To this end, AWS, together with other members of the wireless community and the National Communications System have been working cooperatively to develop a plan that will give access to the next available wireless voice channel to cer-

tain National Security/Emergency Preparedness personnel in times of severe network congestion, while at the same time reserving capacity for customers.

Obviously, no network can be built to a capacity to accommodate all customers and emergency agencies during disasters of the magnitude experienced on September 11. However, we want to ensure that the facilities we do have are used in the most efficient and effective manner possible. We think that the wireless Priority Access Plan currently being discussed goes a long way toward accomplishing that goal.

Need for Government Assistance. AWS is taking all the steps it can in preparing the company to respond to disasters—both natural and manmade—that affect the ability of U.S. citizens to communicate. We believe that the procedures we are establishing today will make us better able to coordinate across all functions of the company in order to patch holes blown in our network as well as respond to customer and government problems quickly. There are a number of issues beyond our control, however, that, if not addressed, have the potential to make these efforts significantly less effective. Accordingly, we are asking Congress and federal agencies to help ensure that wireless carriers are able to obtain access to disaster sites, have sufficient spectrum to meet future consumer demands, and that they can site towers efficiently, all of which are necessary to create the robust networks required to withstand, and recover rapidly from, any type of disaster.

First, as indicated earlier, one of the most significant problems we faced in attempting to restore service to customers and emergency workers after September 11 was coordinating with dozens of federal, state, and local agencies and offices to bring necessary equipment to the affected areas, to obtain permits to site those temporary facilities, and to ensure that our employees had continual access to the equipment once it was in place. One suggestion we have to ensure smoother sailing in the future would be to empower FEMA or another federal agency to oversee issues involving the access of essential companies, such as telecommunications providers like AWS, to disaster areas. Should we ever face similar circumstances (and we pray we do not), that agency could distribute “universal” badges, which the companies could then hand out to their employees as necessary.

Second, the primary constraint on the development of a comprehensive wireless market is the lack of adequate spectrum. AWS is in the enviable position of having enough spectrum to provide the services our customers demand for the first part of this decade. As we begin to roll out advanced technologies on a wider scale, however, we will require additional bandwidth to provide the types of services our subscribers tell us they want and at the same time be able to assist public safety agencies with their needs. The government’s primary role in the development of voice and broadband wireless networks—one which only it can fulfill—is to ensure that spectrum that meets the technical and practical needs of carriers is available. Additional bandwidth is absolutely essential if the wireless industry is to be able to meet future consumer needs, much less respond to such needs during times of disasters.

Much of the globally harmonized spectrum that AWS and other wireless carriers need is woefully underutilized by existing licensees in those bands today. Unfortunately, however, the process for reallocating such spectrum is moving slowly and unevenly. The Federal Communications Commission has declined to make certain fixed wireless bands available to existing mobile operators and, despite the failure of the mobile satellite service (“MSS”) industry to use even a fraction of the spectrum currently allocated to it, it continues to ask the agency to license more MSS operators. It also remains unclear if or when additional spectrum used by the Department of Defense and other federal agencies could be freed up for commercial use.

In this time of bandwidth scarcity, it is unreasonable to let spectrum lie fallow. There are dozens of wireless carriers today that would willingly spend billions of dollars for the spectrum held—but barely used—by some current satellite and broadcast licensees and government agencies, and would construct the networks and serve customers immediately. If 9–11 shows anything, it is that the wireless infrastructure is no longer a luxury service or merely a backup network to the facilities other carriers have in the ground and strung on poles. Rather, it is a vital, robust, and primary means of communication everyday, and especially in times of crisis. Accordingly, AWS respectfully requests that Congress to do everything within its power to ensure that spectrum is distributed in a manner that permits the wireless industry to grow and to create the strong networks the country needs.

Finally, while insufficient spectrum remains one of the greatest barriers to wireless deployment, the inability of wireless carriers to site the towers and other facilities they need to provide such service without unreasonable delay or expense also remains a huge obstacle. Although Congress has directed federal agencies to make federal property available for wireless telecommunications siting, the agencies often

delay approval of applications for unreasonable periods of time or attempt to collect excessive fees for the use of federal lands. Similarly, localities regularly ignore Congress's admonition that they not use their zoning authority to prohibit the provision of wireless service. It can sometimes take years to site a tower and the costs of zoning hearings and litigation are often enormous. These delays and expenses not only affect the quality of service for consumers today, they reduce AWS's ability to deploy the redundant facilities needed to respond to the loss of cell sites in disasters.

Although Congress has made it clear to federal, state, and local agencies that they should not stand in the way of wireless deployment, apparently the message needs to be stronger. Accordingly, AWS urges Congress to set explicit guidelines for the amount of time an agency can take to respond to a siting request and for holding hearings on that request. In addition, we ask Congress to ensure that the fees the agency charges for use of the government property are truly just and reasonable.

Misleading public safety "solutions." Since September 11, a number of parties have come forward with alleged "solutions" to the problems faced by emergency response agencies in communicating during crises. Not surprisingly, each of these plans requires the government to bestow upon the proposing party free and exclusive spectrum without having to go through the process of competitive bidding like similarly situated carriers. In addition—and not surprisingly again—none of these proposals provides a real answer to public safety's communications problems.

One recent proposal, for example, which has been presented to the FCC by Nextel Communications Inc., purports to address interference between public safety operations and commercial systems by swapping various channels in the 800 MHz band. Although this plan would provide Nextel with more desirable contiguous spectrum—including an entirely gratuitous 10 MHz of MSS spectrum—it does not completely resolve any interference issues because public safety radios would still need to be redesigned to filter out interfering signals. More significantly, however, Nextel's proposal would leave hundreds of private radio licensees out in the cold—either paying to relocate their operations to bands with poorer propagation characteristics or lack of available equipment, or operating on a secondary basis to public safety systems. As even the public safety community recognizes, private radio operators provide crucial telecommunications capabilities to gas, electric, water, and other utility companies, which work side by side with emergency response teams during disasters. It makes no sense to curtail utilities' ability to communicate, or require them to expend substantial sums to relocate, to remedy isolated instances of interference that can largely be resolved by better design of public safety radios and the cooperation of affected CMRS providers.

Similarly, certain MSS licensees are now attempting to convince the FCC that their satellite systems are capable of enhancing public safety, homeland defense, emergency service, and military systems in rural areas . . . *but* . . . only if the agency allows them to use the satellite spectrum they received for free to compete as terrestrial wireless providers in urban markets. It is not at all clear why these licensees think they will have any more success in sustaining a rural-only satellite business (and thereby promoting public safety in rural areas) than they have had thus far, when virtually all customers and revenue would come from their (entirely separate) urban terrestrial operations. It is clear, however, that these licensees expect to use the ORBIT Act, which precludes the auctioning of *satellite* spectrum, as a means to use their free spectrum to fulfill their *terrestrial* aspirations. In other words, MSS licensees plan to use free spectrum to compete against companies that paid billions of dollars for their licenses. Rather than permit spectrum allocation and auction decisions to be based on dubious, at best, public safety promises, AWS urges Congress to clarify that the ORBIT Act may not be expanded beyond all semblance of its original meaning.

September 11 taxed resources of all telecommunications carriers in the United States far beyond what we had ever expected or planned for. Nevertheless, we are proud to say that AWS's established procedures, robust facilities, and dedicated employees allowed it keep its network up and running and to restore impaired service in record time. They also allowed us to devote resources directly to the emergency rescue and recovery efforts underway in New York and Washington, D.C.

Today, based on the lessons learned from 9–11, we have begun to take the steps necessary to ensure that our network—and service to customers and emergency personnel—remain safeguarded in the event of almost any disaster. Many of these activities are internal to AWS or involve coordination and cooperation between the wireless and public safety communities. The intervention of Congress, however, is absolutely critical to our ability to obtain the spectrum and site the redundant tower

and transmission facilities that are needed to create truly robust wireless networks. We hope that we can count on you for this help.

Senator INOUE. Thank you very much, Ms. Harris.
Now may I call upon Ms. Herda.

**STATEMENT OF LARISSA HERDA, CHAIRMAN, CHIEF
EXECUTIVE OFFICER AND PRESIDENT, TIME WARNER
TELECOM**

Ms. HERDA. Thank you, Mr. Chairman. Mr. Chairman, Members of the Subcommittee: My name is Larissa Herda. I am Chairman, CEO, and President of Time Warner Telecom, and I want to thank you for the opportunity to talk to you today about what can be done to enhance the reliability and robustness of the Nation's communications network.

Before I tell you who we are, I would first like to tell you who we are not. We are not Time Warner Cable, we are not AOL, nor are we a subsidiary of AOL Time Warner. We have nothing to do with movies, entertainment, Bugs Bunny, or Roadrunner. AOL Time Warner is a large shareholder, but they do not provide funding to our company and they do not manage our business. We are a separately managed, separately publicly traded company.

Time Warner Telecom is actually one of the few viable companies that are competitive local providers providing telecommunications services over our own fiber networks in a local metro area. Today we provide service in 44 markets across the country serving 21 States.

In my testimony today, I will provide a brief summary of our experience during the September 11th attack. I will also explain how the existence, design, and operation of our network provides essential disaster prevention and recovery solutions to the public and the private sector business customers. I will offer my recommendations as to the types of public policy decisions that will ensure that Americans have access to a robust and reliable communications network.

The terrorist attack on September 11th not only reinforced how essential communications are in a time of crisis, but it also raised important questions about the capabilities and durability of our Nation's telecommunications infrastructure. A halt in communications would cripple many elements of everyday life. Time Warner Telecom was instrumental in restoring communications service to the public and private sector after the 9-11 attack. Our network fortunately was only minimally damaged during the attack. Because of our significant fiber investment and the redundancy and diversity that we built into our network, none of our customers that were riding exclusively on our fiber network were affected. Nobody lost service.

Unfortunately, as Mr. Cangemi indicated earlier, New York City Hall did lose phone service following the attacks and, although we were not serving them at the time—we did not actually have fiber infrastructure into their building at the time, my team, working day and night—as my fellow panelists from AT&T Wireless and Verizon said, I do not think any of these technicians ever left during that time. It was really amazing, the amount of work that these people went through, and my team as well. They worked day

and night pulling fiber into the building and they were able to install 300 phone lines for city hall in less than 48 hours in, obviously, a very difficult and dangerous environment. They had to wear respirators and climb many stairs to do it.

Turning up this type of service, just to give you some perspective, would normally take a minimum of, well, under optimal situation maybe 30 to 90 days, because of the need to acquire permits and to construct facilities in the right of way and to gain building access. So you have to gain building owner's permission generally to enter the buildings.

If our fiber had already been in the building, we could have installed service within a few hours, and in fact we had many customers who had lost service from their other providers and we were able to turn up their services almost immediately that day and in days following that.

Additionally, we worked with the Department of Information, Telephone and Technology, Mr. Cangemi's organization to identify other municipal offices that needed service restored. I can honestly say there was a tremendous amount of cooperation between all the carriers that were functioning in the city that day. In such a dramatic situation, I think it was clearly beneficial to have multiple providers in the market to be in a position to be able to restore the critical services.

Many businesses—prior to September 11th many businesses understood the value of building redundancy and diversity into their communications data systems. But obviously, since September 11th they are much more focused on that today.

The best way in our opinion to minimize disruption of critical infrastructure is to avoid having a single point of failure through diverse and redundant network facilities. Customers can obtain optimally—they can obtain optimal diversity by obtaining services from two different facilities-based providers. By doing so, customers decrease the likelihood of complete service outage if one of their competing carriers' services goes down. Also, having an established relationship with more than one carrier facilitates the replacement of services.

Since 9-11 we have increased security at all of our facilities, implemented more thorough disaster prevention and recovery plans, and presented a series of seminars to educate the business community on the value and process of building redundancies into their communications systems. But most importantly, we have always constructed our network in a manner designed to eliminate single points of failure.

To illustrate this, you all should have a diagram of our network here that will explain our network architecture. On this diagram there are four squares in each of the corners of the page that represent our central offices. This one is specific to Manhattan, but our networks pretty much look like this in every city that we go into. You can see the fiber distribution rings coming out from each of the central offices. There are distribution rings to serve customers, to serve carriers, to connect up to the local exchange offices. Then there is a big ring, a big backbone ring that connects up all of these offices as well.

If there is a fiber cut in any of these locations, services are automatically rerouted within 50 milliseconds, which is essentially faster than the blink of an eye, and customers do not experience an outage. In fact, between the two bottom central offices, 60 Hudson and 23rd Street, we did have a fiber cut on September 11th. However, none of our customers lost service because the technology kicked in, the diversity worked, and we are obviously very thankful for that.

The ability to access more than one facilities-based carrier is the best way to minimize disruption to critical infrastructure and reduce down time and loss of major business functions in the event that there is a service disruption that cannot be avoided.

Government can help ensure that public and private sectors have access to these services by reducing the barriers to construction that currently exist. Many customers want network diversity, but too often we are not able to meet that demand because we cannot get permits that we need to access the right of way from the municipalities or we cannot get the building owners to give us permission to enter the buildings in a timely and cost effective manner.

These two barriers of construction are a problem for us because they limit our ability to grow our business. But they also restrict access to the public good and deny businesses the ability to purchase critical services from their provider of choice.

While I encourage you to address these general issues in the marketplace, there are some things that the government can do very easily today to help us address some of the issues. Number one, they can require that the Federal Government—that they need to obtain service from at least two different facilities-based providers in each of their buildings whenever that is possible. Number two, only enter into lease agreements with landlords that will allow other telecommunications providers into the building that are either selected by the Federal Government or any other tenant in the building and to allow them to have physical access into the building promptly and at fair rates on reasonable and nondiscriminatory terms. It is my understanding that these conditions can be added through the Federal telecommunications procurement process and that can be done now by issuance of an executive order.

In conclusion, the need for diversity highlights the important benefits of a competitive telecommunications market. There is no question that the telecom industry has been affected by the downturn of the economy, but the need for competition is more important now than really ever before. Businesses and government offices need access to diverse networks. They need quality services at affordable prices, policies that promote competition are critical, and strict enforcement of the 1996 Act remains the most important tool that the government has to encourage the competition.

Setting aside the other advantages of competition, the attacks of September 11th and the demonstrated support by the competitive telecom entrants such as Time Warner Telecom and the ability of all the carriers that were involved, including obviously the tremendous job done by the incumbent in restoring those critical services, proves the strategic value of competitive fiber facilities-based providers.

I want to thank you for the opportunity to testify before you today and I am happy to answer your questions.

[The prepared statement of Ms. Herda follows:]

PREPARED STATEMENT OF LARISSA HERDA, CHAIRMAN, CHIEF EXECUTIVE OFFICER
AND PRESIDENT, TIME WARNER TELECOM

Mr. Chairman and Members of the Subcommittee:

On behalf of Time Warner Telecom Inc. I would like to thank the committee for the opportunity to talk to you today about the impact the September 11th disaster had on the nation's communications infrastructure. My name is Larissa Herda and I am the Chairman, President and CEO of Time Warner Telecom ("TWTC"), which has grown to be one of the largest new competitive entities in the telecommunications industry. We exist today because of the pro-competitive policies adopted in the Telecommunications Act of 1996. We are unique in a number of respects.

TWTC builds its own local and regional fiber optic networks and delivers "last-mile" broadband data, dedicated Internet access, and voice services to small, medium and large businesses. We provide service to a diverse customer base across the country. The Company currently serves business customers in 44 U.S. metropolitan areas. Since the passage of the 96 Act, we have invested more than \$2.0 billion in building a network infrastructure and have created over 2,500 high-tech jobs nationwide.

The terrorist attacks on September 11 not only reinforced how essential communications is in times of crisis, but also raised important questions about the capabilities and durability of our nation's telecommunications infrastructure. As executives and governments across the world now attempt to anticipate and prevent similar disasters, the imperative of a sound and resilient communications infrastructure has moved to the forefront of national consciousness, as a halt in communications would bring to a standstill airlines, the stock exchange, banks, television, radio to name just a few elements of everyday life.

In my testimony today I will provide a brief summary of TWTC's experience following the September 11th attack, explain how the existence, design and operation of our network provides essential disaster prevention and recovery solutions to public and private sector business customers and offer my recommendations as to the types of public policy decisions that will ensure that Americans have access to a robust and reliable communications network.

SEPTEMBER 11, 2001 New York City

Time Warner Telecom was instrumental in restoring communications service to the public and private sector after the 9.11 attack. Our network, fortunately, was only minimally damaged by the attack. Because of our significant fiber investment, and the redundancy and diversity that we built into our network, none of the customers that were exclusively on our network lost service. Unfortunately, New York's City Hall did lose its phone service following the attacks. Although TWTC was not providing service to the city building at the time, my team, working day and night pulling fiber into their building, was able to install 300 phone lines for City Hall in less than 48 hours—in a difficult and dangerous environment I might add. This type of service would normally take a minimum of 21 days to install because of the need to acquire permits to construct facilities in the right of way and gain the building owners permission to enter the building. (If our fiber was already into this building, we could have installed service within a few hours.)

Additionally, we participated in regular meetings with the city's Department of Information, Telephone and Technology (DOITT) to identify other municipal offices that needed service restored. With the cooperation of the incumbent telephone company and other telecom providers, the industry was able to identify which companies had network in place and restored service where it was needed. Although the incumbent telephone company was working valiantly to restore service, in such a dramatic situation it was clearly beneficial to have multiple providers in the market to restore critical services.

Disaster Recovery Requires Both Prevention and Recovery

Many businesses understood the value of building redundancy into their communications and data systems prior to 9.11, but many more are focused on it today. The best way to minimize disruption to critical infrastructure is to avoid having a single point of failure through diverse and redundant network facilities.

Customers can obtain diversity primarily by obtaining services from two different facilities-based carriers. By doing so, customers decrease the likelihood of a complete

service outage if one of their competing carriers' service goes down. Also, having an established relationship with more than one carrier facilitates the replacement of services.

The Time Warner Telecom Network

We have constructed our network in a manner designed to eliminate single points of failure. For example, in NYC we have switches in two locations—one on 61st street and one on 23rd. We build our network in a ring topology that provide a diverse and redundant electronics in order to reduce the likelihood that service will be lost in the event of a failure in any part of the network. I'd like to take a moment to explain our network architecture.

Since 9.11, we have increased security at all our facilities, implemented more thorough disaster prevention and recovery plans, and presented a series of seminars to educate the business community of the value and process of building redundancies into their communications systems. For illustrative purposes, I have provided the committee with the materials used for some of these seminars.

Policies That Promote Facilities-Based Competition Give Customers Access To a Critical Tool Needed To Plan Against a Single Point of Failure

Businesses must have access to more than one facilities-based carrier. This access is essential to minimize disruptions to critical infrastructure and to reduce downtime and loss of major business functions in the event a disruption cannot be avoided. Government can ensure the public and private sectors have access to these services by reducing the barriers to construction that currently exist.

Barriers To Construction

In order to recognize the goal of true facilities-based competition, companies must physically construct their own fiber network. There is incredible demand for these services in the marketplace. But too often we are not able to meet that demand because we can't get the permits we need to access the right of way or we can't the building owners permission to enter a building in a timely and cost-effective manner. These two barriers to construction—the failure of building owners to open their buildings to competitors and the failure of municipalities to approve construction permits under reasonable terms, quickly and on a competitively neutral basis are a problem for me because they limit my ability to grow my business. But they also restrict access to a public good and deny businesses the ability to purchase critical services from providers of their choice.

Building Access

In order to serve customers with our own facilities, we need to take our fiber directly into the customer's buildings. In order to do this we must obtain access into the buildings in which are customers are tenants. In the initial aftermath of 9.11 we found building owners in NYC much more cooperative in providing access to their buildings. Unfortunately, we are now seeing them return to the practice of delaying this access and imposing unreasonable costs on the price of access. How soon they have forgotten the lessons of 9.11. While I encourage you to address the building access issue for the entire marketplace, there is something that government can do easily today.

First, the federal government should be required to purchase local telecommunications services from at least two providers with distinct network facilities in each market where choice is available. Present law permits, but does not require, purchases from two or more vendors. This requirement is necessary to ensure that federal agencies have telecommunications services that are diverse and redundant. This is a crucial element to protect the ability of the federal government to remain in operation and communication with the public and others during a disaster or other emergency, and to increase the stability of our government's networks.

Diversity involves establishing physically different routes into and out of and a building, and different equipment; so as to better ensure continued operations in the event that one route or network is impacted adversely by a disaster or other form of interference.

Redundancy involves having extra capacity available, generally from more than one source, and also incorporates aspects of diversity. Not only does redundancy entail having capacity in reserve to handle sudden increases in demand or partial outages, but it also entails securing service from more than one provider where practicable. The use of multiple providers increases the probability that service will be maintained or restored in the event of a disaster, emergency, or carrier-specific problem, and decreases the chances that all communications capabilities will be affected in the same way at any given time. It ensures the availability of two distinct

workforces to serve the customer and the opportunity to try two different approaches to solve a common or related problem.

This requirement will help the federal government to reap the benefits of continued competition. Having multiple providers and diverse facilities enables the federal government to increase or decrease the use of a provider or set of facilities, thus creating continued incentive on the part of the carriers to provide good service, favorable pricing and continued innovation and cooperation. A multi-vendor strategy provides valuable leverage to federal tenants.

Ensuring that multiple companies will have a greater opportunity to provide local service and serve federal tenants is a way to promote and advance the goals of the Telecommunications Act of 1996 while at the same time providing a valuable benefit to the federal government in its capacity as a purchaser of telecommunications services. This requirement also would create an economic stimulus that would promote telecommunications investment, competition, and jobs.

Second, where the federal government seeks to lease space from a private landlord, absent special circumstances, the federal government should do so only in buildings where any telecommunication provider(s) it or any other tenant selects can have physical access to the building promptly at fair rates and on reasonable and nondiscriminatory terms.

This requirement is vital to ensure that federal lease dollars are spent only in buildings where federal and other tenants have the right to choose multiple facilities-based telecommunications providers in order to secure diversity and redundancy in telecommunications services to better ensure continued communications during a disaster or provider-specific emergency.

Without this requirement, building access by facilities-based telecommunications providers would be at the discretion of the current or future building owner. Even if federal or commercial tenants chose a *single* telecommunications provider, that choice could be thwarted, and the landlord could choose a different carrier.

This requirement also is necessary to ensure that savings from the competitive procurement of local telecommunications services by the federal government can actually be realized—otherwise the chosen provider(s) may not be able to obtain building access on fair and reasonable terms.

Federal leasing dollars should not be showered on buildings that block, impede or delay telecommunications competition and thereby harm federal and other tenants—those dollars should be spent in a way that allows the federal government and other tenants to reap the benefits of the Telecommunications Act of 1996 and thus spurs the development of network facilities.

Even before the national security implications of access to diverse and redundant telecommunications service were highlighted, there has been bipartisan congressional concern to secure building access for telecommunications providers in buildings with federal tenants.

Last Congress, Senators Stevens, Hollings, Lott and Dorgan, and Congressmen Tom Davis and Rick Boucher, introduced legislation that would require, absent special circumstances, that federal tenants only lease space where telecommunications carriers can have nondiscriminatory access to them.

Congress, aware that the former Administration was considering the issuance of an Executive Order imposing a requirement similar to the one discussed here (the EO was drafted but never issued), adopted language last year in the Conference Report to accompany HR 4475, an appropriations bill, Report 106–940, noting that the conferees were “aware that . . . potential cost savings may be jeopardized by building access limitations for telecommunications providers.” The Conference Report noted the pendency of legislation on building access and then directed the executive branch to “identify building telecommunications barriers and take necessary steps to ensure that telecommunications providers are given fair and reasonable access to provide service to Federal agencies in buildings where the Federal government is the owner or tenant.”

President Bush, as Governor of Texas, signed landmark legislation going well beyond the modest step urged here of requiring that federal leasing dollars be committed only to buildings allowing facilities-based telecommunications carriers building access on fair, reasonable and nondiscriminatory terms so that they may serve a tenant who selects them. The Texas law signed by Governor Bush affords any tenant the right for a carrier with whom he, she or it contracts for service to obtain building access promptly on reasonable and nondiscriminatory terms. And it was implemented aggressively by the Governor’s appointees to the Texas Public Service Commission so as to deter landlords from thwarting consumer choice.

Access To Rights of Way

Timely and cost-effective access to municipal rights of way is also critical for the construction of alternative fiber optic networks. Too often municipalities delay this construction by attempting to charge unreasonable rates and impose unreasonable terms and conditions on this access. In conjunction with other telecommunications carriers—including long distance carriers, competitive local exchange carriers and incumbent local exchange carriers—TWTC has called for the FCC to intervene. The coalition has proposed the following recommended measures to promote reasonable access to public rights-of-way:

- Access to public rights-of-way should be extended to all entities providing intra-state, interstate or international telecommunications or telecommunications services or deploying facilities to be used directly or indirectly in the provision of such services (“Providers”).
- Government entities should act on a request for public rights-of-way access within a reasonable and fixed period of time from the date that the request for such access is submitted, or such request should be deemed approved.
- Fees charged for public rights-of-way access should reflect only the actual and direct costs incurred in managing the public rights-of-way and the amount of public rights-of-way actually used by the Provider. In-kind contributions for access to public rights-of-way should not be allowed.
- Consistent with the measures described herein and competitive neutrality, all Providers should be treated uniformly with respect to terms and conditions of access to public rights-of-way, including with respect to the application of cost-based fees.
- Entities that do not have physical facilities in, require access to, or actually use the public rights-of-way, such as resellers and lessees of network elements from facilities-based Providers, should not be subject to public rights-of-way management practices or fees.
- Rights-of-way authorizations containing terms, qualification procedures, or other requirements unrelated to the actual management of the public rights-of-way are inappropriate.
- Industry-based criteria should be used to guide the development of any engineering standards involving the placement of Provider facilities and equipment.
- Waivers of the right to challenge the lawfulness of particular governmental requirements as a condition of receiving public rights-of-way access should be invalid. Providers should have the right to bring existing agreements, franchises, and permits into compliance with the law.
- Providers should have a private right of action to challenge public rights-of-way management practices and fees, even to the extent such practices and fees do not rise to the level of prohibiting the Provider from providing service.
- The Commission should vigorously enforce existing law and use expedited procedures for resolving preemption petitions involving access to public rights-of-way.

About Time Warner Telecom

Company History

Time Warner Telecom began in 1993 as part of the Time Warner Entertainment Limited Partnership. The focus of the Company was to provide cable/phone services to residential and business customers using hybrid fiber coax (HFC) technology. After an extensive pilot program to test residential service, Time Warner Communications evolved into a company that offers business phone services over fiber-optic networks.

In 1997, the Company added voice circuit switches and began operating as a business CLEC. In 1998, Time Warner Communications became a separate entity from Time Warner Entertainment and began to operate as Time Warner Telecom Inc. During 1999, TWTC became EBITDA positive, acquired an ISP, built a national IP backbone and went public, offering 18,000,000 shares on the NASDAQ exchange. We trade under the symbol: TWTC. In August 2000, TWTC successfully bid, during an open auction bankruptcy proceeding, for most of the assets of GST Telecommunications. This allowed us to double the size of the company and extend our operating footprint throughout the Western United States. By end of 2001, TWTC offered telecommunications services over its own fiber optic networks in 44 markets in 21 different states.

Ownership Structure

We are very proud to carry the Time Warner name. As I described earlier, TWTC was initially created as division of Time Warner Entertainment. While Time Warner

Inc, now AOL Time Warner, owns 44% of Time Warner Telecom Inc. stock, Time Warner Telecom Inc. is an independently owned and operated company. The most important point, from both your perspective and mine, is that we have no financial backing from AOL Time Warner. We obtain the capital we need to do business the same way the rest of the independent CLECs obtain theirs, through debt and equity offerings in the financial markets and from operating cash flow.

Company Growth

During a time when the news is full of stories on bankruptcies and employee layoffs we are expanding our network and hiring new people. In 1996 TWTC had 500 employees, the majority of them located in the corporate headquarters in Littleton, Colorado. Today we have approximately 2500 employees and are providing service and employing people in 21 states. Time Warner Telecom's growth plans focus on geographic expansion, extension into new market segments and development of new data and Internet-based products and services. Our success to date is the result of building and deploying our extensive local and regional fiber optic networks all the way to the end user's building and providing a diverse physical alternative to the incumbent LEC. Our expertise is in selling complex network services that customers want and need over these networks. We execute and deliver on a sound business plan. We provide high quality broadband service to a diverse segment of the small, medium and large businesses in the country. In 1996 we had already constructed 5000 route miles. Today that has almost doubled to approximately local 9800 route miles. TWTC has constructed more route miles than any other local competitive carrier in the U.S. The fiber optic infrastructure we have built is important because it allows us to continue to layer more products and services on our network. One of the distinguishing characteristics of our network is that we have been laying this fiber in metropolitan areas; and the networks are large, averaging 400 route miles per city. We're building fiber where it is needed most, the last-mile. However, it is important that Congress recognize that the largest competitor in all of our markets, the local ILEC, has the ability to stymie our growth. Vigorous enforcement of the Act is the only elixir to the poison pill of anti-competitive behavior and abuse of market power.

Service Provided

This is how we do business. In every city that Time Warner Telecom lays fiber, the sales staff is required to prove in advance that there is business to be had. We don't build a network just to show growth, we build a network to provide a service that is desired. This serves our customers and our shareholders well because it ensures our continued viability in the marketplace. And I can assure you that there is demand for the service we provide. In many cases we supplement the services that the incumbent carrier provides. Often, companies will come to us for their new business or for a specific portion of their telecom needs. As we prove our ability to provide this service, they give us more and more of their business.

The fiber optic networks we have built allow us to offer our customers any technology, product or service solution. With virtually unlimited bandwidth, we can meet the rapidly changing demands of our customers. Our networks allow us to provide voice and data telecommunications services to a diverse customer base including public schools, private schools, universities, health care facilities, banks, the high-tech community, government agencies and military installations, law firms, public utilities, many small businesses, Internet Service Providers, insurance companies and most interestingly many of the telecommunications companies operating in the U.S.

Markets Served

Arizona:	Phoenix, Tucson
Colorado:	Denver
California:	San Diego, Los Angeles/Orange County, Santa Barbara, San Luis Obispo, Bakersfield, Fresno, San Francisco, Oakland, Sacramento
Florida:	Orlando, Tampa
Hawaii:	Honolulu
Georgia:	Atlanta
Illinois:	Chicago
Indiana:	Indianapolis
Minnesota:	Minneapolis
New Jersey:	Northern Jersey City
New Mexico:	Albuquerque
New York:	Albany, Binghamton, New York City, Rochester
North Carolina:	Charlotte, Greensboro, Raleigh, Fayetteville
Ohio:	Cincinnati, Columbus, Dayton
Oregon:	Portland
South Carolina:	Columbia
Tennessee:	Memphis
Texas:	Austin, Dallas, Houston, San Antonio
Washington:	Seattle, Spokane, Vancouver
Wisconsin:	Milwaukee

In Conclusion

The need for diversity highlights the important benefits of a competitive telecommunications market. There is no question that the telecom industry has been affected by the downturn in the economy. But the need for competition is more important now than ever. Businesses and government offices need access to diverse networks, and they need quality services at affordable prices. Policies that promote competition are critical, and strict enforcement of the 96 ACT remains the most important tool the government has to encourage competition.

Setting aside the advantages of competition, the attacks of September 11th and the demonstrated support by competitive telecom entrants such as Time Warner Telecom in restoring critical services, proves the strategic value of competitive fiber facilities based providers.

Thank you for the opportunity to testify before you today. I am happy to answer any questions.

Senator INOUE. Thank you very much, Ms. Herda.

Listening to the testimony of the two panels, it is apparent to me that the problems that existed on 9–11 are still with us. The word “interoperability” is still a desired goal. Some have mentioned training of professionals, and the unknown factor of what is it going to cost. We have no public policy to speak of at this moment.

So my question to all of you: Is there an agency in the government of the United States that can serve as a lead agency for the purposes you have articulated today?

Mr. CROTTY. Mr. Chairman, I believe that I cannot speak to interoperability of radio communications, which seems to be an emergency preparedness thing, but certainly the Congress of the United States and the FCC are best able to articulate policies that talk about the three things that the telecom providers were talking here at the table. That is for diversity and redundancy of our networks. Encouraging facilities-based competition can be done through pro-competitive policies and pro-investment policies. I think that would go a long way towards making our communications networks more robust.

Right now we have a policy which seems to favor resale. That is not a policy that has worked too terribly well in lower Manhattan.

When our network goes and other people are riding on that network, all the customers who are taking service from these resale providers, they are knocked out as well.

As the President of Time Warner mentioned, and this is also true of AT&T, which had fairly robust facilities in lower Manhattan, as did MCI WorldCom, those providers who have scale and scope and do have diverse networks assisted materially in the rapid response to what happened on September 11th. I would suggest that is something that ought to be continued by investment policies and regulatory policies, investment policies sponsored by Congress and regulatory policies sponsored by the FCC.

Senator INOUE. Ms. Herda.

Ms. HERDA. I would actually agree—I guess we do not do that very often, do we, as competitors? But I actually agree from our perspective, Congress and the FCC, for us as well the local PUC's too in dealing with the local municipalities. Obviously, being able to construct into the buildings is very important. You have to get permission to do that.

On September 11th and for quite a while after that, a lot of the standard intervals for those types of things were obviously lifted so that we could all get in there and provide the emergency services. Some of the things that I had suggested—that executive order would be very helpful for building access issues, to get permission from landlords, it sends the right message to the rest of the real estate community, that they need to let competitive providers into the buildings instead of trying to make money off of those services that are coming into the building. It would be much more beneficial for their customers to have access to multiple vendors.

Senator INOUE. Mr. Nash.

Mr. NASH. From the public safety standpoint, we currently are faced with the situation that the systems are locally owned and operated by individual police, fire, and EMS companies. A lot of the problem relates back to the American culture of local control, and the control over the radio system comes into that.

Nonetheless, over the last few years we have seen a number of efforts under way to bring together agencies to develop consolidated plans either on a regional basis or in some cases on a national basis. Currently within the FCC there is a Federal advisory committee operating known as the National Coordination Committee, looking primarily at the 700 megahertz band, but nonetheless we are having discussions about being able to bring together a plan for agencies to interoperate amongst themselves.

Furthermore, at the Federal level there is an effort going on known as the public safety wireless network, which is a joint effort of the Department of Justice and the Department of Treasury which again is looking at the, if you will, proliferation of different public safety radio systems, including at the Federal level, and what we can do to try to bring those systems together and provide for some cooperation and coordination between agencies as we come together in disasters like this.

Furthermore, again at the Federal level and dealing more, quite frankly, in the forestry conservation area, where we every year see tremendous fires, particularly out West, with many thousands of acres being burned down, the U.S. Forest Service, the Bureau of

Land Management, and the resource agencies have banded together and created a centralized cache of equipment and frequencies and plans based out of Boise, Idaho, which again we make use of at the local level.

So there are a number of different efforts going on, perhaps not as well coordinated as they should be, but a lot of efforts are out there going to try to bring together the interoperability problem.

Senator INOUE. Ms. Harris.

Ms. HARRIS. I would agree with both my colleagues to the left and the right of me as we look at what I think the FCC and Congress can help with in either executive order in a number of areas: one particularly, to make sure there is enough spectrum; two, to make sure that, from a cell-siting perspective, that we can get access and get it quickly. We did find that some of the regulations and bureaucracy that was removed in order to respond to the 9-11 crisis made it somewhat easier for us to get our COW's placed, etcetera. But the process in general can be cumbersome and very lengthy to get cell sites on the air. So I think that would be very helpful as well.

Senator INOUE. Mr. McLean.

Mr. MCLEAN. Mr. Chairman, the ComCARE Alliance believes that it will require unprecedented coordination between State, local, and Federal agencies. We have an opportunity with President Bush creating an Office of Homeland Security to have a focal point for the coordination. We have several models to look at. When the Congress and the President adopt a national telecommunications and technology priority, agencies across the Federal Government and in the State and local arena work together.

A prime example of that was in 1996 when this Committee and the Congress and the President said, we will connect schools and libraries to the information infrastructure, and agencies across the Federal Government—Department of Education, Department of Commerce, the Department of Agriculture—focused, FCC, focused efforts to achieve that goal.

With the Office of Homeland Security, we have an opportunity to say that we need to take emergency communications to a twenty first century level of connectivity. You can build on efforts, for example, that Senator Burns has started in his own State to be able to bring the parties together, and Senator Burns has a way of saying: check your jurisdictions at the door; let us just come around the table and work together and solve this problem. That is what needs to happen in all 50 States of this Nation.

Senator INOUE. Let me yield to Senator Burns.

Mr. CROTTY. Mr. Chairman, could I add one further point? As a resident of Manhattan and I have lived and worked there almost all my professional life, one thing you can do—there is a story in Time Magazine this week about a ten-kiloton bomb which was going to be planted in Manhattan. Speaking as a New Yorker and somebody who was intimately involved in the emergency response, I think it was terrible for the Federal Government not to share that information with the city so that the city could have done something about it, either creating some kind of isolation zone or communicating in some fashion or developing their own security arrangement.

After all, the City of New York responded to this terrible attack pretty much on its own. By the time FEMA showed up, we had many of the relief mechanisms already in place, up, functioning and operating, and operating very well indeed.

So for the Federal Government to have this information and not be able to share it with our elected authorities I thought was a terrible commentary on the sharing of information. I would hope that you would be able to do something about that in the future so that information between the Federal Government and the local government is shared on a more open basis. After all, when you talk to the Federal Government they say the local authorities, that we should be reporting information to them all the time. When it comes the other way around, the Federal Government is not very good at sharing information with local authorities. I certainly thought that was a major, major flaw in the Federal Government's involvement with New York City. They should have been sharing that information.

Senator INOUE. Senator Burns.

Senator BURNS. Thank you. I cannot imagine you would get all excited about a little old bomb like that.

Mr. CROTTY. Well, I am speaking now as a citizen who lives at 60th and First Avenue. I was concerned about that, yes.

Senator BURNS. I thank you for that information.

Chris McLean, of course, helped us set our summit up in Montana and I would recommend to our colleagues that they do something like that. We are moving forward, I think, and coordinating our E-911 and our first responders and moving right along, although the deployment of the technology, that is just a little bit slower than we would like. But nonetheless, I understand that there is also economics involved, and we will work our way through those, too.

Mr. Nash, as I mentioned in my statement, one of the most—well, I guess I did not even give my statement. Deployment of E-911 and of this service, deployment of this service, coordination between public safety and wireless operators to ensure it results in end to end systems that quickly and accurately locates wireless 9-1-1 calls, how would you characterize the progress that you are making?

Mr. NASH. At the moment the progress is somewhat disappointing. We see two sides of the problem. The carriers are moving along, but they also are repeatedly asking for waivers to extend the period of time they have to implement the technology. Some of that comes down to whether or not the solution they have selected, whether or not a vendor is able to supply that and it works. There are a lot of arguments that have come into it.

What concerns us from the public safety side is that their continually returning to the Commission asking for an extension of the time just pushes this out.

The other side of it is, from the public safety answering points of this, there is work that we also need to do to prepare the PSAP's to utilize this information. That requires an infusion of money, and a lot of PSAP's at the moment are short of cash in order to implement some of the new technologies, the mapping systems, the personnel that might be needed in order to implement that.

So there are really two parts to the problem. We are working on, from APCO's standpoint, on trying to equip the PSAP's in order to make use of this information. They need to do some work with their legislative and governmental organizations to acquire the funding to do it. But at the same time, we feel it is really necessary to keep the pressure up on the carriers, for them to be moving forward rapidly in selecting a viable technology to implement and start putting that in place so that we can make use of that.

It is vital information for our public safety people in order to respond to just the day to day emergencies that come up every day. More and more of those emergencies are being reported via wireline telephone—or wireless telephone, and we simply do not know where those people are to give them to help that they deserve.

Senator BURNS. I thank you for that. I think there is still some concern in Congress about the deployment.

Ms. Herda, I was interested in—and I have run into this before and I do not know how to approach this, because I am a strong believer in property rights and people should be able to do with their property and allow certain things on their property that they deem for themselves or whatever. Your permits for access in the buildings—sometimes the owner makes a deal with one company and denies the access of other companies.

Is there any merit in the Congress taking a look at those situations in light of emergency conditions, that there should be at least maybe two providers granted access out of how many wants it, but nonetheless there should be two?

Ms. HERDA. In light of emergency situations, you should always have at least two. It is interesting. Property rights issues are obviously a very sensitive issue when it comes to trying to get access into a building. The State of Texas has actually done a really good job in that regard in basically mandating a nondiscriminatory access into buildings. At a minimum what it does is it gives us a negotiating position with the building owners.

We have never said that we needed to go into the buildings for free, unless the local exchange carrier is in it for free. But we have been always willing to pay with reasonable rates, to pay for the access into the buildings and for the distribution within the buildings. So it does not cost the building owners any money to have us in there and in fact it adds additional diversity, and it obviously has a tremendous amount of value in terms of emergencies.

If the government mandated that there were at least two competitors in a building at a minimum, without putting any restrictions on having more in there, it would certainly go a long way. I think that, at a minimum, if the government mandated in their own buildings, in the buildings that the government leases today—and there are many, many of those, and some of them are multi-tenant buildings, too, that serve public companies—private companies, rather, as well, that would absolutely go a very long way to moving the real estate community in that direction. I think that would be an excellent idea.

Senator BURNS. I want to thank this panel because not only did they give us some idea of the challenges that they faced during 9–11 in New York City and of course here in Washington, D.C., and

also the things that they have recommended through their testimony on maybe some actions that the government should consider and some answers to some questions. I appreciate that.

I look forward to reading some other testimony that we are going to take on this thing, Mr. Chairman. But that is basically all the questions I have. I appreciate the thoroughness of your testimony and your statements before this Committee.

That is all I have. I have got a 4:30 appointment. Besides that, if we do not let these people get out of here everybody is going to be asleep out there. Have you noticed folks nodding off?

Senator INOUE. Well, I am going to keep the record open for 3 weeks just in case you have any additional statements you would like to submit.

I would also like to advise my Committee as to whether they would like to submit questions to you. I regret that they were not here, but, as I pointed out earlier, there are two events that made this not possible. But I wish to join my colleague in thanking all of you for your testimony. For a moment I thought I saw the dark shadow of Tauzin-Dingell over us.

Mr. CROTTY. We were told to stay away from it.

[Laughter.]

Senator INOUE. But it is good to see competitors sitting together in one panel and talking to each other.

So with that, this will not be the first and last hearing on this matter, I can assure you, because I for one am still not convinced that we are ready for another big one, and it may happen. I hope not.

So with that I thank you all very much.

[Whereupon, at 4:37 p.m., the Subcommittee was adjourned.]