S. HRG. 107–1118

RESPONSE OF THE TECHNOLOGY SECTOR IN TIMES OF CRISIS

HEARING

BEFORE THE

SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

DECEMBER 5, 2001

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

U.S. GOVERNMENT PRINTING OFFICE

89–682 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

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

ERNEST F. HOLLINGS, South Carolina, *Chairman*

DANIEL K. INOUYE, Hawaii	JOHN McCAIN, Arizona
JOHN D. ROCKEFELLER IV, West Virginia	TED STEVENS, Alaska
JOHN F. KERRY, Massachusetts	CONRAD BURNS, Montana
JOHN B. BREAUX, Louisiana	TRENT LOTT, Mississippi
BYRON L. DORGAN, North Dakota	KAY BAILEY HUTCHISON, Texas
RON WYDEN, Oregon	OLYMPIA J. SNOWE, Maine
MAX CLELAND, Georgia	SAM BROWNBACK, 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*
MARK BUSE, *Republican Staff Director*
JEANNE BUMPUS, *Republican General Counsel*

SUBCOMMITTEE ON SCIENCE, TECHNOLOGY, AND SPACE

RON WYDEN, Oregon, *Chairman*

JOHN D. ROCKEFELLER IV, West Virginia	GEORGE ALLEN, Virginia
JOHN F. KERRY, Massachusetts	TED STEVENS, Alaska
BYRON L. DORGAN, North Dakota	CONRAD BURNS, Montana
MAX CLELAND, Georgia	TRENT LOTT, Mississippi
JOHN EDWARDS, North Carolina	KAY BAILEY HUTCHISON, Texas
JEAN CARNAHAN, Missouri	SAM BROWNBACK, Kansas
BILL NELSON, Florida	PETER G. FITZGERALD, Illinois

C O N T E N T S

RESPONSE OF THE TECHNOLOGY SECTOR IN TIMES OF CRISIS

WEDNESDAY, DECEMBER 5, 2001

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

The Subcommittee met, pursuant to notice, at 9 a.m. in room SR–253, Russell Senate Office Building, Hon. Ron Wyden, Chairman of the Subcommittee, presiding.

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

Senator WYDEN. The Subcommittee on Science, Technology, and Space will come to order. Today the Subcommittee on Science, Technology, and Space of the Senate Commerce Committee begins a series of hearings to examine technology and science issues stemming from the events of September 11th, 2001.

Just as John F. Kennedy gave America's youth a forum for public service, I believe now is the moment that government should throw open its doors to the ideas, the creativity and the energy of our best scientists and technology experts willing to fight the terrorist threat. It is time to mobilize a generation raised on information technologies to respond to terrorism. Let us use the latest innovations in fields like biometrics to help prevent terrorist acts like those of September 11th.

The Subcommittee's first hearing on this subject is going to focus on information technology. When terrorists struck New York and the Pentagon, telecommunications and information networks were flattened by the blow. Land-line and cellular communications were hit hard by an incredible spike in volume, as well as strikes to key assets such as cell towers on the Trade Center and the Verizon hub near Ground Zero. Many wireless calls, including those of rescue workers, simply couldn't get through.

As emergency workers moved in, they were also hindered by the fact that their communications systems were incompatible and simply couldn't work together. In a hearing before this Subcommittee, a fire chief responding to the attacks of 9/11 said that, at times, his only means of communicating directions to firefighters on the front lines were handwritten notes delivered by runners on foot. These courageous emergency workers have told us that the communications breakdowns made their job more difficult and more dangerous.

There were also organizational challenges: the inability to track to which hospitals victims were sent, the inability to match would-be volunteers with needs, and the lack of backup systems for organizations overwhelmed with information.

A true hope for overcoming these obstacles is to tap the potential of scientists and technology experts. The government must create a clear structure to accept and utilize the treasure trove of technological counsel, state-of-the-art equipment, and hands-on help that is available. The Nation's technology leaders tell me that they can contribute most effectively if they have organization and a clear chain of command. Key Federal agencies say they're willing to establish a single point of contact for technology companies and a consistent, governmentwide policy for creating that necessary organization. I am determined to hold both the Congress and the entire Federal Government accountable to get this job done quickly.

There are a variety of ways that this could be tackled.

I believe the government should consider establishing the technology equivalent of the National Guard. I describe it as a National Emergency Technology Guard, or NETGuard, a cadre of volunteers with extensive technology expertise to move in in a moment's notice, not just to fix what's broken, but to create whatever systems are needed most. That could mean repairing and recreating compromised communications systems, setting up command centers, or setting up databases to track the missing and the injured.

There are other roles that such a volunteer force could play. The group could help establish and maintain a strategic technology reserve. Companies could commit to lend their latest and best hardware and software whenever disaster strikes, with trained volunteers able to set it up and implement it in minutes. A Strategic Technology Reserve would be a virtual, as well as a physical, stockpile.

This volunteer force could play a preventive role, as well, offering local officials advice on how to set up their computer and communications systems to minimize vulnerability to hacking and physical attacks. They could also assist in creating and executing emergency drills and maintaining an ongoing database of volunteers and their scientific and technological expertise.

There are other policy issues to consider. This Subcommittee has been told that Federal rules prohibit some government agencies from accepting donations of state-of-the-art equipment, no matter how urgent the need to fight terrorism. We have learned that there are restrictions on private companies sharing information, even in a crisis. We have learned that there is an urgent need for policies that encourage compatibility between emergency communications systems, to keep those first responders from having to use runners when disaster strikes.

It is time to create a high-technology reserve, a talent bank that serves as a new force to confront a new threat. This can be done without creating big new bureaucracies, and there ultimately should be a modest role for the Federal Government. This Subcommittee is going to work on a bipartisan basis with the Administration and our colleagues in the Congress to help our scientists and technology experts marshal their ingenuity and talents to respond to terrorism.

Before I go to our witnesses, I want to offer a couple of special thank yous. To accomplish anything significant in the technology and science field, it is absolutely critical to have bipartisan support. And I want to express my personal appreciation to the Bush Administration, to Richard Clarke, to Dr. Marburger, and to Joe Allbaugh. The Administration has been consistently supportive in efforts to examine these ideas, and we are appreciative. I also want to thank Andrea Richet, founder of the Charity Mouse, which helps wire public schools, who has been very instrumental in helping this Subcommittee examine these issues.

We have a distinguished panel of witnesses today. Dr. Joe Allbaugh, from the Federal Emergency Management Agency; Dr. John Marburger, Director of the Office of Science and Technology Policy; Craig McCaw, a pioneer of the cellular telephone industry; Julie Coppernoll, of Intel; Joe Sandri, of Winstar; Stephen Rohleder, of Accenture; Roger Cochetti, of VeriSign; and Will Pelgrin, Executive Commissioner of the New York Governor's Office of Technology.

Before we go to our witnesses, I want to recognize my friend and colleague, Senator Allen—it has been a pleasure to team up with him already on a number of technology issues—for any comments that you would like to make.

STATEMENT OF HON. GEORGE ALLEN,
U.S. SENATOR FROM VIRGINIA

Senator ALLEN. Thank you. Thank you, Mr. Chairman.

Good morning to you all. Mr. Chairman, I want to begin by thanking you for calling this hearing and for your leadership on this very important issue. Let me make my accolades again to the Chairman, or did you get it?

[Laughter.]

Again, Mr. Chairman, thank you for your leadership and good morning to everyone here. I do also want to express my gratitude to the witnesses who you list off as an outstanding list of individuals headed by Dr. Marburger and Director Allbaugh and Mr. McCaw and a variety of companies that are very important in the diverse technology industry to help us do a better job in the future.

This morning, I hope, Mr. Chairman, to learn from the September 11th terrorist attacks. Whenever you're attacked, you have to do an analysis of how did it happen, what was the response, and how can we do a better job in the future, and also where we need specifically to do a better job in the United States in the future if there are such national emergencies, whether they are such terrorist attacks, whether they are on buildings or other attacks, which we may not want to say publicly, but have to have contingencies before reaction and response if they should befall our Nation.

As the Chairman mentioned, this attack on September 11th clearly was something that devastated our country psychologically, but the confusion that arose right after the attack played havoc with our Nation's telecommunications infrastructure. The collapse of the World Trade Center left hundreds of thousands of New Yorkers without either phone or television capabilities. We find here that—a lot of times—most people found out about the attacks lis-

tening to the radio or watching TV before there was even an announcement by the President. There was going to be an announcement by the President that the attacks had occurred, the bombing was starting in Afghanistan. The television and phone capabilities are the way we communicate and react, and there's a great deal of confusion if that is not capable.

The cellular phone system was overloaded in New York, Virginia and DC. Those of us who were living here—everyone—were worried about what was going on. We were trying to communicate and coordinate, and the cell coverage was obviously overloaded creating communications problems for people who wanted to know how their loved ones were, but also it was a problem for emergency services. The communications breakdown caused confusion, it heightened concerns for many Americans. As the Chairman Senator Wyden enunciated very clearly, the fire, the rescue, the police organizations and coordination all were harmed by that.

The aftereffects of this disaster hampered relief efforts in many emergency aid organizations. The Red Cross reported that its toll-free emergency lines were inaccessible to thousands of callers.

Now, Mr. Chairman, I see the purpose of this hearing today is to investigate what Congress can do to help prevent this kind of communications breakdown and its aftereffects in the future. I was heartened to see that, regardless of any governmental action, that so many stories of generous companies such as Intel, Verizon, Winstar, Accenture, and Cingular volunteered both staff and equipment to restore communications in New York and in Washington, DC. The Nation thanks you for your timely assistance during this emergency.

However, our communications should be capable of performing better in the future. It is important to ensure that our telecommunications network remains functional after an attack, and I look forward to hearing how the Federal Government can better coordinate with, not tell, private companies, but coordinate with private industry to get a quicker and more efficient response for future emergencies. In addition, I think we ought to examine the telecommunications and Internet networks to make sure that they are designed to remain functional in response to any critical attacks or strikes.

Chairman Wyden has also proposed the National Emergency Technology Guard, or NETGuard, that will have the capability to respond to future crises. I look forward to working with you, Mr. Chairman, on this issue, and I especially like the idea of an all-volunteer force based on the best and the brightest minds in the technology workforce of the United States. Leaders in the technology sector have made the United States a world leader in technology, and I would like to certainly listen to their ideas on this issue. I think it is also important to make sure that the government does not duplicate the existing efforts in the private sector and works within the existing Federal critical infrastructure protection programs.

Additionally, I hope we can continue to support the government efforts to work with the private industry to conduct a post-attack analysis of the collapse of the World Trade Center and the surrounding infrastructure. That's more of an engineering—physical

engineering matter, but this analysis will help to develop, I hope, new guidelines to assess the vulnerability of the existing system and improve future safety and security of major buildings and facilities, including the physical and technological infrastructure.

In sum, Mr. Chairman, technology can and must play a major role in helping prepare for future crises, and we should ensure that the diverse high-tech sector is mobilized to help prevent and respond to any future crisis. And so, again, I thank you, Mr. Chairman, for holding this hearing, and I look forward to hearing and learning from the inside testimony of these esteemed, respected witnesses. Thank you, Mr. Chairman.

Senator WYDEN. Well, thank you for that excellent statement. And, as we have done on a variety of issues already, we're going to be working closely together, and I thank you very much for your statement.

Gentlemen, as you can see, there's bipartisan support already established on these key questions. We thank you. You both have been extremely cooperative.

By your own agreement, I think we will begin with Dr. Marburger. I know both of you have tight schedules. Dr. Marburger, why don't you proceed as you wish? We will make your prepared statement a part of the record in its entirety.

Welcome.

STATEMENT OF DR. JOHN H. MARBURGER III, DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Dr. MARBURGER. Thank you very much, Mr. Chairman and Senator Allen. I'm pleased to have the opportunity to testify on the response of the science and technology sector to this war on terrorism. The Office of Science and Technology Policy is playing a significant role in this response, and I want to describe this for you today. My testimony will deal with a somewhat longer-range, longer-term response, although still somewhat short-term, as opposed to Director Allbaugh's function of dealing with immediate responses to situations.

Those of us who are engaged in the Federal response to these attacks have been very impressed by the avalanche of offers to assist, from Americans who want to help in any way they can. And I have attempted to grasp the scope of this volunteered assistance and to shape the Federal interface to mobilize it effectively in support of the Nation's war against terrorism.

So during these few months that I have been in office, I have been meeting with industry associations, non-profit groups, umbrella organizations for universities, and scientific societies, the national academies. And we've attempted to establish and have succeeded in establishing well-defined relationships with these entities to receive input from and provide Federal guidance to their own antiterrorism projects and initiatives. At the same time, we've exercised our congressional and Executive mandates to coordinate activities within the Federal agencies relevant to national issues, relevant to terrorism issues.

OSTP is consequently in a position to call on organizations, both external and internal to the Federal Government, as we provide

technical support to the Office of Homeland Security and other offices responsible for different aspects of this war against terrorism.

And I do want to acknowledge here my thanks to you for raising my consciousness of the need to reach out in this way by your remarks during my confirmation hearing, Mr. Chairman. I know that you've been thinking about how to enlist the Nation's considerable technical expertise to address national challenges, the current war against terrorism and homeland security being the most immediate. And consequently, I've acted on this idea of yours to recruit talent in a systematic way. And it has been a topic of discussion in every one of the meetings that I mentioned earlier.

Some of the organizations I met with are umbrellas for entire sectors of science, industry and higher education. And I will just give one example, and you can read the others in my written testimony. The American Counsel on Education provides a very efficient and rapid means of communicating with the entire higher education sector. Its President, Dr. David Ward, has encouraged positive action by every branch of our very complex post-secondary education system through weekly communications by e-mail that go across the entire post-secondary sector. Also, the national academies have been quite concerned about terrorism issues and have created a committee specifically to interact with Federal agencies on terrorism, and we have been attempting to provide a uniform interface with their committee.

As a result of my meetings with these organizations, I've concluded that a virtual science corps already exists and that creative use of existing public- and private-sector mechanisms can help make present networks stronger and more effective.

To take advantage of these mechanisms, I have acted to coordinate Federal agency activities related to terrorism and provide a coherent interface between the Federal Government and the nongovernmental organizations described above. I won't go into detail about all my activities, which are recorded in the testimony, but I began in late October by calling a meeting of chief science officials from more than 15 Federal agencies to discuss the role of science and technology in combating terrorism, and we have been working together since then to take advantage of crosscutting mechanisms that already exist to make these volunteer efforts more effective.

Under the structure of the National Science and Technology Council, for example, I am establishing an interagency antiterrorism task force with several working groups to address broad categories of issues. One of these task forces is a technical response team which will be an action-oriented team that will establish small subgroups on an ad hoc basis to grapple with emergencies as they arise. The team will serve as a clearinghouse for technical reviews of the many incoming proposals on technologies related to homeland security. And it is important that we assess these proposals for scientific merit and refer them, as necessary, to the appropriate agency or organization for further review, et cetera.

In this connection, we have been working closely with the National Coordination Office for Information Technology R&D—it's NCOITRD—in the Department of Commerce to respond to these offers. This organization will be developing a repository database of non-government people that have offered their expertise to help the

Federal agencies counter terrorism. Contact information and relevant expertise will be available on a password-protected Web site for access by authorized persons in the Federal Government to connect critical human resources to the important work of both agencies and the national academies, which will also have access.

As a case study of how virtual science corps can work within the context of the Federal agencies, I want to mention the technical support that our office, OSTP, is providing to the Office of Homeland Security. During the fourth week of October, Governor Ridge called me to ask that OSTP provide technical support for the treatment of U.S. mail potentially contaminated by *Bacillus anthracis.*

The day after his phone call, I convened an interagency meeting with chief science officials and U.S. Postal Service to ascertain the technical issues that the postal service was encountering. My ability to act quickly was enhanced by the fact that I had already taken steps to call together the chief scientists of a larger number of agencies. This action led to the formation of an interagency technical team that, within days, began evaluating the irradiation facilities at Lima, Ohio and Bridgeport, New Jersey.

The point here is that when the request came to OSTP, we were able to assemble an interagency team—five agencies were involved—quickly and formulate a plan of attack that has worked. In this case, most of the needed expertise existed already within Federal agencies and the U.S. Postal Service, but some of our meetings on the mail issue have included experts from higher education and non-governmental organizations identified by the participating agencies. And in the future, I expect it will be necessary to continue to reach out beyond the agencies through the network of non-governmental organizations to tap the immense reservoir of talent that exists in the private sector.

OSTP has a broad role for coordination and partnership building, but it does not play an operational role. We don't give grants. We don't have line—or responsibility, as FEMA does, for execution. We do not compete with other agencies. We do not duplicate agency expertise, but rather we act as coordinators and recruiters of technical expertise in the service of governmental policymakers and line managers. Because of our historical crosscutting role, I believe OSTP can do this rapidly and efficiently.

I have a section in my written statement on preparedness, and some specific questions and responses that you may be interested in that I will omit in the interest of time.

An overarching goal for all of our efforts that I have described is coordination of the activities of all of those who can contribute to ensuring that our Nation is safer. We're drawing upon the technical expertise housed in our science and technologies agencies, making sure that relevant information and test results are disseminated to the appropriate parties and preventing duplication of effort. I have been very impressed with the breadth and depth of scientific and technological resources available within the Federal Government to address the major challenges we are facing today, great as they are, but I'm just as certain that those resources will not be used to their greatest effect unless we join forces and resolve technical issues together with all of the expertise we can bring to bear upon that.

Thank you, Mr. Chairman, for this opportunity.
[The prepared statement of Dr. Marburger follows:]

PREPARED STATEMENT OF DR. JOHN H. MARBURGER III,
DIRECTOR, OFFICE OF SCIENCE AND TECHNOLOGY POLICY

Good Morning Mr. Chairman and Members of the Subcommittee. I am pleased to have this opportunity to testify on the response of the science and technology sector to the war on terrorism. OSTP is playing a significant role in this response that I want to describe for you today.

OUTREACH

Those of us engaged in the Federal response to the terrorist attacks have been impressed by the avalanche of offers to assist from Americans who want to help in any way they can. During my brief tenure as Director of OSTP, I have endeavored to grasp the scope of this volunteered assistance, and to shape a Federal interface to mobilize it effectively in support of the nation's war against terrorism. To this end, I have been meeting with industry associations, non-profit groups, umbrella organizations for universities and scientific societies, and the National Academies. OSTP has established well-defined relationships with these entities to receive input from and provide guidance to their own antiterrorism projects and initiatives. At the same time, OSTP has exercised its congressional and executive mandates to coordinate activities within the Federal agencies relevant to terrorism issues. OSTP is consequently in a position to call on organizations external and internal to the Federal Government as we provide technical support to the Office of Homeland Security, and other offices responsible for different aspects of the war against terrorism.

I wish to acknowledge here, with gratitude, that my awareness of the need to reach out in the way I have described was quickened by your remarks, Mr. Chairman, during my confirmation hearing. I know that you had been thinking about how to enlist the nation's considerable technical expertise to address national challenges—the current war against terrorism and homeland security being the most immediate. Consequently, I have acted on this idea of yours to recruit talent in a systematic way. It has been a topic of discussion in every one of the many meetings I described above.

Some of these organizations are umbrellas for entire sectors of science, industry, and higher education. The American Council on Education, for example, provides a very efficient and rapid means of communicating with the entire higher education sector. Its President, Dr. David Ward, has encouraged positive action by every branch of the complex post-secondary educational system through weekly communications. The American Association of Universities provides more direct access to the leaders of the institutions that perform most of the nation's federally sponsored research. The National Association of State Universities and Land Grant Colleges is a link to the entire set of public universities, which carry out important research and extension services throughout the nation. The National Academies for Science, Engineering, and Medicine provide similar access to the nation's research community, as do the various disciplinary professional societies such at the American Physical Society, the American Chemical Society, etc., and their umbrella organization, the Council of Scientific Society Presidents. The officers of these organizations have expressed a willingness to designate a point of contact for terrorism issues, and in some cases they have formed committees and working groups to address specific issues such as bioterrorism. The National Academies, in particular, have created a committee specifically to interact with Federal agencies on terrorism.

As a result of my meetings with these organizations, I concluded that a "virtual science corps" has already come into existence, and that creative use of existing public and private sector mechanisms can help make present networks stronger and more effective.

INTERAGENCY COORDINATION

To take advantage of these mechanisms, I have acted to coordinate Federal agency activities related to terrorism, and provide a coherent interface between the Federal Government and the non-governmental organizations described above.

In October, I called a meeting of chief science officials from more than 15 agencies to discuss the role of science and technology in combating terrorism. Several representative agencies made presentations on their current antiterrorism-related activities, and all were asked for additional input to follow up the meeting. I convened a second meeting of this group in November to discuss current activities of OSTP and the formation of a new antiterrorism task force under the National Science and

Technology Council. These meetings gave science officials from various agencies an opportunity to interact and discuss areas of potential cooperation. It also provided a data base of contacts that could be immediately contacted when necessary. Representation by other offices in the White House in these and other terrorism-related meetings varies but generally includes: OMB, Office of Homeland Security, Domestic Policy Council, Office of the Vice President, and Cabinet Affairs.

Under the structure of the National Science and Technology Council, I am establishing an interagency Antiterrorism Task Force with several working groups to address broad categories of issues. The four categorical working groups focus on Biological/Chemical Detection and Response; Radiological/Nuclear/Conventional Detection and Response; Protection of Vulnerable Systems; and Social, Behavioral, and Education Sciences. We are establishing a Technical Response Team as a fifth working group. This action-oriented team will establish small subgroups on an ad hoc basis to grapple with emergencies as they arise. The team will serve as a clearinghouse for technical reviews of the many incoming proposals on technologies related to homeland security. It is important that these proposals be assessed for scientific merit and referred, as necessary, to the appropriate agency or organization for further review, feedback, and action as appropriate.

Many of these proposals have come directly from individuals, and many individuals have volunteered their services to assist in the war against terrorism. In this connection, we have been working closely with the National Coordination Office for Information Technology R&D (NCOITRD) in the Department of Commerce to respond to these offers. The NCOITRD will be developing a repository/data base of non-government people that have offered their expertise to help the Federal agencies counter terrorism. Contact information and relevant expertise will be available on a password-protected website for access by authorized persons in the Federal Government to connect critical human resources to the important work of both agencies and the National Academies.

HOMELAND SECURITY TECHNICAL SUPPORT

As a case study of how a "virtual science corps" can work within the context of the Federal agencies is the technical support OSTP is providing to the Office of Homeland Security. During the fourth week in October, Governor Ridge called me to ask that OSTP provide technical support for the treatment of U.S. mail potentially contaminated by *Bacillus anthracis*. The day after his phone call I convened an interagency meeting with chief science officials and the U.S. Postal Service to ascertain the technical issues that the Postal Service was encountering. This led to formation of an interagency technical team that within days began evaluating the irradiation facilities at Lima, Ohio, and Bridgeport, New Jersey. The key point is that when the request came to OSTP, we were able to assemble an interagency team quickly and formulate a plan of attack that has worked. In this case, most of the needed expertise existed within Federal agencies and the U.S. Postal Service. Some of our meetings on the mail issue have included experts from higher education identified by the participating agencies. In the future, I expect it will be necessary to reach out beyond the agencies through the network of non-governmental organizations to tap the immense reservoir of talent that exists in the private sector.

Congress has mandated that OSTP establish partnerships across Federal, state, and local levels, as well as fostering public-private partnerships in general, and this role may be of special value in meeting the diverse challenges of homeland security. OSTP does not play an "operational" role that would compete with agencies, and we do not duplicate agency expertise. Rather we act as coordinators and recruiters of technical expertise in the service of governmental policymakers and line managers. Because of our historical cross cutting role, we can do this rapidly and efficiently.

PREPAREDNESS

Last month, the President signed an Executive Order to establish a Presidential Task Force on Citizen Preparedness in the War on Terrorism. This task force is cochaired by the heads of the Office of Homeland Security and the Domestic Policy Council and is to identify, review, and recommend appropriate means by which the American public can enhance the nation's defenses against terrorism through voluntary actions. I have taken the President's message forward in meetings with the scientific and technical community and found especially strong interest in supporting State and local public health and safety officials in combating possible terrorist attacks within the United States.

Mr. Chairman, I know you have been an articulate advocate of the idea that there should be a national volunteer organization of trained and well-coordinated IT professionals from U.S. technology companies. And that they would stand ready with

computer equipment, satellite dishes, wireless communicators and other resources to recreate and repair compromised communications and technology infrastructures.

While there are many associated issues that will need to be considered, let me however suggest the following:

1. It seems logical to have a diversity of means for ensuring communications, e.g., satellites as well as land lines; 2. We should encourage voluntary preparedness, such as the IT disaster recovery procedures, which helped so many firms return to business quickly after September 11th; 3. We should promote voluntary standards that enhance the effective coordination of disaster responses, such as the U.S. National Grid map standard for geospatial information systems;[1] and 4. We need to pay attention to protecting our "invisible infrastructure," the radio spectrum, which enables public safety services like the Global Positioning System and E–911 for wireless communication.[2]

I believe that having a diverse portfolio of communication choices, common sense preparedness, standards and protocols for working together, and reliable public safety services will help enable us to weather and defeat any terrorist attacks on our IT infrastructure.

CONCLUSION

An overarching goal for all of the efforts I have described is coordination of the activities of all those who can contribute to ensuring that our Nation is safer. We are drawing upon the technical expertise housed in our science and technology agencies, making sure that relevant information and test results are disseminated to the appropriate parties, and preventing duplication of effort.

In the short time I have been in this position, I have been impressed with the breadth and depth of scientific and technological resources available within the Federal Government to address the major challenges we are facing today—great as they are. But I am just as certain that those resources will not be used to their greatest effect unless we join forces and resolve the technical issues together.

The CHAIRMAN. Dr. Marburger, thank you. Your testimony was very helpful, and we'll have some questions in a moment.

Director Allbaugh.

STATEMENT OF HON. JOSEPH M. ALLBAUGH, DIRECTOR, ACCOMPANIED BY RON MILLER, ASSISTANT DIRECTOR, FEDERAL EMERGENCY MANAGEMENT ADMINISTRATION (FEMA)

Mr. ALLBAUGH. Thank you, Mr. Chairman. Chairman Wyden, thank you for the opportunity to be here this morning. Senator Allen, always great to see you. Senator Nelson, good to see you, sir.

I don't have any prepared remarks, but I do have several points that I think I should make, and then I would be happy to respond to any of your questions.

I do appreciate the Subcommittee's willingness to take on this very tough issue in the area of communications and technology. A lot of these problems, quite frankly, have existed prior to the September 11th attack at the Pentagon and in New York City. And in the world of first responders, we see these types of problems crop up every time there is an incident.

As you know, as a result of those attacks, particularly in New York City, the New York City Fire Department lost its entire leadership command structure, so communication was even inhibited further by the fact of years and years of experience vanished in the blink of an eye. At the Pentagon, we had—if you can say we were luckier, but the site was more restricted, so the Arlington and Alex-

[1] The USNG standard for uniform presentation of geospatial information is now being voted on for adoption as part of the National Spatial Data Infrastructure by the FGDC Steering Committee.

[2] E–911 enables emergency services to locate mobile phones placing 911 emergency requests.

andria Fire Departments, along with Urban Search and Rescue Teams from Montgomery County and Fairfax County didn't have to walk, you know, 12 miles to have a conversation with someone who was in the command structure.

Facilitating orders, decisions that need to be communicated effectively, will do more to save lives than just about anything that I can think of and that I have come across in the short 10 months I've been in this position. I would like to speak specifically beyond those to particular problems and several others that I believed hindered our ability to communicate on September 11th, which you should be aware of.

In New York City, the Emergency Operations Center, where they had spent quite a bit of money—New York City had spent quite a bit of money establishing and Building 7, a first-class state-of-the-art operations center, where they brought in all the city agencies, all the Federal agencies, the State agencies, to coordinate and cooperate under one roof—was decimated. So as a result, we were not able to work out of their emergency operations center. Our team quickly helped the city establish a new operations center at Pier 92, and then we had to establish our own operations center significantly down the street from where action central was, which was near Ground Zero, lower Manhattan.

The loss of local communications infrastructure required us, losing that building, to rely upon satellite communication, wireless networks, satellite phones. It is most imperative when an incident is ongoing that we have accurate information. And if you can't talk to individuals who are on the ground at the site, you do not make very wise decisions and oftentimes put further lives in jeopardy and at risk.

I activated 8 of our 28 Urban Search and Rescue Teams, national organizations, sent 8 of those two New York. We had 3 or 4 initially at the Pentagon. And it was frustrating, especially the first week—a lot of chaos. Individuals, as you alluded to, Mr. Chairman, had to communicate via messengers, runners, passing of notes. The system was totally overburdened. Except for our own infrastructure, using satellites, we virtually had no way to communicate, other than face-to-face, which takes time and, again, puts further lives at risk.

Another issue that we had to deal was the self-dispatching of several emergency response organizations. And because we didn't have a way to communicate with those individuals, they would show up willy-nilly, quite frankly, adding a greater burden to an already stressed infrastructure. I would say that, in particular, and in regard to New York City, that massive event, had it happened anywhere else, the local responders would have been totally overwhelmed. But, fortunately, New York City, given its size—8 million people, 14,000 firefighters, 40,000 police officers—they had the infrastructure to make it work in spite of the communications breakdowns.

Private information technology donations were helpful, but not greatly helpful. And there were often strings attached. And I think the Subcommittee should be aware of those strings. Oftentimes, we would have individuals come in our operations center at Pier 94, offering technology that was not exactly state-of-the-art, wasn't as

current as what we have at FEMA or New York City's fire and police department. And it basically consisted of excess or discontinued items that some companies, quite frankly, wanted to just get out of their inventory.

A lot of the so-called "free" products and services came with a bill at the end of the initial response phase of the incident, particularly in New York City, less so at the Pentagon. Since it was, essentially, a military establishment, we could control access in a much greater way, which helped all of those first responders. Other equipment was free to acquire, but there was money attached at the end to maintain that particular service afterwards.

There is no centralized database to manage donated goods or services throughout the Federal Government—nowhere—so everyone would show up at the front door wanting to donate. We didn't have a system. We had to create a system in conjunction with the City of New York and the State of New York, which works right now, but it is not the type of system that we need as a Federal entity responding to these events.

There really wasn't a centralized go-to desk staffed by industry individuals who could serve as brainpower or a brain trust for immediate needs—SWAT teams or other teams of experts. We could have used, in New York City, industry experts to come in on that first day and help us set up a database to track, not only those individuals who were missing, all the goods and services that were being donated. It was just total chaos, and there's no other way to describe it. Eventually, weeks after the incident, we were able to put together a database, but it would have been helpful to draw upon the brainpower out here at the corridor or in Silicon Valley or anywhere in the United States to help us do a better job of managing the massive amounts of information that we were deluged with and at the same time continuing with our principal responsibility of saving lives and protecting property.

And all of these things together, they're really not, by themselves, technology problems. These are problems that ultimately cost lives. We owe it to the American people to bring together the best available technology to the table when a disaster strikes. And I think we, at FEMA, are on the cutting edge, as much as our budgets will allow, as much as the technology that is affordable will allow. We have access to that, and so we can save lives and property to the maximum extent possible.

Public and private sector IT professionals do need to come together, and so I do appreciate this opportunity to, not necessarily force, but, in a cooperative spirit, ask everyone to the table, in a smart, coordinated fashion, to talk about delivering state-of-the-art technical solutions. This Administration, through Governor Ridge, Homeland Security, others are working on ways to deal with the issue. We, at FEMA, are staffing and supporting these efforts, and I look forward to a continuing and coordinating effort with this Subcommittee and the Office of Homeland Security as we move forward to find solutions.

I brought with me today one of my assistant directors, Ron Miller, who is responsible for all of our IT, from top to bottom, at FEMA. He is available to answer any technical questions which probably will be beyond me, Senator, quite frankly, but I can surf

the Net and turn on my computer, contrary to what my staff says. He's been working on a variety of issues dealing in this arena. He's been onboard for a short period of time. He is my go-to person at any one of these incidents that we have. He has a fabulous staff, well-trained.

And I thank you for the time to appear this morning, and I look forward to trying to answer any of your questions, Senator.

Senator WYDEN. Director Allbaugh, thank you. And Senator Allen and I will divide up the time. I know both of you have just a few minutes at this point.

It seems to me that the challenge is all about the nuts and bolts of organizing this effort. We know the science and technological talent is out there. Both of you have said you are very interested in it. We essentially need the system put in place to get it done. For example, to have a system so as to distinguish between the many, many companies who want to help and are willing to make satellite trucks, wireless systems, computers, routers, and all of this technology available would be very helpful, along with how to distinguish that from some of those that you, Director Allbaugh, have talked about that really were just looking, perhaps, to discard something or figure out a way to make a buck.

I think the vast majority of people in the private sector want to help and have good motives. Now it's sort of the nuts and bolts task of figuring out how to help those companies know where to go, what it is the government needs at any particular time, and to put this in place.

Can the two of you tell us how, in your view, the Executive Branch can make this interaction work more smoothly? Let's have both of you take a crack at it.

Mr. ALLBAUGH. From my perspective, the best thing to do is to locate in one area, one-stop shopping, not only for those of us in the Federal Government, but those in the private sector right now. If you're in the private sector, my guess is you have to go to a multitude of agencies to talk about a variety of issues. We ought to be able to go to one place who knows where all the resources are located and can figure out where they need to be distributed.

For FEMA, it would be very helpful if that responsibility was located in one location. That way we do not have to set up our own shop to test software, test equipment, and can receive valid offers from the private sector.

And I agree with you, Mr. Chairman, the vast majority of the private sector wants to be in a helpful situation. Oftentimes, they are perplexed, as I hear, as to where they need to go to make the latest state-of-the-art technology aware and known to those of us in the Federal Government.

And so that would be the greatest service that we could provide. And I think that the President—I know that the President, Governor Ridge, along with Dr. Marburger, are off on this venture to figure out exactly where it needs to be located.

Senator WYDEN. Dr. Marburger.

Dr. MARBURGER. Certainly the concept of one-stop shopping was one of the drivers for the creation of the Office of Homeland Security. And the coordinating function of OSTP was certainly in the

minds of Congress when they established, in 1976, a very broad mandate for interagency coordination.

The Administration has available to it a number of mechanisms now—some of which, like the Office of Homeland Security, are new—that are just in the early stages of responding to the needs following the terrorist attacks of September 11th. And so I believe that the mechanisms that already exist have not yet been fully exploited. We are all working to exercise these very powerful coordinating mechanisms, like National Technology and Science Council, (NSTC), with its crosscutting subcommittees. We're just beginning to take full advantage of that. And my outreach efforts, which, as I described, were so much stimulated by your ideas on this issue, are just beginning to establish these information and feedback networks within the higher education and science communities.

So I believe we have a ways to go before we fully exploit the statutory and administrative mechanisms that are already in place. And as we encounter obstacles, such as some of those that you mentioned in your introductory remarks, Mr. Chairman, I hope that we can work together to clear away those obstacles and create, as necessary, additional mechanisms.

Senator WYDEN. I want to go to some other areas. I think this is key. What we need is to have all of the Federal agencies—and Director Allbaugh and I talked about this—you could, in effect, be spending your time in front of every congressional committee, at this point, and have every agency involved in this area. And, what we want to do, and what we want to work with you on, is to have a government-wide policy for mobilizing scientists and technology specialists, and then, to use your words, Director Allbaugh, "hold that organization accountable." We are going to work with you toward just that end.

Mr. ALLBAUGH. Thank you, Mr. Chairman.

Senator WYDEN. Let me ask you about a couple of other issues, then recognize my colleague.

Right now, just about every agency in the Federal Government is being inundated with new technology, scientific research proposals that are intended to bolster homeland security. Tell us how, today, the government is, in effect, evaluating those kinds of proposals?

Dr. MARBURGER. I could start with one area of proposals. There is a very interesting mechanism which is referred to as the Technical Support Working Group that is established under the Department of State, I believe, and the Department of Defense, which actually has funding available for quick investigations of short-term technologies that are appropriate for their needs. We are trying to establish, through the working group—the rapid response working group that I described in my testimony—a similar mechanism for exploring other kinds of technologies, perhaps longer-term, that come through the Office of Homeland Security and other agencies for evaluation. So far, we have been able to respond, in an ad-hoc way, to immediate technical concerns and questions that have been raised to us by the Office of Homeland Security. But we hope that a more systematic approach to this can function well.

So the agencies have, many of them, the capability of reviewing unsolicited proposals. I know that immediately after the 9/11

events, the National Science Foundation, for example, produced grants to engineers, visited the site to analyze the structure that had collapsed, and a number of other special cases can be identified. So the mechanisms of government are working in this respect, and I believe that they can continue to work well with enhanced coordination and interconnectedness.

Senator WYDEN. Director Allbaugh, do you want to add to that?

Mr. ALLBAUGH. Senator Wyden, I would ask Ron Miller to respond to your question insofar as what we're doing at FEMA right now, since we do not have a well-coordinated effort and it's probably replicated throughout every Federal agency that you can think of.

Senator WYDEN. Mr. Miller, welcome. And again, thank you for your involvement. Perhaps in answering this question, you would like to follow up on a matter you and I talked about privately.

There has been discussion among a number of scientists about the idea of organizing a Federal test bed that could evaluate these technologies and serve as a resource to other agencies. This Subcommittee, as you know, has had a great interest in the work of NIST (National Institute of Standards and Technology), in terms of being given a role in determining whether technologies meet the needs, say, specified by FEMA and others.

So if you could talk about what's going on now, in terms of evaluating this flood of products and technologies that is coming in, and also in your answer, perhaps incorporate the idea of looking at a Federal test bed to deal with these thousands of products and ideas that are coming in, that would be helpful. And welcome.

Mr. MILLER. Thank you. And thank you, Senator Allen. Right now, as you indicated, we are inundated with offers, proposals. In fact, so much so that we have had to designate a senior engineer on my staff who's going to serve as our chief technology officer, and their sole responsibility is to basically evaluate all of these proposals and, in some form or fashion, determine which ones might be relevant, set up a meeting with these individuals to discuss the kinds of things that they have to offer. And then hopefully, if there is something that we can use it for, try to integrate it into our environment.

There are a lot of difficulties, though, in us doing this. Number one, we're an operational organization. And the time it takes to evaluate this volume of proposals takes away from our ability to actually do our day-to-day business of providing the response and recovery folks the things they need technologically to do their jobs. The other problem is, we don't have the test facilities to be able to evaluate these to the extent that we should. And if a vendor comes in with a particular type of solution, we don't have a way of knowing if there are other vendors out there who might offer similar solutions or solutions that have better return on investment than the one that is being presented to us.

So it would be helpful, from that perspective, to have a filter at the Federal level, a filter, first of all, to look at the volume of proposals and determine which of these proposals actually has merit, not just for FEMA, but for any Federal agency that may have a need in that area, and then actually test them out to see which ones are legitimate, in terms of what they have to offer.

The ideal situation would be one where FEMA would get, from a Federal organization, a package saying, "We have this particular technology or this particular capability that we think will be relevant to your particular situation."

And so what you need is, number one, a standard-setting agency that basically lays out what it is the Federal Government's needs, and that would be a process they could work in coordination with the agencies; Number two, some form of test capability that would allow all of these proposals to be tested out and evaluated independently; and then, Number three, a process by which they can then feed the recommendations to the agencies that most need the capability.

It is pretty significant effort. There are test labs all over the Federal Government. There are science and technology functions all over the Federal Government, and they all have the same general purpose of just to try and deal with this volume of private industry proposals. And I think it would be helpful for that all to come together in some form or fashion.

Senator WYDEN. I'm very impressed with how you're doing it.

I think what I would like to do now, because Dr. Marburger is going to have to get out the door in a minute, is I would like to recognize my colleague. And, Director Allbaugh, with regard to your schedule, if we could have a few questions for Dr. Marburger, and then I could wrap with just a couple for you, and we would have you out the door in just a little after 10:00.

Senator Allen.

Senator ALLEN. I was first going to go to FEMA—just a very quick question for Dr. Marburger, and I will not keep you on the witness stand any longer than necessary.

Listening to what—I've taken notes here of Mr. Miller's commentary—clearly there needs to be a national standard. Do you agree? Do you believe there ought to be a voluntary minimum standard for backup systems in our country—or redundancies is the other phraseology that is used—to make sure that a network is running during an emergency?

Dr. MARBURGER. The word "standards" gives me pause. A well-defined agreement on what is necessary to provide the necessary backup support so that we can work to fill in the definition of what is required. I would certainly agree that we need to know what we're shooting for in the way of backup. Certainly FEMA would be in a position to help define what that support would be.

Senator ALLEN. Well, I will get to FEMA. I'm not sure—FEMA—this is more than just FEMA, the question of communications systems and backup systems. This is important for commerce. This is important for communications. Clearly FEMA gets into it once a disaster has arisen. Would you think it's appropriate at least to review such voluntary minimum standards, because what we hear so often, in reading through some of the testimony, most of this will be in the third panel, and you won't be here—and so much of it is that you hear that they were routed through the same conduits, routed through the same center, and it's just a glut through that, and so there needs to be some sort of relief value, so to speak.

Dr. MARBURGER. Yes. Now I understand what you mean. Absolutely, it certainly is appropriate to have—I'll put "standard" in

quotation marks in this context, but it certainly is important for us to understand what we need in the way of system support that has the robustness necessary to perform in an emergency like this or a terrorist incident. I certainly agree with that. OSTP does have a role to play in communications infrastructure protection definition and regulation, and there do exist—there are some committees in place that can carry this role.

Senator ALLEN. Well, I see it as something that—granted, we're all looking at the loss of life. And that's terrible. We also need to understand that there is a threat of cyber-terrorism, as well. And to the extent that best practices, so to speak can be put together, it is akin, in my view, to the way that the Y2K situation was addressed, although I do not care to have it addressed with worries of litigation and lawsuits for some businesses in the private sector. But to the extent that we can determine safe harbors, so to speak, or voluntary minimum protocols that could be taken, some of that would be by the company or by the entity itself, whether it's a governmental agency or whether it's a private company, but also determine which ways will work and interact with one another. So I look forward to working with you.

Dr. Marburger, I know you have to leave. Thank you. And I'm sure I'm speaking for the Chairman, as well.

Senator WYDEN. If I could—and then I want to recognize Senator Allen once more. Dr. Marburger, just know that we're very appreciative of the work that you're doing. I really do think that now is the moment for the government to throw open its doors to the ideas of scientists and information technology specialists and really call them at a time when it is so critical to our country's future. And we're going to be working very closely with you. And I may also submit some questions to you in writing, in terms of particularly the key points to look at as we try to start tapping this volunteer cadre of scientists and technology specialists. We will excuse you and thank you for your work.

Dr. MARBURGER. Thank you, and thank you for your support.

Senator WYDEN. Senator Allen, please proceed.

Senator ALLEN. Director Allbaugh, in my experiences with FEMA while I was Governor—and FEMA is—or was very well run, and continues to be very well run in recent years—the role of FEMA is one of almost oversight after the fact. And while, in listening to all of these questions, and Mr. Miller answering questions and so forth, FEMA is not a very large organization. It is not a big government agency. It is one of mostly, in my view, coordination after the fact, after the disaster has befallen a community or an area or some people. And you rely a great deal on the National Guard that is activated or, for that matter, law enforcement. And most of the time, it's not even State law enforcement. The first responders are local fire departments, local rescue squads, and the rest. And I think that your value is in determining how best to coordinate it.

I would like to ask you, did you find that, as far as the shortfalls that FEMA has—and you're mostly coordinating with others—you're talking about the Pentagon and folks responding from Alexandria and Arlington and Fairfax—and they're trying locally to put in Cap WIN—or I should say regionally, not just locally—but within the multi-State and District Cap WIN so that the firefighters all

can work together. Do you see that the IT problem of these terrorist attacks here are one of capacity or, let's say, a lack of capacity, as far as communications or IT, or is it one of a lack of technology? In other words, is the technology there, but there's not the capacity? Or the other way around?

Mr. ALLBAUGH. I think we have plenty of capacity. I think it is the technology. Oftentimes you will have an incident where fire and police arrive and they don't have the ability to communicate with one another except face-to-face.

I think it is critical that those individuals can speak with one another before arriving as they're on their way to understand what is happening at the scene. And it's just unbelievable to me that in many communities fire and police do not have the opportunity to—or the technology to communicate. They're on different systems. I'm sure there is a technological answer to that.

If I could say that we, as a government, should do one thing nationwide, it would be to provide the answer in some fashion, a standard, if you will—I happen to believe in standards, quite frankly—but we need to answer the question of how we make sure our first responders—fire, police, emergency medical personnel—can speak with one another, whether it's on the same frequency, the same bandwidth, that is an answer that has to be addressed.

We are a small agency, as you know, 2600 people nationwide. We are responsible for coordinating and facilitating the Federal response plan. We are the ultimate authority of the Executive Branch, the President of the United States goes to when there is an incident, and it is—you know this, being a former Governor—it is so critical to make the correct decisions that could save lives if you have accurate information. And that accurate information can only come in a way where you can communicate, whether by voice or electronically or some other mechanism. And I do believe the private sector has answers to every one of these questions. It's just making sure that we bring everyone together in one particular area and solve them.

Senator ALLEN. The reason I mentioned this—everyone expects FEMA to solve it. FEMA is looked upon, in a time of crisis or disasters, as those folks who come in, coordinate, bring together all the assets. Obviously, the funds, and the assistance are very calming and helpful to those areas and people in those communities that are adversely affected by whatever the disaster might be. So when I ask you these questions it's not as if FEMA is going to solve all of these. It is in coordination with the local or the State or the National Guard or State defense forces. All of them have to work together, and FEMA can give good advice, like they say. They shouldn't be building in an area that floods three times every 5 years. Let's move everybody somewhere else.

Now, as far as the technology breakdowns, as far as communications or telecommunications capabilities, that happened, obviously, on September 11th, does FEMA have any existing plans or are you formulating any plans to restore, say, computer networks or telecommunications networks? I'm not saying that FEMA is doing it themselves, but trying to work with other Federal agencies, State agencies, or local agencies—that if these computer networks go down, or telecommunications networks—do you have any advice

or—number one, do you have any existing plans? Number two, if not completely formulated, are you moving in that direction?

Mr. ALLBAUGH. We do have plans, Senator. And I would ask Ron to respond to that question.

Mr. MILLER. We have been working with the Critical Infrastructure Assurance Office. One of the things FEMA brings to the table is its relationship with State and local governments and communities, and we are working with the Critical Infrastructure folks to try and at least provide a framework within which they can develop standards for inter-operability redundancy. Again, we talk about standards—and I understand Dr. Marburger's apprehension about standards.

Senator ALLEN. He has to be consistent on some other issues, as well.

Mr. MILLER. There's the implication also with standards that you're going to force something on people. And when we talk about inter-operability, one of the key tenets of that is the ability for these folks to use the technology that they have and find some way to make it work together, as opposed to trying to make them all do the same thing.

One of the problems in trying to solve the first responder communications problem is that people are focused on everybody having the same capability, as opposed to looking at the capabilities that are out there and finding a way to integrate and make them work together, which allows them to preserve the communications needs that they have within their local communities. But at the same time, if the disaster expands beyond their scope and they need to interact with others, there's an ability for them to do that. I will say that there is technology out there that will allow that to happen, and it's just a matter of being able to evaluate it and, if it is effective, to be able to deploy it.

Again, you make the point that there is a coordination process involved, and that is where we come in. We understand the emergency management community. We understand the first responder community. We work with them all the time. We know what their problems and needs are, so it is just a matter of trying to identify reasonable solutions and then letting the technology community take a crack at them.

Senator ALLEN. As I mentioned, the National Guard—when the Governor activates the National Guard in such situations, this concept of a NETGuard, which is the technology folks—and I know there are people with good communications technology—awareness, and intelligence, and so forth that are in the State Guards. Would you see a NETGuard being a good asset in that regard?

Say you have purely information technology or purely a technology disaster to solve, how would you see a NETGuard being helpful in providing some necessary services in such an eventuality, a disaster?

Mr. ALLBAUGH. I think their services would be welcomed. When an incident is ongoing, as a line officer responsible for making decisions to save lives and property, it would be helpful to be able to draw upon that brain talent, that pool of answers that they may offer up. So you could be in a position to save more lives. But un-

derstanding when an incident is ongoing, there isn't a lot of time to argue about it. That's why we have a command structure.

So as much as I want the private sector involved in our business, bringing the worldly answers that they have—and I know that we don't have—even though we have extremely talented people, I also want there to be an understanding—give me the array of options here. I will make the decision. When the decision is made, we all walk out the door together. I would think that that would be very, very helpful, particularly to the local responders—fire, police, emergency managers.

I don't receive, as I said and have said many times—I do not receive the 911 phone calls. It is our local folks who receive the 911 phone calls, and I believe that those who are closest to the problem are best equipped to answer and solve those problems. But I think something like this would be extremely helpful.

Senator ALLEN. Thank you, Mr. Allbaugh. Thank you, Mr. Chairman.

Senator WYDEN. Thank you, Senator Allen. Just a couple of other questions, and I want to recognize our colleague from Florida.

On this question of the compatibility of emergency communications, something Senator Allen and I both talked about, my understanding is that there may be as many as ten Federal agencies now looking at this, that this is a subject of considerable discussion in separate agencies. Is this the kind of issue, Director Allbaugh, that you could see Governor Ridge and the Homeland Security organization, in effect, pulling everybody to the table, bringing together the experts in the private field and the local responders, coming up with a policy, working with Senator Allen, myself, Senator Nelson, people who have been interested in the field, saying this is where we want to be, you all can hold us accountable, and then we would be able to proceed, in terms of a difficult issue?

Mr. ALLBAUGH. Absolutely, Mr. Chairman. As a matter of fact, Governor Ridge and I have spoken often recently about the approach, just as you described, figuring out exactly what folks need, issuing the charge and the challenge, providing money to help them get there, but come back and have a mechanism of accountability on the back end to make sure that everyone is doing exactly what we agreed to do. And this, again, is not an incident where I want to be in a position as a representative of the Federal Government of cramming something down some local individual's throat. This has to be done in a cooperative spirit or it will be a failure from the outset.

Senator WYDEN. I think we're on the same wavelength on this point. My understanding is that you all are looking at some approaches you could be talking about with the Hill early next year. I know we're interested in working with you on it, and especially getting that one out of the box early-on in the process.

It is just unconscionable that in our country, at a time when we have so much technological expertise, and at a time of disaster like we saw September 11th, we have fire and rescue folks taking messages by hand to each other. That is just unacceptable, and I'm glad we're on the same wavelength, in terms of tackling that.

Mr. ALLBAUGH. Thank you, Mr. Chairman.

Senator WYDEN. One last issue, then I'll recognize my colleague.

Let's talk for a moment about the concept I call the technology equivalent of the National Guard, and there are similar ideas out there. At the end of the day, we're all looking at the idea of pulling together a cadre of scientists and technology experts with significant expertise who would be in a position to assist the government, both in a preventive kind of way, giving ideas on the state-of-the-art technologies that you and others could begin to use to prevent tragedies, and also to be able to respond.

As we talk to people in the private sector, there are a variety of ideas that they have about how you work on this, some envisage a technology equivalent to FEMA's medical response program. Some see it as kind of a virtual organization, a kind of database of experts in various fields and people with equipment that could be donated. Some have seen it almost as a military-style reserve unit.

As we look at this issue—and, as I say, we're going to work closely together with you and Dr. Marburger on it—what are the key points that you all think we ought to keep our eyes open on? Obviously, we want to make sure that we separate out the many who truly want to be helpful from those who might want to make a quick buck. People are going to need training, and they're going to need to work to do what you've talked about, Mr. Allbaugh, which is to be user-friendly to those first responders to give them what they need.

But maybe if you could—and this will be the last question I will ask—kick off the key points we should keep our eyes open for as we try to figure out how to call on this generation raised in information technology to help.

Mr. ALLBAUGH. Mr. Chairman, I think there are two key points, both of which you've already touched on, that would be cornerstone of any entity responding to future disasters. One would be providing an appropriate database. Just knowing exactly who to go to for that technological or IT brainpower is often a confusing arena. You have a multitude of companies who are in business to make a profit. I have no problem with that. But there are so many companies out there that it is confusing to know exactly who to go to for what particular problem. And so providing that database immediately is more important than having the warm bodies at the site to solve the problems that crop up.

Second, and almost more importantly, utilizing that same brainpower to train our State and local responders is absolutely critical to any success in the future. And so I would envision something that we already do with local responders on a regular basis at Emmitsburg. It operates—it is a campus in Maryland that—we bring in first responders—fire, police, emergency managers—to train them on state-of-the-art. And I would further enhance our training in the IT arena by being able to draw upon these individuals who could talk about state-of-the-art software or hardware in a manner that is easily understood by everyone. And that goes a great distance. Just a little education will bring everyone together and move us further down the road together.

Senator WYDEN. Well, I thank you for all of the assistance. I would also like to just state for the record that when I called Director Allbaugh for the first time to discuss these issues, he was on

his way to taking his wife on a birthday supper somewhere in Oklahoma, and he thought it was so important that we still ought to talk through the weekend, and that is sort of the gold standard, in terms of government responsiveness, and we're very appreciative.

And, Mr. Miller, to you, as well, we thank you for your involvement with us. We're going to be calling on you often. I don't think there's any higher priority than to mobilize, to try to prevent some of the problems we saw on September 11th for this Subcommittee, and we'll be calling on you often.

Let me recognize Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. Thank you, Mr. Chairman.

A few days after September 11th, at the invitation of the Governor and the Mayor, and Senator Clinton, I went up to New York. I want to compliment FEMA for what I saw that day. In the midst of all of that chaos, order was being established. I think you all did a very good job.

Mr. ALLBAUGH. Thank you, sir.

Senator NELSON. I was intrigued by the fact that one of our colleagues from the Florida delegation had arranged for the donation of some satellite telephones as a means to solve an immediate problem. And, I'm just curious—did satellite telephones work under those conditions when normal communications and cell phones did not?

Mr. ALLBAUGH. In the early days, Senator, virtually our entire disaster field office at Pier 94—we relied upon satellite communications. There was no other way, given the fact that the main switches at the Verizon headquarters in lower Manhattan had been severely damaged. There was no other entity, quite frankly, to rely upon. So we had to rely upon a system that we had built over the years. They worked very efficiently. We were lucky to have them. I could only speculate what it would have been like without the reliance of those satellite telephones.

Senator NELSON. And even where you had tall buildings in a high, dense, urban area, the satellite telephones still worked?

Mr. ALLBAUGH. They did, indeed.

Senator NELSON. Well, that's good. Is that part of our plan, then, for the future, that we have a reserve of these satellite telephones for FEMA if such an emergency like this occurs again?

Mr. ALLBAUGH. I think we always will have a repository of those phones. I'm not sure that we want to become 100 percent reliant upon satellite telephones. They do have their drawbacks. Periodically, even though you have a connection, the quality is not what you would want. And I think that will just improve with time. We were fortunate to have those, and I would like to think that many lives were saved as a result of having access to those.

Senator NELSON. Very interesting. Clearly, they have their worth when you get out into rural areas and need to communicate, or in desolate areas, because that's your only means of communication. So it wasn't that that you were referring to that was donated that didn't work.

Mr. ALLBAUGH. No, not at all. I would have to ask specifically whether we used the donated phones. We already have a backbone structure in place that we rely upon, something we have had for a couple of years. But I would check into that, Senator, and respond back to you whether that particular package was used or not.

Senator NELSON. Thank you, Mr. Chairman.

Senator WYDEN. I think the Senator from Florida is making an important point. One of the things we were told is, with everything, essentially crashing, the global satellites, Global Star and Iridium, did not go down. So this will be an area we will want to examine.

Gentlemen, you've been very helpful. Do you have anything further you would like to add?

Mr. ALLBAUGH. Thank you for the opportunity to be here, Mr. Chairman. It's always great to come and visit. Let us know if we can be of any help.

Senator WYDEN. We will be calling on you often. We will excuse you now.

Mr. ALLBAUGH. Thank you.

Senator WYDEN. Our next panel is a resident of the Pacific Northwest. We're very pleased and proud to have him. He is known as the "Father of Wireless" to many, Craig McCaw, Chairman and Chief Executive Officer of Eagle River, Inc., in Kirkland, Washington.

Mr. McCaw, welcome. I've had a number of good conversations with people in the private sector—Andy Grove, of Intel; Steve Jobs, of Apple, and others—but you have, I think, made some particularly helpful and useful contributions, and it's just terrific to have you here. We'll make your prepared remarks a part of the record, and you just proceed any way you feel comfortable.

STATEMENT OF CRAIG O. MCCAW, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EAGLE RIVER, INC.

Mr. MCCAW. Thank you, Senator Chairman Wyden, and Senator Allen, and Senator Nelson.

Obviously, I'm here to support the notion that we have discussed of a technology national guard. And very much in the context of having served for 15 years in NSTAC, looking at potential national disasters, and, frankly, having been through a number of them, and we've seen how the system works and how it doesn't work.

What I think was different in September 11th was both the location, the sensitivity and, I think, the changing standard of threat that we saw. And what I think was firstly important to note is that the country has become increasingly dependent in every level on its extraordinary communications infrastructure, and certainly, the Internet is a large part of that. But every aspect of our democracy, our commerce, and personal communication between individuals has begun to evolve in a way that we wouldn't have conceived of years ago. The notion of instantly communicating from person to person or the amounts of information we expect in our daily lives has changed radically. And the entire functioning of the Nation is dependent on this, in my opinion.

And I would have to say, on September 11th, everything worked as it was supposed to. NSC, NSTAC, individuals, the work of Harry

Radege, Chairman Powell in response to those problems, FEMA, all the people who have testified—were exemplary. However, I think, to the points you've raised, the fundamental way we are organized is much more a throwback to the cold war.

And having been on NSTAC, again, since the says of the cold war, I can say that our thinking has not evolved around the notion of the rising standard of expectation in telecom that has happened in the past 15 years. And I think we could not underestimate the changes that have taken place. And since the cold war, of course, we, in 1984, broke up the Bell system. And Bell Labs was the repository of an extraordinary relationship with government at every level, the military, and key assets that could be called upon almost in a quasi-government form, because the Bell system, AT&T, were really an arm of the government, in a way, since the 1920s. That does not anymore exist.

And what is great is that we have a repository of intellectual capital in this country, distributed across the country, in companies like Intel and, frankly, a huge number of retired people from Microsoft and other companies whose IQ, whose knowledge, and whose time could be put to this process in very much in a National Guard-type of forum, that those type of people, particularly in light of what we've seen happen, and in recognition of what could happen, is simply unbelievable. And I think of my friend, Nathan Mhyrvold, and characters like Bill Joy—Microsoft is the closest thing to Bell Labs we have today in this country—the number of people inside.

And yet this is really a matter of changing the idea of altruism from huge companies to that of individuals. And what we've learned is that the Internet empowered individuals. And what we have is an economy composed of highly capable individuals able to operate without the central core structure of a huge corporation. And much of what we built around was, in fact, framed on the idea of huge companies coming to the aid of their government. And in the military sense, much of that is still true, except perhaps in the high technology areas of computers. In telecom, that's much less true.

And what we recognize is that, in times of disaster, our wireless infrastructure is the thing that we fall back on. What we saw on September 11th, and we continue to see, is that we would have a much worse situation if the people were still actually trying to function in south Manhattan. The decimation of the central office of Verizon and the wired infrastructure that related to that remains as a factor. To our benefit, we're not trying to use it, or we would see that deficiency.

Another oddity was that because so many financial institutions were based in that area, they had constructed backup facilities elsewhere. And the dislocation to the Nation was far less than we would have imagined because of that. That is not true in most other parts of the country.

What I think we recognize now is—and we have certainly had, through the news and through the efforts of the Administration, Governor Ridge and others—is a recognition that we do not know where the next threat comes from. We had a lot of advance notice of Hurricane Andrew and other national disasters. We expect

earthquakes in California and Washington and Oregon. We have planned for those. We can't really plan for the efforts of terrorists against our country now. And I think the notion of having actual individuals ready to go and resources ready to go at every level is critical.

If you have a flight of our productive sector in any part of the country—and let's take New York—because of a disease, bio-terrorism attack, dirty nuke, whatever—no one has really thought through how you would communicate with these key individuals central to our economy or our government if they actually depart from the urbanized areas. We have a high reliance on wired infrastructure in our rural areas, and we have to think in terms of how we build wireless infrastructure that can follow in case of these kinds of disasters. This could be any city—Washington, New York, whatever.

So these dislocations are not, I think, well-thought-through from the standpoint of what do you do, how do you get it in place quickly, and essentially preplanning the process. And I think what you propose is really central to that issue, which is that when you build a complex society, it is vulnerable to stone-age problems, which is that you can take very simple guerilla tactics and make our incredibly productive, sophisticated, wonderful society where there's tremendous communication between individuals, and that is our strength. That's our trading value in the world. And we have a massive benefit over the rest of the world because of that infrastructure.

So I think figuring out in advance what you're going to do if something happens, having those incredible resources, many of whom, quite frankly, are not even active today and could provide a lot of their time to this—would be critical and, secondarily, changing our reliance on centralized infrastructure is probably critical in making that investment. It is more efficient to centrally locate all your switches in one place, and that's cheaper. I think we've seen the result of that in the damage to the World Trade Center and those Verizon switches, which affected every other aspect, almost, of the communications infrastructure in that area. When those switches went down, even the cellular systems couldn't connect to each other, albeit I would note, as a minor thing, that the Nextel system continued to operate because it didn't rely on those. That's my one advertisement for the day.

But I think the elements that have been noted, making sure that we have thought through what we're going to do if something happens, and we can now work against these scenarios with the brightest minds in the country. And making sure that we no longer rely on highly centralized single-source infrastructure is critical. And I think several people have noted the degree to which our key resources are located too much in the same place. And assuming the terrorists have turned out to be much smarter and more sophisticated than we thought, that is not unknown to them, either.

So I think the opportunities are obvious. And I applaud, frankly, the effort to move forward and proactively put in place individuals with the security clearances and the other elements so we don't just rely on the good works of a few people and the time lag that

occurs between a disaster occurring and the other elements falling in place.

The time element of flying in 5 or 10 or 20,000 wireless phones, moving in the other facilities is, I think, too slow in our current expectations. And that's why people are a little discomforted by what they saw on September 11th, no matter how well we did and how well we worked and, frankly, how hard individuals worked.

City Hall was out of service for a quite a long time. And, as I noted in my testimony, one individual worked 60 hours, almost straight, to connect City Hall with almost no direction from management, simply on his own volition. And, of course, that's the wonderful part of the American way. But I think we can reduce our reliance on those elements by actually moving forward with something that is far more organized and actually know who we're going to call, how to reach them on the weekend, because, of course, terrorists do attack also on weekends. And national disasters occur on weekends.

And so, again, I applaud the efforts you're making, and I highly support the intent with which you are moving this forward.

[The prepared statement of Mr. McCaw follows:]

PREPARED STATEMENT OF CRAIG O. MCCAW, CHAIRMAN AND CHIEF EXECUTIVE OFFICER, EAGLE RIVER, INC.

Thank you for the opportunity to address the subcommittee. I am here today to support the effort to establish the National Emergency Technology Guard or the NETGuard. Telecommunications infrastructure is vital to the success of the economy and the need for robust and redundant national communications infrastructure is more critical now than ever. The Nation is well served by initiatives designed to preserve and protect our nation's telecommunications infrastructure—the primary foundation of the economic successes of the past decade. NETGuard is one such initiative.

If we are to improve the way we mobilize the resources and experience of our nation's science and technology community for future emergency preparedness purposes, we must ask tough questions and expect honest, and not always comforting, answers.

The events of September 11 and other threats we now face expose surprising vulnerabilities in our underlying communications infrastructure. Few could have imagined a scenario wherein much of our telecommunications infrastructure in parts of lower Manhattan remains inoperable even 3 months after an incident.

In addressing how to marshal our collective resources and talents to protect against and respond to any future incident, we must analyze the strengths and weaknesses inherent in our telecommunications infrastructure and its ability to respond to future threats.

On September 11, we witnessed first hand the vulnerabilities of our network infrastructure. First, it is clear that we can no longer solely rely on historical monopoly telecommunication networks that in placing a premium on economic efficiency, concentrate network assets into a limited number of central offices. That model reflects a centralized, hierarchical infrastructure that is highly susceptible and vulnerable to attack. The Verizon central office at World Plaza was one of the largest in the world, serving as many lines from that one location as are served in the entire city of Cincinnati.

While deregulation over the past decade has fostered great progress in building a decentralized distributed network infrastructure—the Internet is the prime example—our legacy telecommunications networks still lag behind in transitioning away from its historically highly centralized architecture.

Multiple wireline and wireless competitive distributed networks that were deployed and operational in New York prior to September 11 were critical to public safety and the recovery efforts. Access to unencumbered available spectrum was another crucial element in restoring capacity lost in the September 11 attacks. We saw first hand the value provided by the facilities-based networks of competitive local exchange and wireless carriers. These networks helped to fill the void created by the loss of some of the essential facilities of the incumbent provider. Fortunately,

the FCC quickly granted wireless carriers special temporary authority to utilize 30 MHz of fallow spectrum assigned to NEXTWAVE to meet the overwhelming emergency need for wireless communications services.

The legacy of the monopoly era impacts not only our existing physical infrastructure but also our ability to respond to current disasters. In times of crisis under the old monopoly regime, the government could tap Ma Bell's nearly unlimited resources and talent pool from its affiliated and quasi-governmental entities, such as Bell Labs. Today, while the physical assets of Ma Bell's legacy network largely remain in place, its vast pool of human talent has been dispersed to many smaller unregulated competitors throughout the technology and telecommunications sector. As a result, technical expertise is no longer concentrated in a few monopoly companies but is instead spread throughout numerous entrepreneurial ventures.

The NETGuard could provide the necessary governmental framework to tap into that technical expertise, at the local level, and get it efficiently focused to assist in times of crisis. During the events of September 11, we witnessed numerous acts of heroism by dedicated people who, at the scene, shared their invaluable technical experience and sacrificed their time and energy to assist in the recovery efforts. One example is Bob Oliva, an XO Communications employee, who on his own initiative, worked onsite for over 60 straight hours, with little or no sleep, until telecommunications lines at the Mayor's office in New York were up and running. If an organization such as the NETGuard were in existence on September 11, local authorities could have organized and harnessed the talents of individuals—such as Bob Oliva—during the crisis in a more coordinated and expeditious fashion.

If created, NETGuard, as a Federal entity, would be uniquely positioned to call upon the nation's technical and operational experts and be the clearinghouse for those who wish to support their country in times of need. Unfortunately, today, no Federal body exists to facilitate such a critical function. Federally established multidisciplinary industry committees and councils, (e.g., the FCC's Network Reliability and Interoperability Council (NRIC) or the National Security Telecommunications Advisory Committee (NSTAC)), make a valuable contribution to the policy framework on emergency preparedness issues. Their primary function, however, is in an advisory capacity typically with narrow charter responsibilities and limited administrative capabilities.

The NETGuard would also be invaluable in providing expertise to prepare for future and unanticipated threats on the horizon. How would we respond, for example, in case of a mass population migration into rural areas resulting from the threat of biological attack on a major metropolitan city? It is unlikely that the existing rural infrastructure could provide the additional telecommunications capacity necessary to serve a sudden increase in the population base. The NETGuard could bring to bear the expertise necessary to address the vexing issues associated with providing emergency bandwidth—wireless, wireline or satellite—in rural evacuation areas where citizens will need information and communications services to overcome geographical limitations.

Moreover, NETGuard could also play a crucial proactive role in providing expertise to ensure the development, deployment, and availability of redundant network capacity for end user access to multiple telecommunications networks. Redundant fiber and fixed wireless facilities have been deployed in the past decade. Many of these facilities, however, fall short in reaching existing end user customers, and thus will not be accessible during a crisis.

Just as Congress established government policies that resulted in the creation of multiple distributed networks that compose the Internet, it can promote similar incentives designed to ensure the development and deployment of multiple competitive distributed telecommunications networks that use a variety of technologies and service providers (e.g., broadband satellite, 3G, terrestrial wireless, broadband cable, and wireline).

The NETGuard, under Congressional mandate, could also promote public safety in areas such as public rights-of-way and building access. Such an entity could share its expertise to speed the development and deployment of these redundant and decentralized wireline and wireless networks and so that end user customers have multiple "last mile" access to the nation's telecommunications infrastructure.

Congress would be taking the right step in considering a NETGuard to protect our national communications lifeline. And with little additional effort, the NETGuard initiative can be enhanced to further bolster the emergency preparedness of our nation's telecommunications system. In addition to considering NETGuard, I recommend that Congress adopt the following measures:

1. Ensure the availability and use of wireless networks capable of providing public safety functionality at any time and place irrespective of population density or geographic location within the United States; 2. Create national emergency spectrum

to be held in reserve specifically for public safety and emergency purposes; 3. Develop building access legislation that would promote network access redundancy in government buildings and allow more than one "last mile" telecommunications provider at these locations throughout the country, as well as legislation designed to spur investment in broadband telecommunications networks, such as Senator Rockefeller's Broadband Tax Credit Bill; 4. Promote the deployment of alternative redundant and distributed "last mile" wireline network facilities by strengthening the FCC's existing statutory authority to remove barriers to competitive entry in the public rights-of-way; and 5. Establish a national emergency telecommunication priority access system to allow public health and safety users priority access on all of the nation's various telecommunications satellite, wireline, and wireless networks.

Senator WYDEN. Well, Mr. McCaw, thank you very much. To have someone of your stature who has spent so much time thinking on these policy issues, willing to work with us and, as we have talked about with the Bush Administration, in bipartisan ways. It's enormously helpful.

If it's alright with you, we've got a vote on the floor. Senator Allen and I will get over there and vote quickly, and then we will come right back and have some questions for you, because I think you've made a number of points that are exceptionally important.

If that's alright with you, we will just recess, say, for 10 minutes.

[Recess.]

STATEMENT OF HON. MAX CLELAND,
U.S. SENATOR FROM GEORGIA

Senator CLELAND. I've been asked by the Chairman to proceed. The hearing will come to order.

Mr. McCaw, thank you very much for being here. We appreciate your innovation and leadership, your entrepreneurship, and especially your insight into telecommunications, particularly in terms of a crisis.

I'm an old Army signal officer, and we were talking just before the hearing came to order about the brainpower that used to be concentrated in AT&T, Bell Labs, and so forth. As a young signal officer, I was stationed at Fort Monmouth as the aide to the commanding Army general in signals school. At that time, the Army had a wonderful close working relationship with AT&T, Bell Labs, certainly the Army Signal Corps.

Then I went to Vietnam and learned about communications in combat, when wires are knocked out, when systems that you have in place are destroyed. One of the first lessons I learned in the Army Signal Corps, as a young signal lieutenant, was that redundancy is the secret of reliability.

And that the moment on September 11th that the Pentagon was hit, I saw the smoke across the river out my window in the Dirksen Building and immediately went to my cell phone, which, in effect, was jammed, and jammed in a sense that it was already overloaded.

I wonder what some of your suggestions would be, in terms of satellite communications, in terms of redundancy, and the sense that one of the things we did was flee Washington. I found myself within an hour or so as a refugee across the river into Northern Virginia—the point being, people were fleeing the city or the target or the potential target into rural areas. Then, all of a sudden, I had a Blackberry in the car and began to communicate on that, and that became my only line of communication for a number of hours

with the Governor of Georgia who had a Blackberry as well, and so forth.

So kind of take us from there and see what some of the things that you would suggest we think about in the future so that when we have a hit on the United States—when we have maybe a terrorist attack, the normal lines of communication go down. Where are we, and what should we be doing?

Mr. MCCAW. Senator Cleland, I'm honored to be with you, sir, by the way. Those are really good questions.

To the points you make about the military, as we look at the campaign and the comments that have been made, that there will be more casualties at home than in war, the use that the military has and needs in technology are huge, and they're ongoing. I think the rate at which we, as old timers looking at the old military versus the new—bandwidth used by the military is growing in the hundreds-percent per year in order to protect and save lives in the military and make us more effective. And I think the same applies at home.

Substantially, this is wireless. Because of its flexibility, its ability to be deployed rapidly. And that if you don't happen to be in the place where you're supposed to be, the system doesn't really mind, because it's built around the notion that people move around. And so the wired systems are built around high amounts of information going to fixed locations. Once you have to move away from that, everything changes and you rely on this sort of womb-like structure, as I would want to call it, of wireless infrastructure we put in place in the past 15 to 20 years.

One of the things that we were very lucky—on September 11th, the infamous Next Wave spectrum was sitting in reserve to be employed, through the good graces of the FCC, on an emergency basis to help produce what was an extraordinary over-capacity and overdemand. And we certainly had a problem there.

There is no question that—and FEMA testified earlier their dependence on satellites was almost 100 percent in order to make their effort successful. And I think we have to recognize that multimodal communications are the way that you protect against vulnerabilities. And again, where we would have been 20 years ago was almost totally dependent on one operator, one system, one highly vulnerable central office switch in an area, operating on the one-carrier system. And that resulted in several famous crashes in the signaling system. Seven networks that we remember a few years back, when entire networks went out.

The beauty of the Internet is it's very survivable, and that's why devices like your Blackberry worked. And if we can continue that effort to proactively diversify our resources, I think we can substantially reduce the dislocation, because our country cannot exist without these communications.

I was hearing last night about people in Bangladesh, by the way, now relying—who can't read or write—using the Internet to communicate. And you can send a message now from Bangladesh to the United States, even if you can't read or write, for about ten cents. Somebody will type the message and send it for you by going into a central place in a village. Recognizing that even if Bangladesh, in a country which is recognized as the poorest in the

world, can at least get Internet service and those things, we need to believe that we have—that no matter what happens, what anybody throws at us in this country, we have some forum for people to interact. And we saw a deficiency of that after September 11.

Senator CLELAND. It's interesting to say that we have some poor counties in Georgia that would envy Bangladesh's communications capability.

So where does that leave us? Focusing more and more on space communications, on satellites, on a system of satellites around the globe where we network that way?

Mr. MCCAW. I think we have to ask for all of those things to occur, that we recognize parts of the country will never have any kind of wire-to-wireless service of any kind. And fundamentally, I don't think it is in our interest to have those.

We saw the crash in Pittsburgh of the United flight, and there was no wire-to-wireless service there, certainly not enough to handle the job. We have to be ready for those things, and I think it's critically important that we recognize that there is an overriding public interest in being able to communicate to the entire country at any time and to recognize that—and this is more—this is outside of the central issue, but—if there is some reason for people to leave the city, other than the quality of life in rural areas, which is very high, we need to respect that, enhance it, and make it more competitive, so that just because you happen to be in a rural area, you are not on the wrong side of the digital divide. And I view that as substantially a wireless issue, be it satellite or terrestrial.

Senator CLELAND. Thank you. I've held some Senate roundtables in rural Georgia, and believe me, they are ready for fiberoptic cable, they're ready to communicate, they're ready to tie in, and they're ready to connect. They don't want to have to, quite frankly, move to Atlanta, to the worst traffic in the Southeast. They would much rather stay in Umatilla or Fitzgerald, Georgia, or whatever, if they could only get connected.

So, it reminds me a little bit of the connectivity issue a generation or so ago when President Roosevelt created the REA, the Rural Electrification Association, and the government helped provide expansion of the wires—in this case, electricity—which, in effect, lit up, not only rural Georgia, but rural America.

I wonder if we ought not look upon the connectivity of rural areas of America in the same manner.

Thank you very much for your service and your comments today.

Senator Allen.

Senator ALLEN. Thank you, Senator Cleland. Let me follow up on Senator Cleland's comments.

The specific reference to your written testimony, which I read, and I know you expressed your views, but your written testimony—some of it is in more detail. I suspect that the answer to the question here is as far as communications capabilities, it needs to be a mix. There is no logical economic reason to have wire-to-wire Internet service. There's just too much dirt to dig to get to too few folks out in the country.

And I did live in the country before I was Governor and was very happy when they actually delivered the newspaper to my house as opposed to the end of the road, which half the time it wasn't there.

But at any rate, finally they did, because more people lived on a gravel road.

But it is going to be a mix. It is going be terrestrial wireless. It will be a mixture in some cases, even in some of the small towns, it will be wire-to-wire, but it's going to be satellite. All of those opportunities need to be there.

The analogy I would have in reading your comments about—here, your first point—this is in addition to being in support of consideration of NETGuard—you pointed out "ensure the availability and use of a wireless network—and I would add satellite—capable of providing public safety functionality at any time and place irrespective of population density or geographic location within the United States." I was reading that, and Senator Cleland, it's like the RDA, or what he was talking about. I think this is more like the Interstate system. The Interstate Highway System was designed—one of the justifications was national defense. You're talking about having the system here all over the country, with the side benefit, of course, of the Interstate, being we can drive easier. But it was national defense. And there are stretches of highway that—and I forgot, every so often that it could be used as a runway where there's a straight stretch. Now, obviously, we haven't used it much for national defense, but it's a great way to get around the country.

And the same, while you're talking about having escapability, no matter whether you're out in the country or in the city or the suburbs, that you have this public-safety capability, and that's a reason for it. But again, the other beneficial reason is of communications and of commerce and the exchange of ideas and beliefs and so forth.

So I find that a very interesting analogy and I think that that might be another reason for those of us who want to make sure that all people have those opportunities for their businesses, for their communities, and for their enterprises. This is just another good argument for security, because, in fact, I saw Senator Rockefeller, during this vote and told him of your commendation, commending remarks as far as that idea, and I think you're on that bill too, and we're all in favor of it.

Now, the second point you made was to create a national emergency spectrum to be held in reserve specifically for public safety and emergency purposes. We've had a hearing in this Committee, a month or so ago, about the 3G spectrum. And so my concern with that is, can there be an existing spectrum allocation that could be used, because there's such a demand for existing spectrum that you wouldn't want this effort for national emergencies or public safety situations to have an impact on new entrants or spectrum allocations?

Do you have a specific area that would not harm the ability of others to get into those new spectrums or use the existing spectrum?

Mr. MCCAW. That's a series of very good points. In terms of the 3G notion and public safety, I think we need to see public safety with inter-operability, and we need to see military inter-operability, frankly, the ability for NATO and others to communicate with us. But certainly public safety can accommodate that.

I see much more of this being a public-private kind of cooperation with priority access, for instance. And it is possible to make public-safety spectrum use much more efficient, and we can help them do that. And I think we, in fact, have made a proposal through a company I'm involved with to help consolidate and increase their position while not taking away from the 3G efforts.

And in many ways, whether you look at military or public safety, you need this notion that, in times of need, that you can almost slide back and forth between these elements and have a more flexible infrastructure that allows you to prioritize, based on national emergency, the access to some of that. And I think that would very much answer that question.

Senator ALLEN. So it would not be a dedicated permanent spectrum allocation that could be a prioritization.

Mr. MCCAW. Well, you could have essentially boundaries with the ability of the border to slide back and forth, depending on circumstances and/or simple access across the border using similar technologies, which I think would clearly help a lot.

Senator ALLEN. I understand. We are having another vote, so I have to get back. I am going to yield back to the Chairman. Thank you so much for your testimony and your very valuable time. Thank you.

Thank you, Mr. Chairman.

Senator WYDEN. Thank you, Senator Allen, for keeping all of this going. As you can see, Mr. McCaw, it is really bedlam today.

Senator ALLEN. Thank goodness you all do not run your companies the way this place is run.

[Laughter.]

Senator WYDEN. Again, Mr. McCaw, I am so appreciative of the support and the counsel you have given me, and let me ask some additional questions to see if we can flush out some of these issues, given the fact that we have got your expertise and a chance to talk with you today.

As you know, communications technology is converging in the digital world. The lines between voice and Internet and video or audio traffic and the delivery systems are essentially starting to blur. Would it be your sense that, given this extraordinarily rapid evolution of information technology and its implications for the country's vulnerability, that this could be an added benefit of an organization like NETGuard, because I think that if we are going to get out in front of these terrorists, who are going to have the same capabilities to deal with the new technologies, we need information from those in the private sector.

I wonder, given the fact that you have studied the question of convergence of communications, as technology gets more complicated, whether it might be an added argument for the kind of approach we are talking about that the private sector could give us the ideas and the technical advice to help stay out in front of the terrorists.

Mr. MCCAW. I think it is a really good question. One of the things that has occurred to me is, of course, you always want to be—there are two parts to it. One, you want to make sure that you do not give your enemy the tools to defeat you, and there is some risk of that in our technology being so available, so egalitarian, and

that is a reason that I think you can benefit from the very best minds looking forward and suggesting the vulnerabilities, and what they might do to us, and how to beat that.

So not merely in a defensive, but in an offensive mode, and likewise a recognition of how to protect those certainly can come from those minds, so there are really two sides to it, and both are of benefit from what I would call the deep thinkers, who do not necessarily come with a commercial point of view, because I think there is a lot of risk to a commercial point of view that many committees in the past were built on, because big companies were the repository of those minds, and now those minds, through the power of those technologies they have created, have become very independent and live in funny places all over the country.

Senator WYDEN. I am very interested, as well, in the point you made about the need to move away from highly centralized and concentrated communications networks. I mean, it seems to me that as you look to the future, and the Internet is a perfect example, it is the essence of a decentralized system. You have got all of these opportunities around the world to be part of it, and I wonder if you could amplify a bit on your ideas for moving, particularly in a transition from a centralized kind of system to a more decentralized focus for wireless and wire line networks as it would relate to a NETGuard and a volunteer technology force.

Mr. MCCAW. Well, certainly the Internet, lest we ever denigrate government, the Internet was a government idea for survivability, which the private sector hijacked a very good idea and took it in a lot of directions that were not originally contemplated, and I think it was the brilliance of that on both sides that has created something that frankly has put this country so far ahead globally in commerce as well as trade in those kinds of products, and frankly, the software that goes with it, and so I think continuing that process and facilitating it is a key asset that we have.

Years ago, we dominated transportation, and we no longer dominate transportation globally, except perhaps in package delivery, where I think we still do. In terms of other things, of creation and creativity, that public-private partnership that the Internet represents a form of is just absolutely central to what will keep us ahead in the world, and keeping the minds working closely with the power of the government, the Federal Government in that respect is crucial, and I think that evolution can be frankly substantially enhanced.

But again to your point, the Internet is taking us away from vulnerability. It is a great place that we are going, and then we only have to ask the question to make sure that the connectivity, the baseline networks that serve the Internet, the backbones, are safe from terrorist incursion, and in that sense I include the very broad definition of terrorist, including industrial terrorists who would tend to slow down or move back our economy.

Senator WYDEN. Let me ask you now about national emergency communications sytems. In your testimony, you call for establishing a national emergency telecommunications access system to allow our public health and safety users priority access on the Nation's various telecommunications satellite wire line and wireless networks. How would you envisage that kind of system working?

Mr. MCCAW. That is a good question. I think first, we can recognize that a lot of the information that is now flowing will increasingly become discretionary data. In other words, if someone is out shopping on Amazon, it really is not necessarily central if we grab some of their data capacity and put it to the national defense. It is not like the old way, where we had a fixed number of dial tones and there was a certain grade of service allocated based upon a usage pattern. It was sort of .05 grade that on a normal day, 95 percent of the time you would get a dial tone, and that is binary.

In the new form, I think you can simply hive off some of this discretionary data that people might otherwise be doing and is increasingly part of the traffic, and grant it over to higher use, so priority access will not have the kind of negative repercussions, or the notion that we have now, where your home phone might not work if someone granted priority access to someone else, so frankly we see very little downside to that, and it is a matter, then, of getting us and those network operators to simply create a very simple and effective mechanism that is not subject to undue abuse.

Senator WYDEN. You also spoke in your testimony about what would happen with people in the urban areas in times of emergencies leaving those densely populated areas and going to rural areas, and you indicated the concentration of communications equipment in one area was in your view partially responsible for the telecommunications breakdown of September 11.

I think this is a very interesting point, one that really does warrant further analysis. I wonder what transmission technologies you think are most appropriate to ensure that we are addressing the needs of communications networks in both urban and rural areas in a time like that.

Mr. MCCAW. Certainly, I think I would view it as a wedding cake, perhaps a reverse wedding cake, but perhaps more similar that you have an overlay using all of the technologies. A wired technology is the most efficient way to get huge amounts of data from point A to point B, so if you know two places you want to go, we recognize that is the best way. Fiberoptic cable will do that the best.

It turns out we cannot count on people to stay in the same place, not to move, not to move the kind of traffic, and traffic moves during the day, so within that, then building almost like the arteries of a human being, you build along a structure that takes you all the way up to the ability to—so you go then, next to terrestrial networks that move large amounts of data, and the highly mobile networks, and then networks which are truly egalitarian in their coverage, those being the satellite kind of networks which cover everywhere, but frankly are less efficient simply because they do cover everywhere, and so each one is a little less efficient than the other to provide the flexibility, so it is an efficiency versus flexibility calculus, that in creating an entire mix gives you the kind of infrastructure that will allow you to have those elements occur.

However, I would say—and one can build within those structures flexibility for something like a flight from New York City, or pick any city. That you could concentrate the capabilities and have resources available to put in place rapidly to support those people as they moved out into a rural area where there are five people on a

party line, that is just not going to work, so having those ready to deploy is one element, warehousable, thought through, the NETGuard team ready to deploy and put that in place, as well as flexible and deployable capacity from satellites I believe all fit within that framework.

Senator WYDEN. I think the last question that I had for you, and you have been very patient, is what do you see as the biggest challenge to the communications infrastructure during a national emergency? As you said, the threats constantly change, and it is understood that terrorists are not technological simpletons. They are people who are studying these issues as well. What would you say would be the biggest challenge of the communications infrastructure during a national emergency?

Mr. MCCAW. If I were to answer, my biggest concern is the lack of flexibility in the infrastructure to accommodate massive changes and movement in demand, and I think that is what we heard the most about, so the challenge is to be able to respond rapidly, and by rapidly I mean much more quickly than we did in New York, to cover up the fact that there has been a massive dislocation of people from a place to another place and a massive increase in the need to move information of a critical nature, and that is the balance between the efficiency and the importance of that flexibility.

And so I think that our challenge is to make sure that those assets, the people and the equipment, are available to respond to those circumstances and they will occur if someone attacks, so it occurs from one of two circumstances. Either you move the people from where they normally would expect to be, or you damage the terrestrial infrastructure substantially, and on September 11 we had a bit of both, but frankly much less than it could have been.

Senator WYDEN. Well, to have someone like yourself—and I noted earlier, I think you are really regarded as the "Father of Wireless"—in a position to really call on the Congress to mobilize technology specialists, to mobilize scientists, is just an extraordinary contribution.

I want to see you proselytize, if I can use that word, the way for technology and for the kinds of ideas we are talking about this morning, and we are going to figure out a way to make sure that the government and people in the technology and science fields can come together so we can tap the potential that is out there. Your contribution has just been exceptional, and I know that this fellow resident of the Pacific Northwest is very appreciative. Is there anything you would like to add further, else we will excuse you for being so patient.

Mr. MCCAW. Thank you, sir, and I will proselytize on behalf of the far better minds that we could bring to the process, and it is an honor to be here with you, and thank you.

Senator WYDEN. Thank you very much.

Our next panel will be Mr. Roger Cochetti, Vice President and Chief Policy Officer, VeriSign; Ms. Julie Coppernoll of Intel; Mr. Will Pelgrin, with Governor Pataki and the Technology Office for the State of New York; Ms. Sarah Roche, Director of Client Services for Upoc; Mr. Stephen Rohleder, Managing Partner of USA Government for Accenture; and Mr. Joe Sandri, Vice President and

Regulatory Counsel for Winstar. So if all of you will come forward, we welcome all of you.

We thank you for your patience. We are going to make your prepared remarks a part of the hearing record. Why don't we begin with you, Mr. Cochetti, and let us get you a microphone, and you just proceed.

STATEMENT OF ROGER J. COCHETTI, SENIOR VICE PRESIDENT AND CHIEF POLICY OFFICER, VERISIGN, INC.

Mr. COCHETTI. Thank you very much, Senator Wyden, and thank you for accepting my statement as a part of the written record. First, let me begin by thanking you and the Members of the Subcommittee for sponsoring this series of hearings on what we think is a very important subject, and for the creativity and insightfulness of some of the ideas you have already proposed.

My name is Roger Cochetti, and I am Senior Vice President for Policy and Chief Policy Officer of VeriSign. I am pleased to be here today to address the issues of security and the Internet in the context of the September 11 terrorist attacks. Before I get into the main part of my comments, Senator, I did want to spend a moment and thank you and other Members of the Senate for the leadership you recently exercised in seeing the extension of the Internet tax moratorium.

While there were a cacophony of voices expressed on this bill and what it really meant, the reality is that this bill principally prevented discriminatory taxes against transactions that occur on the Internet, so it was a fairness measure, and we appreciate your and other Senators efforts to seek its support, giving the Internet industry time to deal with a very complex and difficult problem.

It is particularly appropriate, Senator Wyden, that VeriSign participate in today's hearings, because we are the premier trust company on the Internet, and perhaps more than any other company that one can think of, we are concerned about security of the Internet. VeriSign offers critically important digital trust service which include the most important elements of the Internet's domain name system called the DNS Secure Authentication Services in the form of digital certificates called digital signatures and payment services for web-based merchants.

In fact, we are the world's leading provider of domain name electronic authentication of web merchant payment services which together make up the essential elements of the Internet's infrastructure and without which the medium as we know it today could not function.

As the 1997 report of the President's Commission on Critical Infrastructure Protection observed, the Internet has emerged as the single pervasive infrastructure relied on by every other keystone segment of our economy, financial services, electric power, water, health care, manufacturing, transportation, and telecommunications.

Accordingly, all of us at VeriSign are acutely aware of the millions of retail merchants, universities, banks, businesses, libraries, museums, government agencies, and just plain families and individuals who rely on our facilities and our services billions of times each day, and we are acutely aware of our responsibility to main-

tain those facilities and services at the highest possible level of reliability.

Because of our unique and highly trusted role in making e-commerce and the Internet work, we have had a longstanding and fundamental commitment to security, thus, for us, the tragic events of September 11 provided a sad confirmation that our attention to security had not been misplaced. They also served as a reminder that our concern for security must be constantly refreshed and spread throughout the Internet.

Mr. Chairman, you have asked us to comment on the concept of a volunteer technology NETGuard and a strategic technology reserve. Our simple answer is that we think that these are very constructive ideas which obviously require a lot of careful thought. To help that careful thought, let me explain a little bit about how Internet security actually works. The Internet, as you well know, is a network of networks that come together mainly because of common interface software protocols and common numbering and naming systems and services.

The most visible and important of these systems that permit hundreds of thousands of distinct networks to communicate with each other is called the domain name system, or the DNS. This is sometimes referred to as the air traffic control system of the Internet, and under it, top-level domains permit users to navigate among web sites and e-mail users to identify each other and send e-mails to each other. Top-level domains include the ubiquitous .com, .net, .org, and such well-organized domains as .gov, .edu, and more than 240 country code top-level domains such as .cc or .uk.

Among our roles, Mr. Chairman, is to operate the most important elements of the DNS, and at this level we do a lot to maintain the integrity of the Internet as a whole, but the Internet is made up of more than the high-level domain-name system that we operate, and the standards, the high level of security standards we apply. We all know it is made up of millions of individual web sites and hundreds of thousands of interconnecting networks, and it is at this level of the network operator and the web site operator that the greatest vulnerability exists.

This background, Mr. Chairman, is important to understanding both the impact of the September 11 bombings on the Internet and the principal role that a NETGuard and a technology reserve might play with regard to Internet security. We all know today that the Internet continued to operate without any noticeable disruption after the September 11 bombings in part because of our uninterrupted operation of the key route servers and the common domains.

In fact, the Internet was an essential element in both response and recovery for the September 11 events. Millions of people were assured of the safety of their friends, families, and colleagues, for example, due to the smooth operation of the Internet, but while at least the high level of the Internet continued to operate smoothly on September 11, not all of it did. Some individual web sites and some individual networks were adversely affected, and some actually went down. It is at this level that we must focus our attention and consider the role of a NETGuard and a technology reserve.

Not every individual network and not each web site needs to devote as much attention to reliability and security as does VeriSign,

but many need to devote more, and many could use the help of qualified technology volunteers and reserves.

In conclusion, Mr. Chairman, while the Internet has changed quite a bit since VeriSign first assumed responsibility for major parts of the DNS in 1992, one thing has not changed, and that is the trust that people must place in the core network operators, our operation of .com, .net, and .org, is set at a level of reliability that is higher than the six sigma 99.999 percent that is used elsewhere in the industry standard, because we do not think we can take chances at people's ability to reach the web site that they wish to go to. We hope that the Subcommittee as it pursues this subject would focus on several key areas in addition to the NETGuard and technology reserve you have already suggested.

First, we must, as the White House has now done, identify this as an area of priority concern, second, we must, as the White House is now doing, develop a strategy for how to address threats to cyberspace, and third, we must closely monitor the infrastructure and seek early detection of threats to its operational stability.

There are specific things we think the Senate can do, Mr. Chairman and let me enumerate four of them, and thank you for your time in doing so.

One: The enactment of legislation that would reduce some of the risks incurred by companies if they share sensitive network information with Federal agencies concerned about security, a point you have already mentioned in your opening remarks.

Two: The wide use of security audits among both Federal agencies and Federal contractors would be a constructive step.

Three: The strengthening of various Federal consultative mechanisms that permit information-sharing and planning between the private sector and Federal agencies concerned with Internet security would be very constructive.

Four: Federal support for the wider use of both encryption and PKI-based authentication tools, which together can help ensure a significant increase in both the general security of the Internet and the security of e-commerce and e-government would be very constructive.

Thank you for inviting us to testify, Mr. Chairman. We look forward to cooperating with the Subcommittee if you pursue these important proposals.

[The prepared statement of Mr. Cochetti follows:]

PREPARED STATEMENT OF ROGER J. COCHETTI, SENIOR VICE PRESIDENT AND CHIEF POLICY OFFICER, VERISIGN, INC.

Mr. Chairman, Members of the Subcommittee: My name is Roger Cochetti. I am Senior Vice President-Policy and Chief Policy Officer of VeriSign, Incorporated. I am pleased to be here today to address the issue of the security of the Internet in the context of Homeland Security and the aftermath of the September 11th terrorist attacks.

It is particularly appropriate, Mr. Chairman, that VeriSign participate in today's hearings because we are the premier trust company on the Internet and, perhaps more than any other company that one can think of, we are concerned about the security of the Internet. VeriSign offers critically important Digital Trust Services, which include the most important elements of the Internet's domain name system (called the DNS), secure authentication services (in the form of digital certificates called digital signatures) and payment services for Web-based merchants. In fact, we are the world's leading provider of domain name, electronic authentication and Web merchant payment services, which together make up essential elements of the

Internet's infrastructure and without which, the medium as we know it, could not function.

As the 1997 Report of the President's Commission on Critical Infrastructure Protection observed, the Internet has emerged as a single pervasive infrastructure technology relied on by every other keystone segment of our economy—financial services, electric power, water, health care, manufacturing, transportation and telecommunications. Accordingly, all of us in VeriSign are acutely aware of the millions of retail merchants, universities, banks, businesses, libraries, museums, government agencies, civic organizations, and just plain families and individuals who rely on our facilities and services billions of times each day. And we are acutely aware of our responsibility to maintain those facilities and services at the highest possible level of reliability.

Because of our unique and highly trusted role in making e-commerce and the Internet work, we have had a long-standing and fundamental commitment to security. Thus, for us, the tragic events of September 11th provided a sad confirmation that our attention to security had not been misplaced. They also served as a reminder that our concern for security must be constantly refreshed and proliferated through out the Internet economy.

QUESTIONS POSED

In the Subcommittee's hearing announcement, Mr. Chairman, you have asked us to focus on a series of questions directed at the physical technology infrastructure resources—how they were impacted by September 11th, whether a corps of industry experts would benefit the response or aid in mitigating the impact of any future episodes, the usefulness of caches of spare supplies of technology appliances like cell phones and laptops, what other benefits might be derived from such preventive measures and organization.

As the Subcommittee knows, the World Wide Web operates in a hierarchical structure, with Top Level Domains (TLDs) serving as the main divisions among Websites. Domain names serve as the directories for the Internet and the Domain Name System (DNS) is sometimes described as the "air traffic control system of the Internet." TLDs include the ubiquitous dot com/net/org, such well-recognized domains as dot gov or dot edu, and more than 240 country code TLDs, such as dot us or dot uk.

The directory of all of these TLDs is created and distributed in a network called the Internet's Root Servers, and we operate the primary of these root servers, the so-called "A Root", which has been described as the single point where the entire Internet comes together. The authoritative list of the Internet's TLDs originates in our A Root and from there it is distributed to other root servers, including our own, around the world.

In addition, we operate the largest and most popular top level domains on the Internet, .com, .net, and .org, through a network of our own servers in North America, Asia, and Europe. Finally, we operate a number of smaller domains, such as .edu, typically under contract to the organization that is that domain's legal registry operator. In all of these DNS functions, we ensure that the Internet's DNS is available and reliable, notwithstanding both its dramatic growth (we now process more than 5 billion communications and transactions daily) and frequent unintentional and intentional threats to its operational stability.

Because VeriSign operates in this aspect of the domain name system at the highest level of the Internet's architecture and because many of the most serious threats to the security of the Internet occur at the level of the network or Website operator, we cannot claim to have a close view of some of the Internet's most vulnerable elements. It is clear to us, however, that all elements of the Internet, but most particularly network and Website operators who are the most at risk, would benefit from some form of catalogue of experts and reservoir of equipment. So, our short answer to the Committee's questions is generally "yes, it would be useful to pursue something like what has been raised" On the other hand, it would be impossible to predict that either a catalogue of experts or a cache of supplies will be necessary or useful in the event of any future emergencies, since so much depends on the context and circumstances.

BACKGROUND TO THE DNS

Thirty years ago, the U.S. Government began research necessary to develop packet-switching technology and communications networks, starting with the "ARPANET" network established by the Department of Defense's Advanced Research Projects Agency (DARPA) in the 1960's. ARPANET was later linked to other networks established by other government agencies, universities and research facili-

ties and during the 1970's, DARPA also funded the development of a "network of networks;" which later became known as the Internet. The protocols that allowed the networks to intercommunicate became known as Internet protocols (IP).

Until the early 1980's, the Internet was managed by DARPA, and used primarily for research purposes. Nonetheless, the task of maintaining the name list became onerous, and the Domain Name System (DNS) was developed to improve the process. Also, during this time, management of the network was passed from DARPA to the National Science Foundation (NSF), which referred to the medium as the NSFNET.

In 1992, the NSF entered into a Cooperative Agreement with Network Solutions, Inc. (NSI), which company was subsequently acquired by and merged into VeriSign. Under the Cooperative Agreement, NSI (now VeriSign) provided a variety of DNS services, including the domain name registration services and the operation of key parts of the Internet Root. Also in 1992, the U.S. Congress gave NSF statutory authority to allow commercial activity on the NSFNET. This facilitated connections between NSFNET and newly forming commercial network service providers, paving the way for today's Internet.

In 1998 and 1999, after authority over the Cooperative Agreement had transferred from NSF to the Department of Commerce, amendments were negotiated which introduced a new entity into the management of the DNS, the ICANN, and which introduced competition at the retail registration level for .COM, .NET and .ORG names. In the spring of 2001, the agreements between the Department and VeriSign, the Department and ICANN, and VeriSign and ICANN were substantially modified and extended; and later this year, new TLDs—such as dot info—were introduced. All of this against the backdrop of dramatic growth in the use of country TLDs, such as dot de and dot uk.

VERISIGN AND INTERNET SECURITY

While the Internet has changed quite a bit since VeriSign (through NSI) first assumed responsibility for major parts of the DNS in 1992, one thing has not changed much at all: The trust that others have placed in VeriSign and our commitment to the highest level of reliability. This is equally true of our digital signature services—on which hundreds of millions of dollars worth of transactions rely—as it is our domain name services—on which hundreds of millions of users rely. We bring that same commitment to our payment services and our expansion into new Internet services.

For example, in our operation of the dot com TLD, our standard of performance is such that we view the traditional "six-sigma" 99.9999 percent accuracy as insufficient, since it would permit some 40 bad Internet connections daily. If of those occurred on a site like aol.com or Amazon.com, the consequences could be significant. And so, that level of error is simply, for us, unacceptably high.

To engineer a secure system with the level of accuracy and stability required for a nearly error-free Internet is costly and complex. Unlike most other networking challenges, it cannot be shared with our clients and customers, whose technology investment need only be quite modest by comparison to fulfill their role as an ISP or a network operator. Unfortunately, this disparity can exist not only in required investment in physical infrastructure, but sometimes in security practices as well.

SINCE SEPTEMBER 11TH

As I mentioned earlier, the sad events of September 11th proved, if it was needed, that we must both prepare and carefully plan for security threats. Since then, we have expanded our efforts to reach out to both government and others in our industry and share both our experience and accumulated knowledge in this area.

Among the areas that we think deserve continued, priority attention are: 1. We must, as the White House has now done, identify this as an area of priority concern; and 2. We must, as the White House is now doing, develop a strategy for how to address threats at all levels to the Internet; and 3. We must closely monitor the infrastructure and seek early detection of threats to its operational stability.

Finally, in addition to the very important ideas that the Subcommittee is already considering, we would encourage the following steps: 1. The enactment of legislation that would reduce some of the risks incurred by companies if they share sensitive network information with Federal agencies concerned about security; 2. The wider use of security audits both among Federal agencies and Federal contractors; 3. The strengthening of various Federal consultative mechanisms that permit information sharing between the private sector and agencies concerned with Internet security; 4. Federal support for the wider use of both encryption and PKI-based authentica-

tion tools, which together can help ensure a significant increase in the general security of both the Internet and of e-commerce and e-government.

In conclusion, Mr. Chairman, let me say that the events of September 11th were pivotal for the Internet, as they were for almost every other major element in our society and economy. Fortunately, the Internet's core infrastructure, including the DNS, operated without interruption. But September 11th serves as a reminder that the next threat may not be so easily contained and it is for that threat that we must be prepared.

Senator WYDEN. Ms. Coppernoll, thank you, and let me take also special note of the fact that there is a very large employer in Oregon. Intel makes a variety of contributions on many fronts, but you and your Oregon folks have been exceptionally helpful on this, from Andy Grove to a variety of others. We are very appreciative of your ideas and input and all you did to immediately arrive in New York, so you proceed with your testimony.

STATEMENT OF JULIE COPPERNOLL, TECHNICAL ASSISTANT TO THE CHAIRMAN OF THE BOARD, INTEL CORPORATION

Ms. COPPERNOLL. Thank you, Senator Wyden. Thanks for including Intel, and thanks for including me. As you know, I am also from Oregon, and Intel is on the West Coast, so it was a little bit more difficult for us to respond immediately after the events of September 11. But Intel, all of our employees, the entire company had to try and find a way to respond, and we picked up a variety of people and we relocated ourselves along with some equipment with no immediate specific objective except to try to find a way to take the technology that we utilized on a day-to-day basis and to try to help.

We went there with hopefully just the goal of trying to find a way to take the technology, instill it, and set it up so that it could be used for rescue efforts for whatever efforts we could find. We set up three specific projects and offered them just as examples. They are detailed in the testimony, but when you talk about the context of a NETGuard, they might be some examples of ways and conditions and things that actually could be accomplished.

We set up Internet access for all of the FEMA search and rescue workers that were located in the Javits Center. There were approximately 700 of them with three telephones. They did not have access at all to anybody from the outside world, both from news media as well as just communicating with their friends, with their families. The ability to take the Internet and to take the computers and to keep their lives going while they attended to the activity they found incredibly helpful.

We also found that because we are on the ground we ended up finding ourselves in a situation of being IT support for the numerous FEMA workers that were also deployed, and many of those workers, along with the search and rescue teams, were deployed with some technology, not necessarily knowing how to utilize it, or what they can do with it, or what it can accomplish, and they might have some very, very basic skills, but not necessarily anything advanced to even do some of the very ad hoc things that we all know that work with it every day that it can do.

Because we were there on the ground we had lots of other opportunities, and as Director Allbaugh described, it was a little bit of randomness of knocking on people's doors, trying to say we are

here to help, we are here to help you in whatever way we can with whatever equipment and resources we can.

We found ourselves at the Ground Zero site assisting with the military, militia, National Guard reservists that were there trying to provide security. When we walked into that situation, they were keeping records of everybody that they were issuing access to the site on pen and paper, and had no ability to access it, query it. We set up a database for them, helped their processing time, and just tried to take the basic technology that they were not necessarily aware could even do anything for them.

Senator WYDEN. Are you saying that when you went there, there was essentially no information technology effort underway, people were trying to keep track of everything on paper and pencil?

Ms. COPPERNOLL. At the Ground Zero site, that was true. The way they were issuing passes, and ID, and badges, they were doing it on paper, and they did not have the technology that they had been deployed with. There were certainly pockets and areas where there were good examples of where it was being utilized, but that was not necessarily one of them.

And then additionally, one of the other larger projects that we got involved with, just simply also by being on the ground and offering assistance, was in the rebuilding business campaigns. Obviously, there were a lot of affected businesses. We also walked into the situation where there were phone calls coming in to city and State, and the chamber of commerce at the city, of businesses that needed assistance as well as businesses—I am sorry, businesses donating goods and services, and what Director Allbaugh described as no system to match those.

We built a system in about 2 days, of a database for them, while doing a quick search to see whether anything was out there, and so we built a matching system where they could take incoming calls, query them across three State agencies, government agencies, as well as people calling in donating goods and services, and they were just simply amazed that it could be done, and from our perspective it was obviously not a very time-consuming and not a very difficult thing to make their jobs and their lives a little easier.

So I offer those examples as just some of the areas. There were lots of other things that we ended up doing. We did end up being IT resources for a variety of organizations. Stuyvesant High School team has approached us to look at their network before they reopen for business—there are 4,500 students that have been out of the school for about 3½ weeks—when they return there to help bring their network back up.

All of these examples, and the many more that I could describe, were simply because we really were on the ground. We were offering assistance. We were not looking for any compensation, just walking around, and it was very difficult to find the networks, to find the places, knocking on doors.

It was very difficult to get in some of the doors if you were not already previously credentialed, and you walked up and said you are from Intel Corporation and you are here to help, and you have a team of technologists, at the same time trying to explain to people that do not necessarily know what technology can do for them, what it really can do for them in this particular situation, and try-

ing to pick the projects that will give them the highest return and get them up and running as quickly as possible.

For the search and rescue teams, for them it was the ability to keep their lives intact, the ability to do banking for them. They were displaced from their cities for 3 to 4 weeks, attend class, keep in touch with their families, send birthday cards. They would have available free time at 2 in the morning, and that certainly was not when they could pick up the phone and be in contact with anybody that they needed.

We know that technology is very powerful, it is very flexible, it is very dynamic. The more that it is pervasive, obviously, the more people depend on it, and when it is not available the more difficult it is, and so we were trying to make sure that it was available for anything that they could do.

The concept of a NETGuard, we know that there is a variety of ways that it could be implemented. Intel is committed to working through the ideas and finding the ways from the on-the-ground, ad hoc assistance, roll up your sleeves, what needs to be done to the variety of preplanning, predeveloping applications that could be deployed across a variety of State and Federal organizations for these types of situations.

When I took a taxi in one morning with the fire chief for FEMA and was discussing with him the moments of the day, he reminded me that there were 60 other Federal emergencies that were going on that were not getting the attention that New York City was, and when I was explaining to him some of the things we were doing, he said, "we could really use you at some of those other 59 places that we are equally deployed at that also do not necessarily have technology available to them."

There were lots of examples of National Guard people that were deployed out at the site that had laptop computers but did not necessarily know how to turn them into something that was useful for them.

So in conclusion, I think, Senator Wyden, one of the things you said earlier I think is exactly to the point, which is leadership and organization. There were lots of people that wanted to help. They just did not know what to do. They did not know how to take the technology that was available, and Intel was somewhat of an accidental leader in this process.

Because I was physically there, I had hundreds of people coming up to me: "How can we help? Just tell us what to do." We would try to say "what do you need?" to some of the organizations that did not know how to necessarily articulate what they needed. I would go off and say, "OK, what if we did this for you?" They would say, "that would be perfect." I would go off and give leadership and direction to people who could turn around and execute something, deliver something back to them in a day or two, and they could be on their way, and then they could depend on technology that was helpful to them while they were trying to do their jobs.

So I think organization and leadership, I think mobilization and quick response is obviously very important. We did not end up in New York until 5 days after the activity. We obviously would have been more helpful if we had been there earlier, being on the West Coast did not help. Getting across the country was very difficult,

and then trying to plan something from across the country, when Blackberry communication devices were about the only thing you could utilize. Just, it speaks to the obvious of anything we could do to preplan anything that we could do to have contingency plans in place. I think the technology industry itself would easily and happily come together to support that activity.

[The prepared statement of Ms. Coppernoll follows:]

PREPARED STATEMENT OF JULIE COPPERNOLL, TECHNICAL ASSISTANT TO THE CHAIRMAN OF THE BOARD, INTEL CORPORATION

Good morning and thank you to Chairman Wyden and the entire Subcommittee for the opportunity to testify before you today on behalf of Intel Corporation. As a leader in the computing industry and supplier to the Worldwide Internet economy, we were fortunate to have had the opportunity to put our resources to use assisting our Nation with the crisis the struck us on September 11th. Technology has continued to advance and integrate itself into our every day lives, such that we now depend on it for many things. In the aftermath of the tragic events of September 11th, we hoped to take this technology and use it to assist in the relief efforts. I am here to share with you what we were able to accomplish and what we believe technology could do in the context of a technology NETGuard.

As with many people across the country, we were alerted to the crisis through cell phones, pagers, e-mail, the Internet, television and phone calls. Suffering from shock and dismay, everyone at Intel, from our domestic to international shores, from engineering to marketing, from factory worker to executive, all wanted to find a way to assist. Being across the country did not deter or diminish our desire (much like the rest of the country) to find a way to assist. Intel donated $1 million to the Red Cross fund and matched employee contributions of $1 million but we still wanted to do more. We packed up available equipment (approximately 75 computers, networking equipment and digital cameras) and 15 employees headed for New York City.

After several days of planning (a very difficult activity from the West coast), our first project included a 24×7 Internet access center inside the Jacob Javits Center where the Federal Emergency Management Agency's Search and Rescue teams were stationed. Intel employees provided around the clock technical assistance for our 24 computers and quickly became IT support to the variety of other staff and volunteers working within the Javits center.

The 700 Search and Rescue members stationed there would visit us before and after they returned from 12-hour shifts at Ground Zero. Our computers reached close to 100 percent utilization 24 hours a day. They reached out to friends, they assured family members of their safety, maintained contact with their jobs, completed their banking, sent birthday cards, and even attended class over the Internet. Many of the rescue workers were not familiar with personal computers: for them we provided a high touch personal assistance, a sort of digital concierge. Others were PC experts, and although they had brought laptop computers, they had no connectivity until we set up a wireless network.

Technology made the experience a little more palatable for many of these individuals. We received many tear-filled words of thanks from rescue workers who were able to stay in contact with their loved ones, in an environment with only 3 phones available to the 700 workers. I have also included one of the thank you notes we received via e-mail:

Subject: Thanks from Miami Florida

I would like to say thanks to the group from Intel that was present at the Jacob Javits center in Manhattan, New York after the Sept 11 tragedy. I am a member of South Florida Urban Search & Rescue Team FL–TF 2, we were deployed to New York and during our 16-day journey, our team, as well as other US&R teams had to leave our families and jobs to assist the city of New York. Your team arrived and setup a well-needed link to our families and the rest of the country.

At 1:15 p.m. 9/11/01 most of the US&R teams were alerted or standing vigil, awaiting word from FEMA. We were all cut off from the media and eventually ended up in military installations, basically we were not able to watch the news because we were preparing our equipment and ourselves for what we were about to see. When the computers were setup, we were able to see the news from around the world as well as our hometown. My family really appreciated the fact that I could send a picture of myself along with an e-mail. My young children can't relate to words, but the picture really made their days. I am speaking for everyone by say-

ing thanks and please send this to everyone that was present as well as your superiors.

Sincerely, Kevin Bartlett, Cooper City Fire Rescue.

We sought out other projects to utilize our fully contained (generator, trailer, satellite dish) mobile PC center. We were invited to station ourselves next to the Office of Emergency Management's ground zero branch at PS89. This facility was operating in conjunction with the Militia Forces of the State of New York, who were providing perimeter security. Until our arrival, the security management system was a pencil and paper operation. We built and deployed a simple security application data base for their use. After a security management team member was approved for access to the site, he or she entered the individual's name along with other personal information into the data base before issuing an access badge. Besides an increased processing time (three times faster), this method allowed the records to be backed up, transferred, printed, and accessed later for quick verification. We quickly become the IT support at PS89, supporting any technical needs that the operating team had.

Another area of focus for us was rebuilding businesses. We were invited to participate in some of the early discussions and planning for the rebuilding activities that The New York City Partnership began. Intel supported this organization with personal computers for their volunteers, developed an Internet application that would log donations of goods and services and track affected businesses. A link was established between the City and the State call centers to allow these organizations to work together, on the same data and the same customer. We stationed an Intel employee full-time at the Partnership's location to assist as affected businesses began articulating their technology needs and to decipher what they needed and match it to what was available. Technology assisted in unifying three government teams trying to service the same audience.

Our presence and willingness to help provided us with several other meaningful opportunities. Although it was difficult to broadcast our offers of assistance, word eventually spread through casual networks. We assisted the Board of Education with an evaluation of the Stuyvesant High School's network before they reopened the school. We loaned laptops to the several members of the FBI/NY Port Authorities joint terrorism task force. We restored infrastructure for one of our customers, Reuters. We relocated and helped rebuild operating infrastructure for an Intel Capital Portfolio company. We loaned equipment to several small businesses trying to restart operations. We counseled and consulted with several non-profit organizations as they began to restore operations.

We wish we could have done more. We let the grass take root where it did.

Technology played a critical role on September 11th. Many of us used it to communicate with our loved ones, our family members, our friends and our business associates in order to ensure their safety, to hold hands with each other over the Internet, and share in each other's pain. Within a few hours of the initial attack, the Internet, computers, pagers and our cell phones supported our quest for information. Some of the statistics that have been reported show the following happened with the first few hours: 1.2 billion instant messages were exchanged on AOL compared with 650 million normally/day. Volume was up 40 times at Yahoo!News and Yahoo's new PC-phone calling was up 59 percent. CNN.com received 9 million page views within hours versus 11 million in an average day. For the handheld Blackberry e-mail device, traffic was up 57 percent. The Internet gave us an instant platform for community action with $50 million in donations collected within the first 3 weeks.

There is no question that technology could have done more to assist in the aftermath of the disaster by providing quicker access to information as well as supporting more families, more businesses and the rescue teams. There are many examples of where technology could have been deployed to ease and speed access to information, to organize and plan, collect and distribute critical information where the IT industry could help. This leads to the discussion of a Technology National Guard. From the experiences that I described above, I can confidently say that the IT industry has both opportunity and skill to contribute. Technology is clearly a critical part of our nations infrastructure. Ensuring that the technology is available and utilized to its capacity is something that the IT industry or trained IT professionals are uniquely positioned to accomplish.

There are many different focus areas that a NETGuard could focus upon and different services that could be provided running the gamut from basic to the more complex and technical. Our industry can assist in developing contingency planning for both physical disasters as well as cyber security of the infrastructure. Our industry could assist in predefining and developing applications such as the program we

developed to service an immediate need of matching donated goods to those in need or the security data base we created. The IT industry combined with the communications industry is certainly able to provide some level of assistance in returning critical infrastructure from data centers to communications networks to operation. Finally, the type of on the ground, unplanned, ad-hoc assistance that was needed in its simplest form (roving IT support) was critical for on the ground communications and operations.

The solution is not obvious. A single plan may not be the immediate solution, but rather multiple plans that support a variety of needs. We certainly support exploring the options as the concept is developed. I believe there are many members of our industry that are anxious to share what we learned, how we conduct our business and how we could, at the minimum, provide ideas on how to utilize the technology that is available today. Industry could lead to train and organize teams that could be deployed in emergency situations. Teams could participate in pre-planning and development of packaged solutions to be deployed by National Guard teams. National Guard deployment skills could include IT workers deployed for that specific purpose. Other options are viable. Intel is interested and committed to explore the options with each of you as the proposal is solidified.

I am grateful that I had the opportunity to organize and lead Intel's effort. I am grateful that I work for a company that was willing and able to be of assistance. Thank you for the opportunity to speak with you today. I am happy to answer any questions you may have.

Senator WYDEN. Well, as an Oregonian, and someone who has watched how you all have made a difference, we are very proud, and as you know, there was an exceptional effort on the part of many in Oregon. Sho Dozoro, one of our leading travel executives, led a very large delegation to New York that was widely publicized. I do not think what Intel did was so widely known.

I really disagreed with only one thing you said, and you said you all provided accidental leadership. I do not think this happened by accident. I think it happened because you and Andy Grove and others cared, and you said, "We may be 3,000 miles away, but we are going to mobilize." We are going to mobilize with the trucks, the equipment, the personnel, and the other resources that you wanted to bring to bear to make a difference. I think Intel really provides a textbook case of what a company that cares can do in a time of emergency, so we are going to be calling on you often, and know that this Oregonian is plenty proud this morning.

Ms. COPPERNOLL. Thank you, and we are happy to help, and we would have done more. We were accidental just from the fact that we did not go out necessarily to mobilize industry or big groups of people, and in some cases we ended up doing that.

Senator WYDEN. Excellent testimony.

Representing the State of New York is Mr. Pelgrin, who is Technology Officer for Governor Pataki, who has also been very interested and helpful in terms of working with us. We welcome you. We will make your prepared remarks part of the record, and you may proceed.

STATEMENT OF WILLIAM F. PELGRIN, DIRECTOR, NEW YORK STATE OFFICE OF TECHNOLOGY

Mr. PELGRIN. Thank you very much. Good morning, Mr. Chairman, Senator Allen. On behalf of Governor Pataki, I am honored to represent New York State and discuss the role of technology in responding to the events of September 11. The tragic events of that day have forever changed the things that we understood to be absolute truths on September 10. Never before has the ability to communicate, gather intelligence and protect public safety been as

heightened as it is now, and technology will be a focus of many of these efforts.

Technology played an important role in responding to the terrorist attack of September 11. I will quickly highlight what technology was most impacted, what technology was most helpful and effective, and what technology we need for the future.

First, what technology was most affected. New York worked to quickly assess the technology impact, determining that some 2,250 data circuits were damaged or destroyed, affecting 40 State agencies. Connectivity to New York City was gone, and many critical applications were down. We prioritized the 2,250 circuits into a list of approximately 500 priority circuits based on criteria of public security, public safety, and human services. Because of our prior planning for Y2K, the State agencies had contingency plans in place and, in fact, deployed to ensure that critical programs continued.

Currently, 29 of the priority circuits are still out. However, we are working diligently to get them operational as soon as possible.

I would like to take a moment to commend Verizon for its response not only to addressing the government's need in a timely fashion, but also for restoring the Stock Exchange, the financial center of the world. If anyone saw 140 West Street, Verizon's central office, you would know that was a monumental task to get us back up and running.

I would like to highlight two areas in which technology was most helpful. First, application development. A 24×7 emergency call center was operational within 1 hour of Governor Pataki activating the State's emergency management office. It was staffed within that hour with 150 operators. The outpouring of support in the hours and days following the attacks was tremendous. We quickly realized that we needed a system to capture the data on the donations being offered. By September 13, we had an operational web-based application for collecting this information.

Over 187,000 calls were logged. At our peak, we were answering over 27,000 calls per day. 50,000 offers from businesses and citizens donating goods and services were entered into the database. The application provided an easy and efficient tool for emergency management personnel to access the donation and to allocate resources.

In my opinion, one of the best technologies deployed in New York State's response efforts was the use of our digital ortho imagery. We quickly determined the need to fly to the disaster site. With the cooperation of the Federal, State, and local entities, we obtained clearance to fly to the restricted zone. We flew each day from September 13 through October 23. We flew there to capture three different types of images. The first was digital ortho imagery. That is digital aerial photos with all the distortions removed. Thermal imagery, which measured surface temperatures, and LIDAR, which is light detection and ranging, to measure elevations.

The reason digital ortho is such a great technology is because of its ability to overlay the data. As the maps that I have brought today illustrate, digital ortho photos were overlaid with thermal images and gas line data. We were able to put the proximity of the fires to the gas lines.

We also used thermal images taken over multiple days and overlaid them to show where fires were either expanding or receding. Information was provided daily to FEMA, the State, New York City Emergency Management Office, and the fire department. This data was a critical component in the response and rescue efforts.

Looking forward, the technology direction for the future is the implementation of New York State's statewide wireless network. As you clearly stated in your memo, Mr. Chairman, responders were hampered by a lack of interoperability among communications systems. New York State's current wireless communications system is failing. Replacement parts are difficult, if not impossible to obtain, and most importantly, the current system is not interoperable.

New York State will provide the necessary backbone infrastructure for a statewide emergency communications system. This new system will allow responders to communicate with each other. The current status of this initiative is that there is a draft request for proposals on the street for comment. We are hopeful to issue that in final in early January, or by late January.

In conclusion, in addressing the purpose of this hearing, Governor Pataki's philosophy with regard to technology has always been one of collaboration and mutual coordination, developing strong public and private partnerships. We cannot do it alone. Our successes are collective efforts.

We look forward to working cooperatively with the Federal, State, and local governments as well as the private sector to prepare for and respond to any disaster. I am reminded of a quote by St. Francis of Assisi: "Start by doing what is necessary, then do what is possible, and suddenly you are doing the impossible."

Mr. Chairman, the Governor would like me to extend his appreciation for your leadership and that of Senator Allen and the other Senators in this effort. Your support is especially appreciated in these trying times.

Thank you very much.

[The prepared statement of Mr. Pelgrin follows:]

PREPARED STATEMENT OF WILLIAM F. PELGRIN, DIRECTOR,
NEW YORK STATE OFFICE OF TECHNOLOGY

Good Morning, Senator Wyden and members of the Committee. On behalf of Governor George E. Pataki, I am honored to represent New York State to discuss the role of technology in responding to the events of September 11.

The tragic events of that day have forever changed the things that we understood to be absolute truths on September 10. There will be—and must be—much change as we move into this new, uncharted world.

Never before has the ability to communicate, gather intelligence, and protect public safety been as heightened as it is now and technology will be the focus of many of these efforts. Technology played an important role in responding to the terrorist attack of September 11.

- Geographic Information Systems (GIS) to obtain sophisticated, detailed imagery of the disaster site;
- Databases for tracking financial donations and supplies; and
- Use of the Internet as a communication tool.

Many agencies and individuals came together in solidarity to join in the rescue operation.

We have a tremendous opportunity now to critically examine our emergency response capabilities, not only in New York, but across the nation, and across jurisdictions. We need to examine the policies, procedures, and priorities that currently exist within our information technology infrastructure and, using some of the les-

sons learned from September 11, assess where we need to go from here. By learning the lessons from the past and working and training together for future responses, we can better prepare to meet the challenges that will face us all in this new era. Our efforts are focused on four phases: Protection, Detection, Response and Recovery.

I'd like to take this opportunity to discuss some of our response efforts in New York State, and illustrate some of our lessons learned. I'm prepared to address what some of the communications issues were, and what we've learned from this.

WHAT HAPPENED

Moments after the attack, Governor Pataki activated the State's emergency management operations center (SEMO), under the direction of James Natoli, Director of State Operations. Twenty-plus agencies responded to SEMO and operated on a 24×7 basis.

The Governor activated the statewide Mobilization and Mutual Aid Plan making available to New York City all State resources of the fire services of the State of New York. The Governor's Capital Region Urban Search and Rescue Team was also activated and remained active for 16 days in assisting in recovery. The Insurance Emergency Operations Center (IEOC) was also activated. By the following day, executives from the largest writers of personal and commercial lines insurance in the NYC area were assembled and working from the IEOC. A satellite video link between the IEOC and the State Emergency Management Office was created to enhance communications. Immediately real time information was exchanged with SEMO, the insurance industry, the press as well as consumers. A dedicated toll-free hot line was activated for consumers to call for information relating to insurance.

A temporary adjuster permit application process was utilized. This allowed insurers to apply for temporary adjuster permits over the Internet instead of completing paper applications. Almost 400 permits were issued.

Other security issues were addressed offsite, including the monitoring the State's data center and networks. State Police were immediately dispatched to secure the data center locations; security was heightened for all State office buildings.

A 24×7 emergency call center was activated within 1 hour, staffed with 150 operators. Over 187,000 calls were logged from businesses and citizens offering to volunteer or donate goods and services. At our peak, we were answering over 27,000 calls per day. All information was recorded in a database that was used by SEMO officials to deploy resources.

New York worked to quickly assess the technology impact, determining that some 2250 data circuits were out, affecting 40 agencies; connectivity to NYC was lost, and many critical applications were down.

Because of our prior planning for Y2K, State and city agencies had contingency plans in place that enabled them to respond to the loss of key telecommunications lines. We were able to implement alternate emergency procedures, ensuring that critical human service programs continued.

We prioritized the 2250 circuits into a list of approximately 500 priorities, based on public safety and human services, and subsequently added another 100 circuits to the list based on their impact, such as Banking and Tax operations. We worked closely with the impacted agencies and our business partners to address the situation. In some cases, we were able to provide the agencies with alternative solutions via our Statewide network or other providers.

The Tax Department's NYC Office was located in the World Trade Center. In addition to the terrible loss of life, we lost our business records—case records that were painstakingly developed as part of our audit program. The potential loss related to audit recoveries that have been lost or deferred has not been calculated. We lost all our desktops and servers. A lesson from this experience is that while we, like most organizations, are diligent in regards to backup and offsite storage of our mainframe data, we must carefully assess the extent that our business records are maintained on servers and desktops, where we may not be as diligent in our backup and recovery procedures. Do we have the ability to recover our business records in the event that the site is destroyed?

The NYC Downtown Hospital, one of the major staging areas for victims, lost communications. Cell phones and runners were the only forms of communications available. This highlights the need for backup or redundant communications systems.

The outpouring of support in the hours and days following the attacks was tremendous. However, we quickly realized that we had to devise a system to capture the data on the donations of finances and supplies. By September 13th, we had an

operational web-based database application for collection of this information. We received over 50,000 offers from businesses and citizens donating goods and services:

- IBM provided PDAs, desktop computer, services to a variety of organizations; and also provided office space to relocate State agencies' operations; Microsoft has donated $10 million in funding and resources to assist with the World Trade Center disaster response efforts;
- AOL Time Warner hosted the donation website; and
- JP Morgan Chase provided free banking services to assist in the World Trade Center Relief Fund.

And the list goes on and on . . . ranging from medical supplies and offers of medical services to recovery equipment.

A critical component in New York State's response efforts was the use of Geographic Information Systems, commonly known as GIS. Using GIS, we were able to collect detailed imagery that proved vital to the fire department and other emergency responders. Using thermal imagery, we were able to determine where the "hot spots" were, and the location and progression of underground fires. This imagery was overlayed by gas pipe line data to provide crucial information about the location of fires relative to gas lines. This data was used by the NY Fire Department in deploying their resources. We contracted with EarthData, a firm out of Maryland, for daily flyovers of the disaster site, and processed that raw data into usable imagery within 8 hours—a process that would normally have taken weeks.

SECURITY HAS BEEN A NUMBER ONE PRIORITY OF GOVERNOR PATAKI PRIOR TO THE DATE CHANGE (Y2K)

Governor Pataki has long been active in ensuring that appropriate response mechanisms are in place in the event of a disaster—whether it be natural or otherwise. He made information security a priority during Y2K. In this regard, Governor Pataki placed a priority on the activities of the State Disaster Preparedness Commission, issued an Executive Order establishing a Commission on Terrorism and most recently established the Office of Public Security.

The Office of Public Security, under the leadership of James Kallstrom, was created to to ensure central coordination of all State activities related to public security. These activities have proven critical in our ability to respond to September 11 and for any future event that may occur.

As we move forward, the technology areas that we are focusing are: enhancing security, GIS technology, deploying wireless technology, and enacting enabling legislation that will secure the legal framework for these initiatives. These are recommendations that apply to NYS and the Nation as a whole. Our success can be best assured by careful coordination with the Federal Government as well as the private sector.

ENHANCING SECURITY:

Physical Security: New York is establishing a statewide critical infrastructure workgroup, that will be responsible for gathering detailed information about the State's critical infrastructure, and developing strategies for protecting it, including scenario simulation exercises.

Information Security: We are addressing this on a number of fronts. In early 2000, the Governor established the State's first statewide information security office to provide a coordinated, comprehensive approach to developing policies and procedures to protect the State's critical technology infrastructures, such as networks and data centers. The Governor required every agency to have an information security officer.

In addition, the Office for Technology is enhancing the State's intrusion detection and vulnerability scanning abilities. The Office is looking to use its successful collaborative agreement model used in our GIS data sharing cooperative to establish cooperative Security partnerships within State agencies, and other entities. Currently, we are sharing information with 60 State agencies and five other States.

We have drafted legislation that will further enhance information security, and protect the confidentiality of information regarding known vulnerabilities.

Information Security is the number one priority for the Governor's Office for Technology. It is imperative that we employ the proper methods and procedures to protect, detect, respond and recover from attempts to compromise the integrity of critical infrastructures. The Office for Technology works closely with the new Office of Public Security in recommending technology strategies in protecting the State's critical infrastructure and in researching and recommending technologies that can improve physical security for the State.

The Office provides the overall information security policy, direction and training to State agencies' Information Security Officers. It also provides:
- Security Training;
- Statewide Security Policy & Procedures;
- Security Incident Handling; and
- Annual Security Conference for State and local government.

ENHANCING GIS

One Agency w/GIS Expertise is given "Lead Responsibility" for GIS during emergency activations.
- Management of GIS services at the emergency operations center.
- Management of a mobile onsite GIS unit.
- Distribution of geospatial data and analyses to all participating agencies.
- Coordination of GIS resources available from other agencies.
- Contracting for additional geospatial resources as needed.
- Getting Relevant Geospatial Information to Field Staff & back.
- Effective contact with emergency response personnel in the field is critical both to ensure that GIS products and services are available to those in need and to ensure their needs are accurately identified. It is also critical to insuring accurate information from the field is brought back to key decisionmakers at the emergency management operations center. Locating a mobile GIS unit as close to the emergency site as possible is vital. GIS staff must not only provide geospatial information, but also educate onsite emergency personnel on how it can assist them.

RECOMMENDED ACTION ITEMS:

- Identify primary GIS contacts for each agency involved in the emergency response (including 24 hour contact work, home and mobile phones and e-mail addresses), their responsibilities, and the data that their agency can provide.
- Maintain GIS space, hardware, and software capabilities at the emergency operations center.
- Establish emergency services contracts for aerial imagery data.
- Establish a "mobile mapping & GIS unit" at or near the site of a disaster.
- Review the need for hard copy maps onsite both at the emergency operations center and at the emergency site itself.
- Establish procedures for collecting and forwarding geographically referenced data from the site to the Emergency Operations Center.
- Establish local interface/liaison procedures.

New York State has implemented the following:

Created the Office of Public Security, with lead responsibility for developing a comprehensive statewide strategy to secure New York State from acts of terrorism or terrorist threats. The Office will coordinate all State efforts to detect, identify, address, respond to and prevent terrorists acts from occurring within the State.

Assigned one agency (Office for Technology) with lead responsibility for technology:
- Maintain a technology contact list, including up-to-date phone numbers and e-mail addresses;
- Coordinate all applications development, planning and support in preparation for, as well as during an emergency;
- Coordinate information technology security measures, as necessary.

Implement monthly multi-agency meetings to focus on a particular topic and develop a set of defined deliverables:
- Business Continuity;
- Disaster Recovery;
- Physical Security; and
- Information Security.

COMMUNICATIONS

- Developing a web template to provide clear and concise information for the public.
- Implementation of Wireless Communications

We are developing a Statewide Wireless Network. Using state-of-the-art technology, this new radio system will provide both voice and data communication capability. In crisis situations, where seconds count, all responders will be able to instantly communicate with each other.

Under the new system, New York State will provide the necessary backbone infrastructure for a statewide emergency communications system which localities may join at their option, based on each individual locality's needs. The Statewide Wire-

less Network is committed to pursing partnership arrangements with government organizations to ensure maximum interoperability, reduce overall costs of the system, and reduce the time necessary for implementation.

As Mr. Joe Allbaugh, Director of FEMA, testified on October 16, "if there is a single item that we could do, (it) is to make sure that police, fire, emergency responders can communicate with one another. Oftentimes, I go into a community and there are all types of bands and frequencies used and folks, literally, who are responding to an incident can't talk to one another."

The bravery and courage of our firefighters, police and other emergency responders to the horrific events of September 11th has given special meaning to the word heroes. If we are to protect their lives and safeguard the public we serve, we must provide these and other heroes across the State with the ability to communicate effectively and quickly with each other.

Because natural and man-made disasters know no bounds.

We are now living in the world of wireless communications. Our first responders, however, use incompatible and often obsolete radio equipment—complicating their ability to communicate with each other. In fact, runners are often still used for communication by first responders in emergencies.

We are also ensuring redundancy and back-up capabilities through our Statewide communications network.

Governor Pataki's philosophy with regard to technology has always been one of collaboration and mutual coordination—developing strong public and private partnerships.

"We can't do it alone; our successes are collective efforts."

In that regard, a proposal to coordinate the local, State, Federal and private sector as envisioned in the NetGuard proposal is commendable.

We respectfully suggest that any such coordinated effort bear in mind the first responders are at the local level. Federal and State government need to be in a position to assist and support, not impede these efforts.

Any applications that are developed must be readily accessible by the each State's Emergency Management Office.

We need to build on the foundation that has already been established—and works well—from the local emergency offices, to the State emergency operations center, to the Federal emergency office. We must not add more layers that make effective response more difficult.

The Governor would like to offer New York's assistance in providing our resources that are already or will be in place, including our databases for critical infrastructure, donations, and asset management.

By working collaboratively across all levels of government, we can achieve success and provide an even-more significant response.

Thank you for the opportunity to be here this morning.

Senator WYDEN. Thank you very much. We will have some questions in a moment. Thanks for working with us.

Ms. ROCHE.

STATEMENT OF SARAH ROCHE, DIRECTOR, CLIENT SERVICES, UPOC, INC.

Ms. ROCHE. Good morning, Mr. Chairman and Senator Allen. Thank you for the opportunity for me to be here today and to submit my testimony as part of this important hearing. I am here as a New York citizen to give my personal account of the morning and the day of and the day following September 11.

I was at work at our offices on Broadway and Wall Street, which is adjacent to Trinity Church, two blocks south of the Twin Towers. As I look at the map there, you might even be able to see where our offices were, although they are not marked on there, it is that close.

I work for a wireless company, Upoc, which provides a platform for sending SMS text messages from any cell phone or PC to groups of cell phones across all carriers and devices.

The morning of September 11, I was at work at 8:15 for a client conference call. I was on that call when the first plane went into

the Tower. Not knowing what was really going on, we continued our call until we heard a loud boom and our building shook.

We ended the call, and I immediately noticed my cell phone had begun beeping with messages. The text messaging group that includes all Upoc employees was buzzing. One advised us not to go to work, or to head away from the World Trade Center if we had started that way. Another said that there was a plane that had gone through the World Trade Center.

I looked out of our office window and saw the people outside scurrying toward the bottom of the island of Manhattan. It was like a scene out of a movie. People were running, car alarms were going off, and there was a sense of sheer pandemonium.

Uncertain of what was going on, I tried to look online, but web sites were flooded and unreachable to find any news. Then I tried to use the phone, but to no avail. Messages, however, kept coming through our phones, and the five of us that were at work were discussing what we had been reading, and any other information that we had been able to find out on our own.

At this point, we actually left the building to see if we could make sense of what was going on. None of us imagined that we had been targeted by terrorists and that our lives were in serious jeopardy. I tried to place cell calls, and then realized that everyone around me was plagued by dead cell phones. Already, the lines of the pay phones were 20 people deep.

I returned to our office, thinking that amidst the chaos, familiar shelter made some sense. In our wildest dreams, we could not have imagined what would be happening next. Land lines and cells continued to be inoperable. None of us knew what to do. We were continuing to get messages telling us where to go, who was where, what were the right things to do. Within a few minutes, we accounted for everyone who was at work and in the office, and that people who were actively managing this group from various locations throughout the city were accounting for the rest of the employees.

Though I still could not believe planes had crashed into the Towers, it was what my coworkers had told me, and even though it was shocking, it was comforting to have information from a trusted source. I remember specifically saying to my coworker that terrorists really knew what to go for. Clearly, the World Trade Center and the Pentagon would be the obvious targets. A few minutes later, a text message came through that the Pentagon had also been hit.

Just when we returned to our building, it began to shake, and the plumes of smoke that everyone would see billowing on television in the next few days were the reality outside of our office windows. We all hit the ground and hoped that our building would remain stable. As we ran for the hallway, I grabbed my purse and my phone to escape our building.

We were brought to the bottom of the building, and we were all text-messaging other Upoc employees who could maybe phone our families and loved ones to let them know that we were OK. We continued to get updates from them letting us know who they had been in touch with and what to do.

We eventually left our building to go eastward, only to be caught outside when the second Tower fell. It again, was hysteria, but we found another building and continued to console each other and be in touch with the rest of our coworkers, letting them know that once again we continued to be OK, and let any of our friends and family know that information.

Personally, it was how I reached my fiancee. He was at Arlington Hospital, and they had gone into disaster mode, meaning that no outside lines were available. Since he is seldom allowed to use his phone inside hospitals, I expected it to be off, but it was my only option. The text message did reach him, and I received my first text message ever from him. He was thankful to hear I was OK, and glad to have a way to get in touch with me.

We all made it home OK, and were glad to be away from downtown. Over the next week, our text messaging was crucial to our work and well-being. Phones, cell and land, did not work regularly for weeks, though the text messaging did.

One coworker who was a volunteer with EMT let us know what was needed, or what we could do if we wanted to help in any of the efforts around the city. We accounted for everyone eventually, and continued to be in touch while we all dealt individually with the impact on our lives. Today, we continue to work in the financial district in the same offices, blocks away from Ground Zero, and still we have intermittent problems with phone lines, but it is less and less every day.

Our lives day-to-day have a sense of normalcy now, though they are forever irreversibly changed. Thank you for letting me have the opportunity to speak today.

[The prepared statement of Ms. Roche follows:]

PREPARED STATEMENT OF SARAH ROCHE, DIRECTOR, CLIENT SERVICES, UPOC, INC.

Good afternoon Mr. Chairman and Members of the Subcommittee. Thanks for the opportunity to speak today. I am going to give an anecdotal account, and I will be followed by Alex LeVine, who will explain the technology behind the story. For the sake of brevity, let me get right into the details of September 11th. I was at work at our offices on Broadway and Wall Street—which is adjacent to Trinity Church, 2 blocks south of the Twin Towers. I work for a wireless company, Upoc, Inc., which provides a platform for sending SMS Text Messages from any cell phone or PC to groups of cell phones, across all carriers and devices.

The morning of Sept 11th, I was at work at 8:15 a.m. We had a client conference call, which I was on when the first plane went into the towers. Not knowing what was really going on, we continued the call until we heard a loud boom and our building shook. We ended the call and I immediately noticed my cell phone had been beeping with messages. The text messaging group that includes all Upoc employees was buzzing. One advised not to go to work, or to head away from the WTC if you'd started, another said that there was a plane through the WTC. I looked out our office window and saw people outside scurrying toward the bottom of the island. It was like a scene out of a movie, people were running, car alarms were going off and there was a sense of pandemonium. Uncertain of what was going on, I tried to look online, but websites were flooded and unreachable. Then I tried to use the phone—to no avail. Messages kept coming through and the 5 or us that were at work were discussing what we'd all been reading on our phones as well as any dribbles of info we'd found out on our own. At this point, we actually left the building to see if we could make sense of what was going on. None of us imagined we'd be targeted by terrorists and that our lives were in serious jeopardy. I tried to place a cell calls and then realized that everyone around me was plagued by "dead" cell phones; the lines at the pay phones were already 20 people deep. I returned to our office, thinking that amidst the chaos familiar shelter made some sense. In our wildest dreams we couldn't have imagined what would happen next.

Landlines and cells were inoperable. None of us knew what to do. We were, however, continually getting text messages. Within a few minutes, we'd accounted for who was at work and the people who were actively managing the group from various locations were accounting for all employees. Though I still couldn't believe planes had crashed into the towers, it was what my co-workers had told me, and even though it was shocking, it was comforting to have information that I trusted. I remember specifically saying to a co-worker that terrorists knew what to go for—clearly the WTC and the Pentagon were obvious targets. About 5 minutes later, an SMS came through about the Pentagon.

Just when we returned to our building, it began to shake and the plumes of smoke everyone saw billowing on TV were the reality outside our office windows. We all hit the ground and hoped that the old building would pull through. We ran for the hallway, though I paused to grab my purse and phone.

We were brought to the bottom of our building and were all text messaging other Upoc employees who could maybe phone our families and let them know we were okay. We continued to get updates. We eventually left our building to go eastward, only to be caught outside when the second tower fell. It again was hysteria, but we found another building and continued to console each other and be in touch with the rest of our co-workers as well as friends and family who were using text messaging. Personally, it was how I reached my fiancé. He was at Arlington hospital and they'd gone into disaster mode, meaning no outside lines were available. Since he seldom is allowed to use his phone inside hospitals, I expected it to be off, but it was my only chance. The text message reached him and I received my first text messages ever from him—he was thankful to hear I was okay.

We all made it home okay and were glad to be away from downtown. Over the next week our text messaging was crucial to our work and well-being. Phones—cell and land—didn't work regularly for weeks, though text messaging continued to work. One co-worker was a volunteer with EMT and he let us know what was needed and what we could do. We accounted for everyone eventually and continued to be in touch while we all dealt individually with the impact in all our lives.

PREPARED STATEMENT OF ALEX LEVINE, VICE PRESIDENT OF OPERATIONS, UPOC, INC.

Good afternoon Mr. Chairman and Members of the Subcommittee. The events of September 11th affected all of America, but those of us who work in the Wall Street area of downtown Manhattan were among the most impacted. I am honored to have this opportunity to relay to you my company's experience, and to detail some key technologies which withstood the attack, and which I believe could be leveraged in the future for more effective emergency management.

My company, Upoc, Inc., provides a platform for sending SMS Text Messages from any cell phone or PC to groups of cell phones, across all carriers and devices. The offices of Upoc, Inc. are located two blocks south of the WTC in New York City. As the planes hit, the first thing that happened was phone lines began to overload from people all around the world calling their friends and family in NYC to check on them. All the access tandems for long distance lines in the city began to fill up, and there was no way to make calls in and out of the region, although local calls still worked. But as the events continued to unfold, saturation of phone lines increased—cell towers and local switches reached maximum voice capacity and stayed there, and people watching the conflagration couldn't make calls on their cell or office phones—there were simply no available lines.

Once the Twin Towers fell, things got even worse as Verizon's downtown switch got knocked out. Even more local landlines stopped working, as the switch served a large percentage of the lines in Manhattan. Cell phones worked rarely.

Later in the afternoon, as the Verizon headquarters began to fall over, power was turned off for the entire downtown region. This took out the cell towers downtown, as well as all office phones and e-mail systems—all electrical communications that were not battery powered. Some buildings had backup generators, but as the power outage stretched into days, the generators ran out of fuel, and any systems based in lower Manhattan were taken totally out of commission.

The experience of the staff of Upoc was affected directly by these breakdown phases. After the first plane, we were in landline communications with each other, but the ability to get through got worse and worse. After the towers fell, the landlines were useless; in my home in Manhattan, the local Verizon switch was so overloaded that I couldn't even get a dialtone—it was as if everyone was picking up their phones at once, and there wasn't even enough bandwidth for a dialtone, let alone an actual call.

We immediately switched to other realtime or near realtime, non-voice communications. Before we were evacuated from the building, PC-based instant messenger and e-mail were working well, as the internet connection to our office seemed to be holding up fine, even after the first building fell. The whole time, we also used our own technology to communicate via SMS text messages, in groups and one-to-one, on our cell phones.

Once we were evacuated, we used two key wireless technologies: RIM's Blackberry wireless e-mail pagers, that are connected to our e-mail systems, and Upoc's text messaging platform over SMS. Both worked perfectly, but once power went out to our building, the e-mail servers on which the Blackberries depend shut down, and we stopped using them. At that point, SMS text messaging was all we had left, and we used it *almost exclusively* for communications between employees, family and friends for the next week, as phones lines still gave busies and our office remained off limits and without power.

FAILURES

Because of obvious dependencies on the physical infrastructure, anything in the downtown area requiring a wireline network connection or power was at risk of failure. This means that everything from office phones and servers, to payphones and trading terminals, were unusable.

The inability to handle call load in the general voice telecom networks was due to systems that the telcos simply never built for such capacity. In fact, it would be financially unwise to build a voice network with the amount of overcapacity that would be required to support the Sept. 11th level of calls, since it is such a rare occurrence.

WHAT WORKED

The key communications technologies that continued functioning on 9/11 were based on 4 factors: (1) battery powered network devices like cell phones connected via (2) wireless links to (3) packet-based redundant networks using resources on (4) remotely collocated servers. More detail on each of these 4 factors is in the written testimony [see the end of this document]. The Upoc application continued to work during the attack and aftermath because it leverages all of these factors. But it could not work without something called SMS.

SHORT MESSAGE SERVICE, OR SMS

Today, every digital cell phone in the U.S. is capable of receiving SMS messages. These are up to 160 character text messages that travel across the same network as voice calls, but in a different channel. In Europe and parts of Asia, it has become extremely popular to send SMS messages between cell phones, but it has yet to really catch on in the U.S.

SMS runs over the SS7 layer of the telephony network. This is a packet-based, but non-internet, technology that handles tasks such as call set up and caller ID. Imagine, for example, when you get called on your cell phone: you see the caller ID of the person calling you. This is a tiny piece of data, delivered to your phone right when it first rings, over the SS7 layer. Once the Caller ID packet is delivered, you don't need to get any more packets, so you are no longer using any of the capacity of the SS7 portion of your carrier's cellular network. Once you pick up and start talking, you have grabbed a circuit on your carrier's network, and it is one of a limited number of circuits—if enough people in your cell tower coverage area are on their phones, no one else can receive or make any more calls, because all the voice lines are taken.

However, even when all the voice lines are taken, the SS7 packet-based portion is there, available to transmit packets to other cell phones in the coverage area, but more or less unused, as no new calls are coming in, so no Caller ID packets need to be delivered.

That SS7 bandwidth can be used to deliver text messages to phones, even when no calls can be made, and it does so dependably. Even if a cell tower goes down, if your phone can get the tiniest bit of signal from another nearby tower—not even enough for you to make a call—the SMS text message can be delivered to your phone.

Upoc's platform takes the 1-to-1 aspects of SMS, and extends it to groups. One SMS message can be sent, from a cell phone, through Upoc's service and it can go out to a group of any size, reaching each group member on their cell phone wherever they are. It was our own technology that allowed us to track down all of our employees after the attack to confirm everyone was OK, and it allowed us to begin plan-

ning for temporary office space and coordinate employees immediately, even with all our office e-mail and voice systems down.

Any wireless data-based system will be the best bet for communications survival during an attack or catastrophe. Many cellular carriers are rolling out new wireless data networks now, called GPRS and CDMA 1XRTT, that will improve availability for packet-based, battery powered, wireless devices. However, these new devices have yet to be purchased in most cases. SMS is already on every digital cell phone, on every digital cellular network.

CONCLUSION

SMS is then an ideal transport for emergency messaging, available now. Cell phones are battery powered and wirelessly connected to a packet-based network that is sitting on a redundant core, speaking to a remote server. All the key factors for catastrophe survivability are in place.

However, there is not a very high level of awareness in the U.S. about SMS Text Messaging. As Upoc's story shows, and as, I hope, the arguments I outlined explain, SMS was an invaluable communications tool in a very dire communications situation on and after September 11th. We believe that there is a need and an opportunity for the government, carriers, and messaging providers like Upoc, to make U.S. citizens, 120 million of whom own cell phones, aware of this already existing technology. I would like to thank the subcommittee for this opportunity to discuss our experience, and I look forward to answering any questions you might have.

KEY FACTORS:

1. Batteries. Sure it is obvious, but when the power goes out, you need communications to run on some sort of supplemental power. Although generators and uninterruptible power supplies kept servers running for some time, they could only last for a brief period, as none of these things, in everywhere but the most emergency-oriented facilities, were supposed to keep systems running for a week. Servers and other machines designed to be plugged into wall outlets are rarely designed to conserve power effectively, and they drain batteries very quickly. They also tend to depend on physical wire connections to voice and data networks.

Cell phones and pagers are ideal devices when power is out, since they were designed from the start to run off batteries. They also work wirelessly. So they form the most straightforward foundation to any emergency communications planning.

2. Wireless links. Wireless links are a clear way to avoid having lines "cut" by explosions or attacks, since there are no lines to cut. However, cell towers can lose power or be destroyed, rendering the area around that tower incommunicado for the customers of that cellular provider. Since the core of wireless carriers' networks are generally redundant, if the tower does keep power it is generally going to continue providing service. Cell towers are then one of the most reliable communications points since they sit on redundant core networks and connect from there to cell phones through unseverable wireless links.

This is in contrast to wireline switches, which might still be running, but if their copper trunks are destroyed they have no one to provide service to: the core on which they sit might be redundant, but the clients they serve have only one point-to-point connection, which fails completely when severed.

Wireless data links have the most promise, since they do not suffer from the circuit-switched hard limit that cellular voice does.

3. Packet-Based Redundant Networks. Voice networks have a hard limit on the number of people that can use them at one time. This is because every voice call requires a full circuit to be opened between callers, and it is held open for the duration of the call—they are circuit-switched. If all lines going in and out of a region-say downtown Manhattan, or a long distance access tandem, or even a cellular base station-are in use, that's it: no more calls can be made.

Data networks work on the principle of packets. Data, like an e-mail message, is broken into little pieces that are transmitted across a network in an almost arbitrary fashion and reconstituted at the other end; as such, there isn't any hard limit on the number of messages or number of people served by a data network. Congestion can occur, and messages will arrive more slowly, but as long as the network remains intact, the message will get through. In the case of Sept. 11th, intact data networks rerouted their packets around the failed networks at WTC and essentially allowed continued operation throughout, so e-mail and instant messages to New Yorkers got through when calls did not. In many cases, voice *worked*, but was so overloaded that most attempted calls resulted in busy signals. Not so with packet-based data.

However, it is critical that a network remain *intact.* Most of the cores of New York's network providers are based on SONET rings. These are fiber loops that carry the bulk of the network's data from one point to another. Because of their ring topology, they allow a cut to occur, and can still connect between any remaining points on the network. Unlike the telephone lines that were connected to Verizon's WTC switch, which were point-to-point and simply died after a cut, the cores of both data and voice networks' SONET architecture allowed for continued operation.

4. Remote Co-location of Servers. In a disaster, we now see that we need battery powered wireless communications devices, and packet-based, redundant core networks, to maintain connectivity. The last component for success is the survival of the servers that handle the data, the machines through which the communications devices reach each other.

Our RIM Blackberry pagers fit my first 3 criteria: they were battery powered, and kept working after power was cut; the data is delivered in packets, which kept working, albeit a bit more slowly due to all the traffic. However, once the power to our e-mail servers failed, the Blackberries became useless, because they had been set up for e-mail only. In fact, Blackberries can be set up to communicate directly through the core of RIM and Cingular's networks (called "PIN-to-PIN"), but few people had set that up, since most Blackberries are installed with e-mail functionality only.

Upoc's servers are located in New Jersey, quite far from Manhattan. As a result, communications that depended on Upoc's application kept working: the servers were in a remote location, far from likely attack targets, the devices were battery powered and as long as the data networks between the devices and Upoc's servers were redundant and stayed up and available, the Upoc application kept working for us and our customers.

Senator WYDEN. Well, thank you for coming, Ms. Roche. Nothing is a substitute for having someone like yourself, who has been through it, sort of take us specifically through the implications of trying to reach loved ones and family. I sure appreciate you doing this. We will have some questions in a moment.

Mr. Rohleder, please proceed, and thank you. I also want to commend Accenture for all you did as well.

STATEMENT OF STEPHEN J. ROHLEDER, MANAGING PARTNER, USA GOVERNMENT MARKET UNIT, ACCENTURE

Mr. ROHLEDER. Thank you, Chairman Wyden, Senator Allen.

I am Steve Rohleder, the Managing Partner of the USA Government Market Unit of Accenture. Accenture is the world's leading provider of management and technology consulting services and solutions. We employ 75,000 people in 46 countries, including 30,000 here in the U.S., and we serve clients across all industries. I commend you for holding today's hearing, and I appreciate the opportunity to testify.

My testimony today will focus on three areas, Accenture's work with the City of New York post-9/11 to establish the Family Assistance Center, discuss the importance of contingency planning and infrastructure and security investment to meet the opportunities and challenges ahead, and finally I will discuss ways to advance public-private collaboration.

On the days following the terrorist attack on the World Trade Center, Mayor Giuliani's office asked Accenture to manage the establishment of a new Family Assistance Center. In less than 72 hours, 130 Accenture employees worked with city agencies and charitable organizations to spearhead the transformation of an empty warehouse in Manhattan to a fully functioning facility.

The Center serves as a primary resource facility for relatives and friends of those missing since the disaster, as well as those who

lost their jobs or homes as a result of the disaster. Since the facility opened, there have been visits for more than 60,000 families.

The Center provides a variety of services, including tracking the status of applications for death certificates, distribution of memorial urns, analyzing information regarding the number of missing persons, and helping families apply for financial assistance. In the future, we believe the victims of terrorism should be able to access government assistance with the least amount of trauma. This can be achieved by working with the private sector to utilize best commercial practice and technology.

Over time, virtual assistance can and should be provided to all victims on an ongoing basis. The response in New York City has been a model for public-private partnership, hundreds of government agencies, relief organizations, and companies working together to restore and rebuild the return to normalcy.

In order to respond more effectively in the future, contingency planning is essential. While many of our business and government clients had continuity plans, most did not seriously consider the types of threats that have become familiar in the past 2 months. Both government and industry need a new kind of planning for the future that focuses clearly on initiating immediate recovery on a moment's notice, and anticipating the loss of facilities, not just recovery of software systems, establishing temporary operations so that companies and government are not scrambling to identify a location to set up shop during a crisis.

Third, we should focus on determining permanent operating facilities, including geographic concentration and dispersal of employees, and finally, preparing for economic impacts in advance of a crisis, government and private sector should work together to closely ensure that all are better prepared in the future.

One way to advance this cooperation is by fostering public-private partnerships, an effort that Accenture strongly supports. Accenture recently deployed a manager to serve as a Department of Commerce fellow to assist small and medium businesses affected by 9/11. Earlier this year, we supported Congressman Tom Davis in the establishment of a digital tech corps which would provide the exchange of government and industry IT professionals for up to 2 years. Should the tech corps legislation pass, loan executives could serve to develop best practices for emergency IT responses.

Creating a NETGuard to respond to information technology needs in a crisis is an interesting idea that should be examined further. Clearly, the details need to be fleshed out. However, I would like to highlight a few areas for the Subcommittee's consideration.

Considering that NETGuard volunteers could come from across the IT industry, proprietary data and technology should be protected, skills of volunteers to be matched to the needs of a crisis, a person with project management skills may not have the technical background to restore the components of a telecommunications network. Companies affected by future crises and who also employ NETGuard volunteers may need an exemption from releasing personnel for service if they are key to a company's ability to restore its own operations.

Finally, another way that government could access centralized IT services rapidly in a crisis would be to have the Federal Emergency

Management Agency, in conjunction with the Office of Homeland Security, establish IT crisis recovery contract vehicles similar to those used to address surge capability by the Department of Defense. The centralized contract vehicles would only be activated in crisis situations, and would allow government to obtain technology services in specific competencies on an as-needed basis.

Finally, Accenture strongly supports the Office of Homeland Security playing an integral role in helping the public and private sectors come together to provide continuity planning, enhanced cyber security, and serve as a home for innovative ways for intergovernmental and public-private information sharing to defend against any new terrorist attacks. Any new efforts to address cyber attacks should be coordinated with the Office of Homeland Security, FEMA, and State and local authorities.

In conclusion, the terrorists sought to undermine our businesses and to destroy the American way with fear. As business and government leaders, we can stand united to take the best we have to offer to secure this Nation's infrastructure and to take this opportunity to lead with innovation.

Mr. Chairman, thank you for inviting me to appear before the Subcommittee. I look forward to your questions.

[The prepared statement of Mr. Rohleder follows:]

PREPARED STATEMENT OF STEPHEN J. ROHLEDER, MANAGING PARTNER, USA GOVERNMENT MARKET UNIT, ACCENTURE

Chairman Wyden, Senator Allen, Members of the Subcommittee, I am Stephen J. Rohleder, the Managing Partner of the USA Government Market Unit of Accenture. I appreciate the opportunity to testify before you today.

Accenture's expertise is in the areas of technology and business. We employ more than 75,000 people in 46 countries who serve clients across all industries—telecommunications, electronics, high technology, financial services, resources, products, and Federal, State and local governments. We serve 86 of the Fortune 100.

As part of the normal course of business, we conducted an assessment of the situations faced by our clients, the impact on their industries, and how they should meet the opportunities and challenges ahead. I will share some of these findings and suggestions today. I will also comment on the idea of establishing a NetGuard to respond to future terrorists attacks.

GROUND ZERO

On September 11th, Accenture, along with the rest of the civilized world, watched in horror as the tragic results of unprecedented terrorism unfolded in New York, in Pennsylvania and in our nation's Capital. Our employees, our clients, our families and friends have all been directly touched by the devastation. We, like so many New Yorkers, were also called to serve in a government-private partnership to help the city in a time of crisis.

In the days following the terrorist attacks on the World Trade Center, Mayor Guiliani's Office asked Accenture to manage the establishment of a new Family Assistance Center. More than 130 Accenture people, along with some of their families, worked with the Office of Emergency Management, the New York Police Department, the Medical Examiner, the Red Cross, the Mayor's office and other private companies to create the new center, which enables people to gain information about loved ones, as well as to leave information about the people they are seeking, request a death certificate or apply for financial assistance.

In less than 72 hours, Accenture employees spearheaded the transformation of a barren warehouse located on Pier 94 in Manhattan to a fully functioning facility, installing 130,000-square feet of carpet, over 250 workstations, a network supporting more than 250 personal computers and 500 phones and free Internet access. The Center has served as the primary resource facility for relatives and friends of those missing since the disaster. Since the facility opened, there have been more than 60,000 family visits. The families who utilize the services of the Center include not only those who lost loved ones, but also those who lost their jobs or homes as

a result of the disaster. Once operational, Accenture built applications to facilitate processes that helped people, including tracking the status of applications for death certifications, distribution of memorial urns, and analyzing information regarding the number of missing persons.

There are a number of important lessons learned from the establishment of the Family Center.

• Governments must be able to establish crisis management centers rapidly to meet unexpected large-scale human disaster.

• They need to utilize information technology and customer relationship management techniques to ensure that citizens are served rapidly and easily.

• Victims of disaster or terrorism should be able to access the assistance of the government with the least amount of trauma—one-stop assistance should be the goal.

• Governments need to team with the private sector to provide services using best commercial business processes and technology.

• Over time, virtual assistance can, and should be provided to families on an ongoing basis.

AMERICA ON NOTICE

Today, the markets have rebounded to the levels they were in early September. And the good news is that market indicators point to further gains in 2002. The terrorist attacks on America have failed to achieve their financial objectives, but we *have* been put on notice. We have learned that war can now be waged on our shores, and our infrastructures are tempting targets.

The attacks on the World Trade Center were in many ways a wake up call—vivid illustration of the centrality of our information infrastructure and its value in times of threat—to government, to business and to individuals. Cell phone calls from stricken United Airlines flight 93 over Pennsylvania seem to have played a role in preventing the terrorists from reaching their intended target. Wireless e-mail messages from World Trade Center brought family members together and sometimes grief. Internet messages got through when traditional phone networks strained under the load of record call volumes.

Unfortunately, the value and vulnerability of our nation's information infrastructure has not gone unnoticed by those terrorists who would target the United States. The proliferation of the Internet and the increased integration of our nation's infrastructures create the opportunity for a new form of asymmetrical threat. Many government and private sector computer systems are interconnected through the Internet, a network originally designed to support robust network interconnection, not high security.[1] The original Defense Advanced Research Agency (DARPA) design has worked remarkably well, with over 400 million users now online worldwide.[2] New technology developments including Internet-enabled cell phones, wireless e-mail and mobile commerce are expected to expand Internet usage exponentially. And yet as Internet usage increases, the likelihood and impact of cyber terrorism goes up concomitantly—unless we take actions now to appropriately secure the infrastructure for public and private sector use.

The President's appointment of Pennsylvania Governor Tom Ridge to head up the Office of Homeland Defense sets the stage for unprecedented cooperation and coordination between the private sector and government to tackle these cyber security weaknesses. It also can serve as "home" for innovative ways for intergovernmental and public-private information sharing to defend against any new terrorist attacks.

In fact, the United States and many of our allies present a wide array of potential targets beyond military systems. These include: the air traffic control system, banking and capital markets, telecommunications systems, power supplies, water resources, and oil and gas delivery systems. Let's look back, and then look forward.

THE AFTERMATH

In the aftermath of September 11, our clients faced a number of challenges. We need to learn from this, and certainly leading executives and organizations must be prepared for business continuity along the following five areas.

(1) Initiate Immediate Recovery—Most large companies had effective disaster recovery programs for major software systems. But data located in departmental "local area networks," many of which perform very important business functions, was lost. Many did not figure on losing facilities. Many small and medium enterprises had

[1] David D. Clark, "The Design Philosophy of the DARPA Internet Protocols," Proc. SIGCOMM '88, Computer Communication Review Vol. 18, No. 4, August 1988, pp. 106–114)

[2] *CIA World Factbook 2001.*

greater challenges, often unable to afford or focus on business continuity planning. Government, including Congress, faced challenges being on-line and connected to its constituents when buildings were evacuated, highlighting the need for a "virtual" government planning.

(2) Establish Temporary Operations—Companies scrambled to secure temporary working facilities in hotels, or through telecommuting from home or other offices, but business communications capabilities continue to be limited because so much of lower Manhattan's phone system was concentrated in hubs that were located in or near the World Trade Center. Despite remarkable efforts by the phone companies involved, lines are often inadequate, access to voicemail and e-mail—required business tools for many—remains severely limited.

(3) Determine Permanent Operating Facilities—Companies are evaluating the wisdom of geographically concentrated staffs as they make plans to secure permanent facilities. Some are dispersing employees in the local area or beyond. These shifts in worker locations are causing aftershocks in areas ranging from city planning to suburban telephone systems.

(4) Embrace the Virtual Workplace—Organizations can reduce the risk of terrorist attacks by employing information technologies that enable "virtual" workplaces. Examples include: instant messaging, electronic mail, groupware and web conferencing, some of the most reliable technologies during and immediately after the attack.

(5) Preparing for Ensuing Economic Impacts—Many companies immediately understood what this "demand shock" meant to them—and they moved to reduce their costs accordingly. A few businesses are thriving. For others, it will take months or even years for the full impact to be understood. "Supply" must be adjusted accordingly.

These are basic elements of business continuity planning. Most business and government continuity plans we have seen didn't seriously consider the types of threats that have become familiar in the past 2 months. Businesses and Government need a new kind of planning for the future. We believe there is a strong role for the Office of Homeland Security to play in helping coordinate Federal, state, local and private sector coordinated continuity planning.

LOOKING FORWARD FOR BUSINESS AND GOVERNMENT PLANNING

As business and organization leaders, we are all trying to grapple with a great deal of uncertainty. What then lies ahead for business and government in this new era? Will fears of terrorism lock the economy in a death spiral, or will fiscal and monetary policy result in a soft landing and quick recovery?

We must be better prepared for attacks on our soil, we must integrate greater security in what we do, and we must work together as public and private sectors. As business leaders, we are challenged to do what we have done so well in the past: marshal technology and our creative genius to continue to drive better business and society toward a successful future. Government, too, must heed this wake-up call, and move promptly to protect its information systems. Beyond the need we have discussed to have business continuity planning that recognizes today's threats, there are several things we must do:

INVEST IN INNOVATION FOR GLOBAL COMPETITIVENESS

At a time when terrorists would want us to retreat, we need to recognize where we are in the current business and technology cycles. We are seeing business trends like outsourcing creating efficiency and an improvement in global standards of living. We are seeing the "industrialization" of systems development—using labor arbitrage and new technologies to improve cost efficiency and productivity. In fact, despite the spectacular decline of technology markets recently, technology is poised for a rebound. Every important digital technology over the past 50 years has seen a boom followed by a major shakeout that lasted typically four to eight quarters. After the shakeout, the surviving competitors enjoyed marked growth, as much as 100-fold. New high-speed Internet-ready computers, broadband networks, wireless devices and, most importantly, software that enables dynamic inter-business commerce, will power new approaches to commerce while fueling the next market advance. Government and business leaders must have the courage to drive investment. Policymakers must take advantage of bipartisan times. Businesses could take advantage of historically low interest rates to deploy new innovation for stronger global competitiveness tomorrow. We must invest for the future.

LEVERAGE TECHNOLOGY TO ACHIEVE SECURITY WITHOUT SACRIFICING PRODUCTIVITY

Conventional wisdom is that increased security costs more without any benefits. When we think in traditional terms—hiring high quality security guards, increased monitoring, etc, that is certainly true. On the other hand, investments in security-related technology often bring many side benefits that lead to greater productivity. A new operating system is more secure, but also has many more features to be exploited. In many organizations, over 90 percent of the operational information is still in paper form. Investment in digital content management systems can replace paper with their digital equivalents so information can be safely distributed and easily reproduced. But at the same time digital content can be used for new, more efficient approaches to training. Certainly the Federal Government could serve as a model, streamlining paper-heavy processes, while utilizing technology to tackle some of its most pressing homeland security training needs.

Investment in a high quality, secured network could allow greater collaboration with reduced travel. Advances in networking hardware and software enable us to achieve new levels of inter-enterprise integration that further secure while streamlining transactions with trading partners. Investment will also provide the added benefit of network redundancy.

Mobile wireless devices and advanced security techniques can create safe, virtual workplaces for our people. This technology exists today. The right investments in technology for security's sake could in fact stimulate key sectors of our economy. As policymakers, for example, you should consider using tax incentives like accelerated depreciation of technology equipment to stimulate such investments.

Technology can be used to protect people as well as networks. For example, in the area of airline security, Accenture recently conducted a study that found six of 10 airline travelers who have canceled their upcoming holiday flights are doing so because of security concerns and the likelihood of long lines. Technology can help improve security long before passengers reach the airport, increasing passenger confidence and ease of travel.

BUILD PUBLIC/PRIVATE PARTNERSHIPS TO FURTHER A SECURE COMMERCE INFRASTRUCTURE

While we will face challenges in the short-term, economic and technological indicators point to recovery next year. Among the many opportunities we see, one stands out: the secure, broadband digital commerce infrastructure. Technology companies have worked to establish portions of this infrastructure, but the job remains unfinished. Today, the right public-private partnership can help create secure information infrastructure that will be the backbone of tomorrow's economy. Mechanisms to stimulate deployment including regulation, tax incentives, and government funding, should be considered.

Congress should examine existing emergency response processes already in place through the Federal Emergency Management System and State and local authorities. While industry can dedicate volunteer resources, knowledge capital and skills, industry efforts should complement Federal emergency management efforts to organize and provide infrastructure. Partnerships should be created at the Federal, State and local level.

Clearly, there is a need for the public and private sectors to carefully plan for the most efficient and effective response to terrorist attacks. When the city of New York asked Accenture for help, we were able to respond without haste because of the capabilities, resources, and dedication of our employees. The response was not limited to network-building and technology, but implementing industry best practices and coordination among agencies. There are a number of areas where Government can help facilitate public-private partnerships.

NetGuard

The concept of a NetGuard is an interesting one that should be examined further. Developing a trained and technology-able corps of volunteers to support information technology restoration could be beneficial to government, the community and business. Clearly the details need to be fleshed out. NetGuard may have some practical problems in implementation. The following are four recommendations for the Committee's consideration:

(1) Protection of proprietary data and technology will be a major issue for businesses. NetGuard volunteers would likely be drawn from across industry and from competing companies. There would need to be safeguards put in place to provide protection for proprietary assets accessed by NetGuard volunteers.

(2) A major challenge for the deployment of a NetGuard would be matching skills with need. For example, a project manager might not have the technical skills to

restore the various software and equipment elements of telecommunications networks. A process would need to be developed to effectively match technology skills to need in times of crisis. In addition, a protocol would need to be developed to determine how NetGuard volunteers would be deployed. Government should consult closely with the private sector on these plans to ensure fairness.

(3) Companies will need to plan for and assess the impact of losing key personnel for an extended period of time during a crisis. There may also need to be exemptions provided for personnel in companies that are directly impacted by a crisis who may be NetGuard volunteers.

(4) Training of a NetGuard force would need to be dynamic to keep up with technology and allow for flexibility since volunteers will likely be located across the United States. Accenture is working with a number of clients to migrate more "on-site" classroom training to web-based training in a "virtual" classroom. Given the rapid changes in the industry, web-based training could allow for rapid deliver of training material while also reducing costs.

Digital Tech Corps

Accenture strongly supports public-private partnerships. In response to September 11th, Accenture offered a manager to become a fellow at the Department of Commerce. This fellow is assisting small to medium-sized businesses get back on their feet.

Earlier this year, Accenture supported legislation introduced by Congressman Tom Davis that would establish a Digital Tech Corps. H.R. 2678, the Digital Tech Corps Act would provide for the exchange of government and industry IT professionals for up to 2 years. While we supported the concept to help ease the shortage of IT workers in the Federal Government and to spur cross-pollination of best practices, we believe it could also serve as an opportunity for public and private sector IT professionals to share best practices for emergency IT responses.

Office of Homeland Security

We also believe that the Office of Homeland Security should play an integral role in helping the public and private sector provide continuity and disaster planning for their communities while coordinating an effective and coordinated response in times of crisis. Information technology should be utilized to facilitate more effective communication and coordination between all appropriate law enforcement agencies in a secure, real-time fashion. We believe that by utilizing commercial technology, some of the challenges of interagency and intergovernmental agency communication and cooperation could be diminished significantly.

CONCLUSION: MAKE THIS OUR FINEST HOUR

The terrorists sought to undermine our businesses and to destroy the "American way" with fear. As business and government leaders, we can stand united to take the best we have to offer to secure this nation's infrastructure and to take this opportunity to lead with innovation. Years from now, as we look back upon this time, let history show that we did not give in, and that the tragedies of September 2001 spurred us all to our finest hour.

Mr. Chairman, thank you for inviting me to appear before the Subcommittee. Accenture is committed to working with you as you further develop the NetGuard proposal.

Senator WYDEN. Thank you. We very much appreciated all Accenture did to step in and assist.

Mr. Sandri, welcome.

STATEMENT OF JOSEPH SANDRI, SENIOR VICE PRESIDENT AND REGULATORY COUNSEL, WINSTAR COMMUNICATIONS

Mr. SANDRI. Thank you, Mr. Chairman. Timothy Graham is in New York today, I appreciate, and he appreciates, the opportunity to comment.

Good morning. My name is Joe Sandri, and I am Senior Vice President and Regulatory Counsel with Winstar Communications. I am also here on behalf of the Association for Local Telecommunication Services, or ALTS, and the Wireless Communications Association. Today, I will discuss my company's participation in network survivability and restoration efforts after the recent tragic

events, provide data on what worked, and suggest improvements needed to capitalize on the lessons learned.

Winstar is a fixed wireless facilities-based broadband services company providing high speed Internet and competitive local exchange services. In terms of geographic coverage and total megahertz, Winstar is the Nation's largest holder of commercial spectrum, with ubiquitous holdings covering every road, building, and State in the country.

Winstar is also the largest winner of Metropolitan Area Acquisition (MAA) local service contracts from the Federal Government. Winstar is the only MAA contractor offering services primarily using fixed wireless. Winstar is currently in the sale process under section 363 of the U.S. Bankruptcy Code.

In response to the horrible events of September 11, Winstar created voice and data network access in New York City, Northern Virginia, and Pennsylvania. In lower Manhattan, Winstar provided facilities-based access to three City of New York emergency relief centers, FEMA, the U.S. District Court for the Southern District of New York, the U.S. Marshal Service, the Department of Corrections, Citigroup, brokerages, insurance companies, and many other facilities. Winstar also met requests for help from Sprint, MCI, and other carriers to provide network assistance. In many buildings, Winstar was, and in some instances still is, the only service remaining.

Communications users learned hard lessons. In a definitive September 22 *New York Times* article, third party experts reached conclusions about the physical structure of the U.S. Internet and communications network, noting that many users relied heavily on built-in redundancies, but, quote: "The disaster did expose some of the limits of those contingency planning. Some of those multiple lines traveled the same conduits to the same routing centers. If something happens to those conduits or routing centers, as it did in many cases in September 11, all the redundancy in the world does not help. All the cables would be damaged."

"Roy A. Maxion, Director of the Dependable Systems Laboratory at Carnegie Mellon University in Pittsburgh, has long preached the value of physical diversity in networks. 'I would not want to be alarmist about this,' he said, 'but what I think is interesting is how the system is not set up. A lot of these contingency plans are not in place.' He added that 'as a Nation, we are dangerously vulnerable.'"

On November 9, Harvey Pitt, who is Chairman of the Securities and Exchange Commission, stated: "Wherever possible, business continuity planning should seek to avoid reliance on single points of failure in critical systems. Single points of failure can occur in ways that are unforeseen, and even odd. The lines of competing telecom providers may all lie side-by-side in old, obscure conduits."

And on October 19, the *Wall Street Journal* ran a front-page article detailing the dangerous concentration of communications traffic in the offices of the incumbent local exchange carrier (ILEC). The article notes that often nearly all local and long distance traffic (not to mention the bulk of all international traffic), often routes through a single ILEC office in even our major cities.

Earlier this week, Verizon Chairman Ivan Seidenberg endorsed the redundant facilities.

What are some solutions? They belong in three broad categories: (1) Public education and direction by government; (2) Establishment of physical diverse facilities-based networks that enter and exit buildings at physically separated points; and (3) Modification of the Federal Emergency Management Agency (FEMA) warehouse system.

Congress, the Executive Branch, and expert agencies such as the FCC and the National Institute for Standards could help by issuing bulletins advising the public of: (1) Dangers of improper reliance on systems that may be redundant in some fashion but do not have physically separate facilities-based networks which ingress and egress the buildings at points separated to the maximum extent feasible, for example, by levels in a multifloor building, or by at least 100 feet in single floor buildings; and (2) Discussing possible requirements that these basic issues be addressed on a priority basis.

As you are likely aware, lower Manhattan is home to the greatest number of communications company operations in the Nation. This did allow for a restoration of services over a period of months. The rest of the Nation does not enjoy access to such a multitude of readily available services.

Moreover, the Nation likely cannot afford to suffer a breakdown in communications from critical government or commercial sectors. Hospitals, research facilities such as the Centers for Disease Control in Atlanta, the National Science Foundation, NIST, Emergency services (police, fire, paramedics), securities exchanges, brokerages, courts, prisons, central banks, financial institutions, and many other organizations in theory must never go down.

The Federal Government, primarily under the management of FEMA, maintains warehouses in the event of a natural disaster (floods, hurricanes, et cetera). These supplies include basic handheld voice communications systems. Additionally, certain spectrum bands are available for their use.

The Federal Government should expand this model to assist in protecting urban environments and the Internet. For example, certain broadbands, spectrum bands and equipment should, in agreement with private sector partners, be made available.

The equipment could be kept in strategically located warehouses and accessed in the event of an incident. Consultation with private industry as to the type of equipment and arrangements needed to restore broadband Internet to key government and commercial centers could result in the development of an inventory of items and services needed.

In conclusion, without the swift institution of these recommended measures, we remain as unprepared as we were when the third party experts opined in *The New York Times* and *Wall Street Journal.* Leadership and decisive action such as yours will be more appreciated over time, as people reflect over the critical decisions made at this juncture. NIST holds a seat on the Presidential Critical Infrastructure Board established by Executive Order on October 16 of this year.

This Subcommittee's jurisdiction over the Internet, NIST, and other scientific institutions and standards-setting bodies sits at the center of decisionmaking.

Thank you for allowing me to testify before such a relevant institution during such an important phase in our development. Thank you.

[The prepared statement of Mr. Graham, submitted by Mr. Sandri follows:]

PREPARED STATEMENT OF TIMOTHY R. GRAHAM, EXECUTIVE VICE PRESIDENT AND GENERAL COUNSEL, WINSTAR COMMUNICATIONS, INC.

I. OPENING AND INTRODUCTION.

Good afternoon Chairman Wyden (D–OR) and members of the subcommittee. I appreciate the opportunity to appear today to discuss NetGuard and accordingly recommended methods for providing emergency restoration and network security to the national communications and technology infrastructure. My name is Timothy Graham, and I am the Executive Vice President and General Counsel of Winstar Communications, Inc. I am also here on behalf of the Association for Alternative Telecommunications Services (ALTS)). Today I will discuss my company's participation in network restoration efforts after the recent tragic events, provide data on what worked, and suggest improvements needed to capitalize on hard lessons learned.

II. BACKGROUND.

Winstar is a fixed-wireless broadband services company providing high-speed Internet and competitive local exchange services. Winstar, in terms of geographic coverage and total Megahertz, is the largest holder of commercial spectrum in the United States, with ubiquitous spectrum holdings covering every road and building in every State in the country. Winstar is also the largest winner of Metropolitan Area Acquisition (MAA) program contracts from the Federal Government, winning contracts in 14 of the 23 areas that have been awarded. Winstar is the only MAA contractor offering services to MAA customers primarily using a fixed wireless broadband technology for last mile connectivity.

III. EMERGENCY RESTORATION EFFORTS.

In response to the horrible events of September 11 Winstar created voice and data network access in New York City, Northern Virginia., and Pennsylvania. Winstar responded to calls from the city of New York to provide access to three emergency relief centers in lower Manhattan (Centre Street, Gold Street, and Worth Street), provided service to the Federal Emergency Management Agency (FEMA), and installed local service to numerous businesses and government bodies including the Department of Justice (U.S. Marshals), Federal Courts,[1] the Department of Corrections, Citigroup, and other facilities in lower Manhattan. Winstar also met requests for help from Sprint, MCI and other carriers to provide network assistance. In several buildings throughout lower Manhattan, Winstar was the only service remaining. Typical is the situation at 111 John Street, where Winstar provided services to a number of businesses, including The Rubin Group, Nixon Gallagher Company Insurance, Marstech Consulting, York Claims Service, AFG Partners, and All Risk Brokerage. In the Washington, DC area Winstar installed communications services for Cingular, providing emergency restoration of backhaul services for the cellular network in the vicinity of the Pentagon. In Philadelphia, Winstar assisted the American Red Cross by doubling its phone line capacity in just a few hours, enabling it to handle over 500 calls an hour from those wanting to donate blood or provide other aid. Winstar is also using its WirelessFiber technology to support many users and other major interexchange carriers.

[1] *The Wall Street Journal*, A10 (November 30, 2001). "It has been a trying few months for many businesses and organizations located near the Trade Center. The 700 employees of the U.S. District Court for the Southern District of New York still lack basic landline phone services, despite many visits from Verizon technicians, according to court executive Clifford Kirsh. The court continues to rely on a service from Winstar Communications, Inc., which sends calls and computer data via fixed wireless connections."

Numerous media reports chronicled the emergency restoration efforts of a variety of communications companies.[2] In many cases the only available restoration technology involved facilities-based fixed wireless systems.

IV. LESSONS LEARNED.

Hard lessons were learned by major users of information technology. In a definitive New York Times article, the conclusion of third party experts about the physical structure of our Internet and communications networks bears direct quotation:

"As planned, the telecommunications system also relied heavily on built-in redundancies. Many companies, for example, have more than one line from their offices to high-speed access points. But the disaster did expose some of the limits of those contingency plans. Some of those multiple lines travel the same conduits to the same routing centers. If something happens to those conduits or routing centers—as did in many cases on Tuesday—all the redundancy in the world doesn't help: all the cables would be damaged."

"Roy A. Maxion, director of the dependable-systems laboratory at Carnegie Mellon University in Pittsburgh, has long preached the value of physical diversity in networks. 'I wouldn't want to be alarmist about this,' he said, 'but what I think is interesting is how the system is not set up. A lot of these contingency plans are not in place.' He added that 'as a Nation we are dangerously vulnerable.'"[3]

On October 6, 2001 another *New York Times* article about the disrupted operations of the Bank of New York went even further in discussing the danger of improperly designed redundancies from the perspective of the consumer:

"Everyone had redundant telecommunications facilities, but a lot of them turned out to be routed through the same phone company offices," said Thomas F. Costa, chief operating officer of the Government Securities Clearing Corporation. "We've all learned that when we have backup lines, we should know a lot more about where they run."[4]

And on October 19, 2001, the Wall Street Journal ran a front-page article detailing the dangerous concentration of communications traffic in the offices of the incumbent local exchange carrier (ILEC). The article notes that often nearly all local and long distance traffic (not to mention the fact that the bulk of all Internet traffic) often routes through a single ILEC office in even our major cities.[5]

On November 9, 2001, Harvey Pitt, Chairman of the U.S. Securities and Exchange Commission, delivered a speech stating that "critical functions need backup capabilities with fail-over functionality allowing rapid recovery." In particular he said:

"[W]herever possible, business continuity planning should seek to avoid reliance on single points of failure in critical systems. Single points of failure can occur in ways that are unforseen, and even odd. The lines of competing telecom providers may all lie side by side in old, obscure conduits."[6]

Major third party studies also confirm the need for diversity, the fact that the Nation is not fully prepared, and that a false sense of security abounds where people have installed redundant systems, but those systems are not properly configured to be truly redundant.[7]

---

[2] *Internet, Telecom Networks Put to Test in Wake of Terrorist Strikes on U.S.,* Network World Staff, (Sept. 17, 2001.): *See also*, Berman, *Disaster Gives New Life to Wireless Telecom Firms*, *The Wall Street Journal,* B1. (Oct. 3, 2001): *Companies Assist Restoration Efforts, Wireless Week* (Sept. 24, 2001): and *Broadband Carriers Aid to Get Networks Working, RCR Wireless News*, (Sept. 24, 2001).

[3] *See* Guernsey, "An Unimaginable Emergency Put Communications to the Test," *The New York Times*, at *http: // www.nytimes.com/2001/09/20/technology/circuits/20INFR.html* (Sept. 20, 2001).

[4] Hansell, "Disruptions Put Bank of New York to the Test," *The New York Times,* at *http: / www.nytimes.com/2001/10/06/business/06BONY.html.* (Oct. 6, 2001)

[5] Young and Berman, "Exposed Wires: Trade Center Attack Shows Vulnerability of Telecom Network. Damage to Verizon Facility Snarled City's Phones; A Legacy of Monopoly?," *The Wall Street Journal*, A1. (Oct. 19, 2001).

[6] Chairman Harvey L. Pitt, U.S. Securities and Exchange Commission, Remarks at the Securities Industry Association Annual Meeting (Nov. 9, 2001). *www.sec.gov/news/speech/spch521.htm*

[7] Cyber Attacks During the War on Terrorism: A Predictive Analysis, *Institute for Technical Security Studies at Dartmouth College*, by Michael Vatis, Director, (Sept. 22, 2001) (at p.16 Mr. Vatis notes the routing vulnerabilities: "Routers are the 'air traffic controllers' of the Internet, ensuring that information, in the form of packets, gets from source to destination. Routing operations have not yet seen deliberate disruption from malicious activity, but the lack of diversity in router operating systems leaves open the possibility for a massive routing attack." *See also*, Nation Under Attack: U.S. IT Infrastructure Responds in Midst of Calamity, *Testimony to U.S. House of Representatives, Committee on Government Reform, by Harris Miller, President, ITAA*

What are the solutions?

V. ALL KEY COMMERCIAL AND GOVERNMENT BUILDINGS NEED TO BE SERVED BY AT LEAST TWO SEPARATE FACILITIES-BASED NETWORKS, THAT ENTER AND EXIT THE BUILDING FROM POINTS SEPARATED BY MULTIPLE LEVELS IN MULTI-STORY BUILDINGS, AND BY AT LEAST 100 FEET IN SINGLE STORY BUILDINGS.

The examples of emergency restoration efforts, and the observations of third party experts in media reports and white papers, confirm the pressing need for *physically diverse facilities-based networks as a means of ensuring network security in emergency situations and preserving the national communications infrastructure.* Those networks must enter and exit the building at points as far apart as possible.

VI. THE PUBLIC NEEDS TO BE EDUCATED.

Congress, the executive branch and expert agencies, such as National Institute of Standards (NIST), need to issue bulletins advising the public of the:

1. Need for redundancy; 2. Dangers of improper reliance on systems that may be redundant in some fashion, but do *not* have physically separate facilities-based networks which ingress and egress the building at points separated to the maximum extent feasible (such as by levels in a multi-floor building or 100 feet, etc.); and 3. Requirement that these basic issues be addressed on a priority basis.

As you are likely aware, lower Manhattan is home to the greatest number of communications company operations in the nation. This allowed for the restoration of services over a period of months. The rest of the Nation does not enjoy access to such a multitude of readily available services. Moreover, the Nation likely cannot afford to suffer a breakdown in communications from critical government or commercial sectors. Hospitals, Research facilities such as National Science Foundation (NSF), NIST and the Center for Disease Control in Atlanta, Emergency services (police, fire, paramedics), Securities exchanges, Brokerages, Courts, Prisons, Central Banks, Financial institutions, and many other organizations must never go down.

Of course, more detailed studies will be, and should be, made. Those studies will address many more details about the national communications infrastructure. However, it would be irresponsible if the basic and obvious solutions identified herein were not immediately adopted.

VII. EXPAND THE FEMA WAREHOUSE MODEL TO URBAN AND TECHNOLOGY SECTORS.

The Federal Government, primarily under the management of FEMA, maintains warehouses in the event of natural disasters. Primarily, the purpose of that program is to provide tools for fighting forest fires, flood and hurricane recovery, and other efforts. The supplies, which consist of tents, shovels, etc., also include communications systems. Those communications systems are typically walkie-talkie and other hand-held systems. Additionally, certain spectrum bands are set aside for use by Federal emergency personnel to use these hand-held wireless devices.

The Federal Government should expand this model to assist in protecting urban environments and the Internet. For example, certain broadband spectrum bands and equipment should, in agreement with private sector partners, be set aside by the Federal Government. The equipment could be kept in strategically located warehouses and accessed in the event of an incident. Consultation with private industry as to the type of equipment, and arrangements needed to restore broadband Internet to key government and commercial centers could result in the development of an inventory of items and services needed.

VIII. CONCLUSION.

Maintaining secure and reliable communications are vital to the safety and well being of this country and its populace. Leadership and decisive action such as yours is needed and will be more appreciated over time as people reflect over the critical decisions made at this juncture.

Without the swift institution of these recommended measures, we remain as unprepared as we were when the third party expert opinions were published in the *New York Times.*

(Sept. 26, 2001). "One issue that needs further but quick examination is the need to create more redundancy in our telecommunications infrastructure, particularly diversity of egress and ingress in buildings with major telecommunications facilities. Having backup telecommunications systems that are located in the same part of a building and that go in and out of the building through the same pipes may create a false sense of security. This issue is especially important when essential government telecommunications systems are involved."

Thank you for allowing me to testify before such a relevant institution during such an important phase in the development of this nation. NIST holds a seat on the Presidential Critical Infrastructure Board, established by Executive Order Oct. 16, 2001. I clearly recognize that this subcommittee, with direct jurisdiction over the Internet, and a broad variety of U.S. Government scientific institutions and standard-setting bodies, including NIST, sits at the center of decisionmaking. It is an honor to have had the opportunity to provide this information to the official record for your consideration.

Subject: Needed Telecommunications Emergency Restoration and Network Survivability Measures.

Goal: Establish Physically Diverse Facilities-Based Telecommunications Egress and Ingress Points in Government and Commercial Buildings.

(1) Guernsey, "An Unimaginable Emergency Put Communications to the Test," *The New York Times*, at *http: // www.nytimes.com/2001/09/20/technology/circuits/20INFR.html* (Sept. 20, 2001)

(2) Hansell, "Disruptions Put Bank of New York to the Test," *The New York Times,* at *http: // www.nytimes.com/2001/10/06/business/06BONY.html.* (Oct. 6, 2001)

(3) Young and Berman, "Trade Center Attack Shows Vulnerability of Telecom Network," *The Wall Street Journal*, A1. (Oct. 19, 2001)

(4) Chairman Harvey L. Pitt, U.S. Securities and Exchange Commission, Remarks at the Securities Industry Association Annual Meeting (Nov. 9, 2001). *www.sec.gov/news/speech/spch521.htm*

(5) Cyber Attacks During the War on Terrorism: A Predictive Analysis, *Institute for Technical Security Studies at Dartmouth College*, by Michael Vatis, Director, (Sept. 22, 2001).

(6) Nation Under Attack: U.S. IT Infrastructure Responds in Midst of Calamity, Testimony to U.S. House of Representatives, Committee on Government Reform, by Harris Miller, President, ITAA (Sept. 26, 2001).

(7) Emergency Restoration and Network Survivability Services to Lower Manhattan, the Pentagon and other sites.

- Berman, *Verizon Says It Has Now Restored Most Circuits Affected by Attacks, The Wall Street Journal*, A10. (Nov. 30, 2001).
- Berman, *Disaster Gives New Life to Wireless Telecom Firms, The Wall Street Journal,* B1. (Oct. 3, 2001).
- *Companies Assist Restoration Efforts, Wireless Week* (Sept. 24, 2001).
- *Internet, Telecom Networks Put to Test in Wake of Terrorist Strikes on U.S., Network World Staff,* (Sept. 17, 2001).
- *Broadband Carriers Aid to Get Networks Working, RCR Wireless News,* (Sept. 24, 2001).

Senator WYDEN. Thank you, Mr. Sandri.

Ms. Roche has to get on a train in a few minutes.

Ms. ROCHE. It is fine. I am OK.

Senator WYDEN. Well, you are not going to get off easy.

[Laughter.]

Senator WYDEN. Let me ask the question that I was going to let you get out the door with, out to the train with, and then we will go from there. Let us, because of everything you went through—and this is, of course, after the fact. If you could have had, say, two technologies in your hand at the time of the attack, what would they have been?; and then let us say, if somebody could, like NETGuard, have supplied you with two technologies immediately after the attack, what would they have been, given all that you went through? Why don't you take a crack at that?

Ms. ROCHE. Well, one of the coworkers I was with had his Blackberry with him, and that was a hugely helpful device, because it really—we were able to have more than just a few words of communications. We could really get in touch with a lot of people and be able to send messages.

And so I think had something like that been more widely deployed—I know that myself and all the people that I saw were hysterical, because there are so many tourists down in that area all the time and they are not familiar with New York, and they do not necessarily always have cell phones or whatever it was.

That also would have been helpful, to have some sort of mechanism that just would not fail, that even cell phones in regular circumstances are often in a dead zone. In this case, we were completely inoperable for weeks, and so I think having some sort of device like that widespread that people had access to would have been really helpful.

Senator WYDEN. That would be your choice ahead of time, right?

Ms. ROCHE. Right.

Senator WYDEN. What would be helpful to you based upon what you went through that NETGuard could have provided as quickly as possible after the attack?

Ms. ROCHE. I think one of the big problems was that there was not an organized effort to really communicate. I do not think anyone, when we were in all the bottoms of buildings, or people were coming into our building, there was no one that had the accurate information, and I do not know if it was security guards or police officers, or whoever it was that were kind of there corralling people and trying to create a sense of calm, I do not think any of them had any clear information or had any idea of what to do.

It would have been great if they would have had some way of immediately having access to information that was immediate and that was accurate, so that we all could at least—I mean, there were people that were hysterical and that were by themselves, or that were on the street that were coming into our building, because it was the first door they came to when they were running away from the Towers.

None of us ever, I do not think—unless I had had a text message to let me know what was going on, at least it gave me some calm, but there was never a sense that the people that were kind of looking out for our best interests had any way of letting us know what was going on, or where we should be going next, or what was in any way a safe or somewhat safe way to head, and I think that would have been hugely helpful to have that information to them.

Senator WYDEN. Senator Allen, would you like to ask anything of Ms. Roche right now?

Senator ALLEN. You mentioned the Blackberry, and Blackberries are fine. I would think that a Palm, where you were trying to get information, not just having to rely on messages back and forth, but actually getting information, that the Palms—and no one mentions that, and I do not know why, but it seems to me they have greater capabilities in that regard to get information.

I know here, watching CNN in our office, and watching one of the Towers collapse, the first one that collapsed, we were watching it on TV. Now, obviously, I suppose you could get streaming and so forth on it, but to me, any of those capabilities would be good, and I would not want to exclude Palm, because it seems to have much more capabilities to it. I think that Senator Wyden's views were the same.

Having lived through it, you said the one thing is obviously, communicating and getting information, and that is the key to it. I will only ask you a somewhat personal question, and I cannot believe you have this with your fiance—is the Arlington Hospital, is it Arlington here?

Ms. ROCHE. It is Arlington here, unbelievable.

Senator ALLEN. That was the other jurisdiction.

Senator WYDEN. We are looking at partisan pride.

Senator ALLEN. The sad thing is, New York City and Arlington, Virginia are the two places that were hit.

Ms. ROCHE. It was a terrible coincidence that our parents bemoaned for weeks, but I do think that something like the Palm—I see your point—especially if I was not familiar with the area and was trying to get some sort of map or something like that, to at least know which direction to head if there was not someone to tell me.

Senator ALLEN. Plus information of what is going on.

Ms. ROCHE. But I think in those moments there were not people trying to like, surf around and figure out—I just do not think you are sitting there in an emergency situation looking around at your Palm, looking at CNN or whatever. You want someone to be telling you that.

Senator ALLEN. You cannot see CNN on it.

Ms. ROCHE. But at least get some sort of information from it, and I think it would probably serve some of the same purposes that a Blackberry would. I just know that the Blackberry just tends to always be efficient, and you are always able to get across, and the Palms are not—they do not seem to be as always able to get the information that you need.

Maybe they are and I just do not have as much experience with them, but I think anything like that, that would have allowed you to be in touch, but the thing with that is, you also have to know that someone that you are communicating with, that they have a way to respond to you, too, so it is great if I have one, but it is only as great as—I do not think my mom would have had one.

Senator ALLEN. Well, thank you very much. Do you have a wedding date set?

Ms. ROCHE. May 18.

Senator ALLEN. Good luck. Best wishes to you. You are from New York City, but you are very easy to understand.

[Laughter.]

Ms. ROCHE. I went to school in Virginia, and I am from the Midwest, so that kind of balances me out.

[Laughter.]

Senator WYDEN. I am not going there.

[Laughter.]

Senator WYDEN. Ms. Roche, let us do this. We will liberate you now, if you would like to go, and recognize that if you stay you are liable to get some more questions.

Ms. ROCHE. I am happy to stay.

Senator WYDEN. Terrific. We are happy to have you. Let us go, then, to you, Mr. Pelgrin, to give us sort of an overall assessment of some of the issues that are important to New York. In your view,

what types of technology assistance was most important for New York that you had trouble getting quickly?

Mr. PELGRIN. Actually, the amount of assistance that came out right after September 11 was phenomenal.

Senator WYDEN. We are all stipulating to that. We all agree that it was extraordinary, but obviously, given what Ms. Roche and Ms. Coppernoll, and I am sure your own people have found, clearly there were, in spite of these extraordinary efforts, some gaps out there. I think what I am interested in knowing is what types of technology assistance was most important to New York that you needed and was hard to get your hands on as quickly as it would have been?

Mr. PELGRIN. In certain cases, the ability to communicate with the people that you needed to speak to very quickly. For example, with the 2,250 circuits that were down, that was very difficult for us to be able to. While Verizon did everything in its power to get those circuits up, for us to get to the people that we needed to get to, to use that contact list that you referred to, and to be able to have somebody who is standing by—both on a private sector basis, and on a State basis—we needed to contact State and local agencies, along with others, and communication was difficult during that process. Getting good information, also getting it accurately and immediately is something that is critical in emergency management situations.

The ability to have devices like Palms, like Blackberries that you could get and read very quickly is critical, but from a gap perspective, Senator, it was really the case that all the vendors came forward immediately and offered their assistance, both directly to me, but also through an 800 number to which they could donate.

There were computers that were just gone, offices—I mean, this was an incident that—with Y2K, we looked at an infrastructure, a technology infrastructure potentially failing, but what occurred in this situation, we had human infrastructure, a physical infrastructure as well as a technology infrastructure impacted. We were in the process of relocating State agencies, and we were dealing with and consoling victims' families, so in that perspective we dealt with it on a day-to-day basis. I spent 2 weeks in our State emergency management bunker and did not see the light of day for almost 2 weeks, and I know that the assistance, when we needed it—people were there.

Senator WYDEN. Do you think that a pre-existing database of available private sector resources would have been helpful to you in the aftermath of 9/11?

Mr. PELGRIN. Absolutely, and in fact, back in Y2K we started to develop that capability. However, as human nature goes, a lot of that was not kept up-to-date.

One of the charges the Governor has given me is to bring together, at least on a State level, those agencies that have critical infrastructure, and to make sure that that critical infrastructure, both from a contact perspective, and a location perspective, is identified and maintained.

Senator WYDEN. It seems to me that that is relatively low-hanging fruit. I mean, there are some of these issues that are going to be difficult. Certainly, the question of assuring enough spectrum,

for example—I mean, this is a difficult issue, and the fact of the matter is, this country is close to running out of oceanfront property.

We have a system, frankly, and I and others have spoken and focused on spectrum reform that needs some dramatic kinds of changes. The current system discourages innovation, but that is going to be a difficult issue, and there are strong views on both sides, but there is no reason, for example, that all across the country in communities that are so concerned about this issue, that we cannot have these pre-existing databases that in effect make clear what the resources are, where you go to turn to, to track volunteers and their expertise.

We could have lists of doctors that are familiar with health kinds of concerns, technology professionals who are knowledgeable in computer viruses. It ought to be possible to turn quickly to this talent bank, and I appreciate you making it clear for the record that would have been helpful to you all in New York City.

A question for the private companies, for Ms. Coppernoll and Accenture and other people who helped so much on the private side. To whom did you all provide the most help to in the aftermath of 9/11? Was it mostly to the local government? Was it to the Federal Government, non-governmental relief agencies? Who needed the most help, and why don't we start with you, Ms. Coppernoll, and we will just go down the row with private companies.

Ms. COPPERNOLL. It is difficult to say who needed the most help, because I did not, obviously, see everybody, but we spread the offer widely. Dr. Grove made some phone calls to Governor Pataki. We got in contact with the Mayor's office, and we also got in contact with a lot of the military groups as well as a couple of directors at FEMA. All of the organizations said "yes, individually we need assistance. We are just not 100 percent sure what we need."

We had to go there physically and see what we thought we could do to help them, because it was very difficult for them to scope what exactly it was that they needed, and then once we were there, people would start to come to us and ask us, so there were good examples of FEMA workers that had been deployed that really needed some assistance, and I had a long list of requests from people that were making maps, people that were trying to link into other agencies just to get reports out. They needed assistance, and they probably I would put at the top of my list, just because we spent the most time with them.

Certainly down at Ground Zero, the military and national reserves that were there, they needed a lot of assistance. The things that they were dealing with, as you have heard over and over again today, technology could have definitely helped them. Some of the examples you have already heard. Some of the other ones, you talked about deploying resources. The branch chief down at the OEM office said we had people with highly trained skills that were serving food. We did not know how to find those people and get them to the right place at the right moment.

We would have teams of people that were deployed down to the site, search and rescue teams that we would have to ask to wait for 6 hours because we were moving a piece of equipment and we did not know that that was going on, and we had no way of sharing

information, getting information distributed. They were in serious need of assistance, and those were probably the two that were most visible.

On the business side, once businesses were trying to figure out what to do and where to go, a lot of them did not have access to the Internet. Their computers were gone. They needed a place where they could go. It was not obvious immediately that that was necessarily the most immediate place to distribute information from them, because they had a hard time receiving it on the other side.

Mr. ROHLEDER. I would separate our constituencies into two groups, first of all, and it varies by phase of the work. Immediately when we were helping establish a Family Assistance Center, we worked directly with the city officials, city IT officials, and to a certain extent some of the State officials, to help establish a program management office and put the processes in place to get that center up.

As we transitioned that in and made progress there, we worked more shoulder-to-shoulder with the relief organizations to help connect the different types of relief available and connect back into their legacy systems so that we could essentially provide a virtual relief center, having one-stop-shopping at the Family Assistance Center, so I would say the city government IT people, and then following up the relief organization IT people.

Senator WYDEN. Mr. Sandri.

Mr. SANDRI. Everyone needed help. We brought people up from Virginia, and we were also in Manhattan. So, we decided to prioritize, sort of a snap judgment. We talked to a department in the City of New York called DOIT. Then we provisioned FEMA, the Federal courts, the Department of Corrections, and the three emergency response centers in lower Manhattan. We provided broadband, and we focused on, for example, the U.S. Marshal Service location at 26 Federal. That address is where all the Federal agencies were, and it needed restoration. We identified a few other areas, with some difficulties.

For example, getting our crews in was difficult. There was a surreal moment where I was trying to get crews to help restore FEMA, and I was on the phone with FEMA explaining to them how we were trying to get through below Canal Street and the city police department was manning those barricades, and of course, they were not getting information about who was allowed through with service trucks. You had people needing to get diesel fuel in to get generators moving; people who wanted to get on rooftops to deploy wireless systems while the President was flying in; and of course, nobody wanted to see anybody on the roof with equipment at that time. So there were a lot of coordination issues there that certainly could have benefitted from a database.

Senator WYDEN. Another question for the private companies. Since we are sort of in the hindsight business here this morning, kind of looking back at what else might be done in terms of the private companies, has 9/11 made you all aware of any assets you have that in hindsight you wish you had been able to mobilize, or to mobilize more quickly in support of the relief effort?

Ms. Coppernoll.

Ms. COPPERNOLL. I think yes. I think we definitely in hindsight, everybody stepped back and said yes, we could have used our people, resources more effectively. We could have used our relationship resources more effectively. We could have thought through ideas more quickly and come up with databases more quickly, and solutions. I do not know that there is one thing specifically I think for us. Because we are a West Coast company, we thought of the resources that were at our fingertips. You think of the people that you know that you can deploy yourselves with that can move very quickly.

The type of resources that we deployed with are the type of resources that go around to trade shows and set up demonstrations, because they are extremely flexible, and they can work under very unique environments, and you do not know what you will find when you walk in to do a trade show in Beijing. You just have to deal with it, and do whatever you can.

We had resources in New Jersey and Massachusetts, but we did not necessarily immediately think about deploying those people for quicker solutions.

Senator WYDEN. That is an interesting point. So as you step back, and you came to meetings with me and others on the West Coast, and thought about how it would have been done differently next time, you would say there are some resources that we have elsewhere, in maybe New Jersey or somewhere that would be close, in this case obviously to New York City, and that would be the kind of thing that would change.

Ms. COPPERNOLL. That would be one of them, yes.

Senator WYDEN. Very helpful.

Mr. Rohleder, Mr. Sandri.

Mr. ROHLEDER. A first area would be criminal investigation tools. There are a number of technologies we work with. Frankly, had we had the foresight to be able to get some traction in the government, I think frankly there is a lot of information out there, and there are tools that could have helped identify potential terrorists.

I also think in the knowledge management area there are a number of tools that are available right now to help agencies begin to break down the silos of information that they have and connect them more efficiently. The Department of State, for example, is involved in a prototype that connects 43 different agencies together to share information using commercially available tools.

They started this before 9/11, and we are involved in implementing that in New Delhi, in Mexico, and DC., and I think tools like that that allow collaboration and knowledge management are absolutely essential as we move forward and break down some of those.

Senator WYDEN. Out of curiosity, we are aware, Mr. Rohleder, of some very good work that is being done in the Drug Enforcement Administration along those lines. Are you aware of that?

Mr. ROHLEDER. Yes, we are.

Senator WYDEN. We will follow up on that.

Mr. Sandri, on that point.

Mr. SANDRI. I would echo what Ms. Coppernoll and Mr. Rohleder were saying. In addition, in hindsight, I think we would have focused on some processes, two processes in particular.

One is credentialization. Obviously, the company credentials their employees in a certain way, but we might have thought through how to coordinate those credentials to officials and in the Federal and in the State and municipal governments, because that was one of the key problems in identifying who you were and how you needed to get to a certain point if a service had been ordered from you.

The second piece is N stack and the network reliability and the interoperability councils, which advised the President and the Federal Government about how to handle emergencies, are currently staffed by CEOs and executives from basically almost a pre-1996 Act companies, and in essence there is no competitive carriers, and therefore the notion of our more complex telecommunications Internet environment has not seeped into emergency response efforts in that infrastructure. Therefore, we would have pushed much more vigorously to get members of competitive companies on those groups, and that is I think a pretty poignant hindsight there.

Senator WYDEN. One last question on this round, then I will recognize Senator Allen.

We have been told in some instances some key information technology personnel had trouble gaining prompt access to the critical areas. I am curious whether any of you had folks that experienced that problem, and maybe we will start with Mr. Sandri on that, and could a kind of technology guard be helpful here, because then you would have something, again, to an official credential that local authorities could recognize.

Mr. Sandri, why don't you take a crack at that?

Mr. SANDRI. I would give that a robust endorsement. We had people—I was on the phone on Sunday at 3 a.m., people trying to get barricades, critical services were down. You were hearing from the municipal governments and Federal Government as well as brokerages. The President said he wanted the market back up. The brokerage houses were down and we were trying to get in, and our people were driving in from, like, for example Virginia and New Jersey and elsewhere, coming in on trucks. Trucks were not allowed in southern Manhattan, so they got on any type of transportation they could, carrying equipment, getting to borders, unable to get over the borders.

They were uncredentialed in any respect, even though we did call NCS, the National Coordination Service, which was managed by GSA, which was established after the Cuban Missile Crisis, and it works in conjunction with FEMA, but a lot of the folks there, they had just been—they were Federal Government employees usually from GSA, and they had been sort of staffed at the last minute. Even though we gave them their name and told them what we were doing and wire service had been ordered from us, and why we needed to get to southern Manhattan—they typed us into something, but when our people showed up, often it was at very funny hours. There was no coordination, and therefore what you are suggesting, I think, is very needed.

Senator WYDEN. Mr. Rohleder, others.

Mr. ROHLEDER. We may be in a little bit different space. The people that worked for the Family Assistance Center actually were local individuals that were working with local city officials, so I

think there were some fits and starts, but after that it ran very smoothly.

Senator WYDEN. Others.

Ms. COPPERNOLL. Only one slight humorous comment. Intel in those circles often means "military intelligence," so we had a little bit easier time.

[Laughter.]

Mr. COCHETTI. Senator, if I could add, on just one point that was brought up, and I think there have been enormous efforts since September 11 on the part of the entire Internet industry to work more closely on contingency plans and to strengthen their ability to withstand both cyber and physical attacks, but I do want to note that I think that the Bush Administration and the White House has made what we view as extensive efforts to reach out to the Internet industry to expand in light of the events of September 11 the network of contacts and cooperation, which had historically grown up around the telephone industry understandably throughout the 1960s and 1970s, and even into the 1980s, so we have made what I would view as probably a decade's worth of progress in the space of the last month involving the Internet industry and emergency preparedness.

Ms. COPPERNOLL. I actually do have a serious comment on it, being down at Ground Zero where the credentialing system was going on, and it was a very difficult situation. You had to be down there to get credentialed, but you could not get down there unless you had credentials, so it was somewhat of a catch-22 difficult environment.

But the branch operations management down there was working with the team that does credentialing for the Olympic Committee and trying to figure out a way that they could credential people, and I sat in on some of their meetings where they had some of the local representatives from fire and police trying to figure out a way that they could credential their entire teams, both from the perspective of getting them in, being able to have hand monitors so that they could check and verify who was allowed in. It would change on a day-to-day basis, but it was an overwhelming task for them to try to implement that something after the fact. It was just too difficult.

Senator WYDEN. The key, of course, is to address as many of these issues as you possibly can ahead of time. That is why I asked the question of Mr. Pelgrin about these databases that, should they be pre-existing. Everybody was trying to help. That is not what is at issue. Nobody was sitting around saying "let's be rotten to people from Oregon who want to help." Quite the opposite.

People wanted this kind of assistance, but you have got to make sure that people have the necessary expertise and the right motive so you can get the vast majority of people quickly in, while having a process to make sure that small number of people who do not have good motives are kept out, and that is why we are going to work on this. It seems to me that this is again illustrating how the government, with a very modest sort of role, working with the private sector, could have a credentialing process so that you have these systems available on a pre-existing kind of basis, rather than

try after a tragedy occurs to play catch-up ball to try to put them in place.

I will have a few last questions, but I want to recognize my patient colleague for anything he would like to ask.

Senator ALLEN. Thank you, Mr. Chairman. I want to say how much I thoroughly enjoyed listening to all of your comments and your insight on this, and we were first talking about NETGuard, and that is one thing, but some of the things you have been saying here are very important for us to understand, as well as our colleagues, and Ms. Coppernoll's comments, and we are so grateful to Intel, if you would like to have a presence on the Eastern Seaboard there are some great places in southside and southwest Virginia, and you could join VeriSign in Virginia.

I would like to say to Mr. Pelgrin, you are fully understandable. I completely can understand what you are saying, and if you would relay to Governor Pataki what an outstanding job he has done. His leadership, his steadiness, his calmness, working with Mayor Giuliani, meant a great deal. I was looking through your presentation here, and what a well-organized way you are looking at everything in New York and how you are looking to improve it into the future.

And while you are talking about Wall Street reopening, why that was important to New York City, but boy, that sent an important signal to this country and, indeed, all around the world that Wall Street could operate. We did not like the results those first few days, but nevertheless, it was an understandable reaction.

The other thing I think we can learn from this, Mr. Chairman is in looking at it, it reminds me of what a government of a State such as Virginia or New York or the Federal Government was doing on the Y2K situation. We are analyzing where are the deficiencies, and then with that, once you have that assessment, you work to test whatever remediation, and you fully remediate, and it is that same sort of strategic corporate planning that business would have, but the same as a governmental operation, and in this situation, just when you look at this, you see there is great reliance upon the State, on the local people, and this can be a model.

I know Governor Gilmore in Virginia and other Governors are doing similar things, but this is a model of how I think we ought to have oversight at least for Federal operations from what you all are doing in New York.

I mentioned, Ms. Roche, earlier Mr. Rohleder's comments and Accenture's view on the criminal justice efforts and collaboration. This is one of the things that is most surprising to me on preventing this as far as a matter of criminal situations, and you were in some of those briefings which we cannot really talk too much about, other than to say, people did know about the background of some of these individuals coming into this country.

Now, maybe they have so much information they do not know, what, 5 percent of that information is probative, but there needs to be much better collaboration. I call it a hand-off. They are fumbling the hand-offs. They have the ball and they hand it off, but it is fumbled for whatever reason, and I think the technology is going to be so important for all of our external or international agencies. Whether it is the CIA, defense intelligence, working with

INS, working with FBI as well as with State and local law enforcement is going to be important.

We thank you for your testimony there, and also we are grateful to Accenture and also Winstar for all of your work here.

I wanted to ask some questions of Mr. Cochetti of VeriSign, and that has to do with the A route and the Internet. The A route, and are there any backups? What backups are there to prevent a major breakdown in the Internet if that is attacked, because one of the key concerns that I have—and I am chairing the High Tech Task Force for the Republicans, and I am also in agreement with Senator Wyden, but one thing we are concerned about is cyber security, and more specifically cyber terrorism, and so what are the backups for the A route, and what is its vulnerability?

Mr. COCHETTI. Thank you, Senator, and let me, if I may, begin by expressing our thanks to you, not just for your leadership in high technology issues for the high tech technology and Internet industries in Virginia, but also for your support recently for the extension of the Internet tax moratorium, which we felt was a very important piece of legislation which both of you exercised leadership on.

Your question I think is important, because in most of our discussion today we have been talking about what most planners would think of as the transport layer for the Internet, the basic layer of connectivity, and that is quite appropriate, because the September 11 attacks were merely a physical attack, and they primarily eliminated physical infrastructure, without which you cannot have the upper layers, but above the physical layer obviously is the logical layer, and above that are the applications, the web sites and the e-mail and everything that people actually use the Internet for, and we are quite concerned about and sensitive to the issue of security at the mid-layer, because without it you do not do anything with the connectivity.

There is probably no single resource in the Internet that is more important at that middle layer than what you have described as the A route service. This is the facility that has been managed by VeriSign, and before it, Network Solutions, under contract to the Commerce Department in the U.S. Government that provides the central directory for the Internet.

The facility is protected in a variety of ways from both physical and logical threats, not all of which it would be appropriate for me to discuss at a hearing of this sort, but all of which we would be more than happy to brief both of you on.

Sufficient to say, we take the reliability of that facility very seriously, are reasonably confident that it would take an enormous effort for it to come under any serious threat, and use all of the conventional techniques that most people would think of, including redundancy and diversity and random reallocation and things of that sort, as well as unconventional techniques that probably would not be appropriate to talk about, and so I think as a Virginian you can be proud that the home of the Internet is in Virginia. One of the most important facilities of the Internet is in Virginia, but I think you can also be confident as a Senator that the facility is well-regarded.

I would, if I may, like to introduce into the record of the hearing a statement that was issued by the Commerce Department on November 13. A high-level delegation from the Commerce Department led by Deputy Secretary Bodmin came out to our facilities on November 13 to take a look at them, and they were joined by officials from the White House. Following their visit, they issued a statement indicating their sense of confidence and gratitude for VeriSign for the work that we had done, and so I think without going into the details of exactly what we do, I can say that the Executive Branch, on looking at it, has given us their commendation and support.

Senator ALLEN. Well, that is comforting to hear. Let me ask you this question. Without divulging how you provide for the security of the A route or the J route, for that matter, as well, we had a meeting on cyber terrorism, and it was amazing how many more viruses, and who knows if it is coincidental, just taking the Department of Energy, and how many viral attacks, Internet viral attacks there were, and it just shot up after September 11, and who knows if it was pranksters or not.

Can you say, or would you feel comfortable in answering this question: have the number of attacks on your servers increased or decreased after September 11, and does the current State of affairs, in your view——

Mr. COCHETTI. If I may answer your question——

Senator ALLEN. Maybe if you feel that somehow in answering this question in any way in your mind would be harmful to the security or the psychology of our country, just say "I decline to answer."

Mr. COCHETTI. I am happy to answer the question, but I may not give you the precision that you or others might have in mind, to simply say that operating facilities of the sort that we do, we are accustomed to online threats, some of which are unintentional, some of which are intentional and have developed a variety of systems that are designed to both avoid, prevent, and respond to those threats whenever they occur.

They have been a continuing fact of life for Network Solutions and VeriSign both before September 11 and after. There have been few, if any occasions that these have been successful in disrupting our service for the Internet, so we are comfortable that we understand most of the known threats, and we have taken every precaution to deal with them, but beyond that, I think it is probably something we would rather discuss with either the Senators or the Members of the Committee outside of the hearing.

Senator ALLEN. You would prefer not to say whether they have increased since 9/11?

Mr. COCHETTI. Let me ask one of my colleagues here. We have not experienced an increase since 9/11, no.

Senator ALLEN. That is good. That is good to know.

One other, and you had so many ideas or comments in your testimony. One of them, you stated that the six sigma, the 99.9999, the six sigma is, as far as your standard of reliability, it is an insufficient standard of liability, or performance. Now, how many sigmas are needed? I mean, you talk about 40.

Mr. COCHETTI. Misfires.

Senator ALLEN. 40 bad Internet connections daily. Now, to get it to say, seven sigmas, or eight sigmas—and I could understand for an Amazon.com this is awful, or AOL and so forth, but what is the cost of the added sigmas?

Mr. COCHETTI. Well, it adds considerable cost. We have not sought to quantify it, but there is no question but that seeking the level of liability we have has imposed a significant financial burden on VeriSign simply because what you must do is scrub everything for accuracy and provide multiple levels of redundancy and reliability, as well as the protections against outside intentional or unintentional threats that occur.

So that what we have is a series of filtering techniques, devices, and facilities that try progressively to ensure that what gets through to the .com, .net, and .org databases, or to the route levels are at the highest accuracy level possible, adding and maintaining those filters, and doing so in a way that each of them would survive problems to them is what creates a cost structure, so it would be the equivalent of building walls around walls around walls, a fort, and then having redundant walls to the walls, in case any of the individual walls went down. Then obviously, each time you add a wall you create a new cost structure, twice or more if you provide redundancy for it.

Senator ALLEN. Let me ask you one final question, then I would like to ask a question of Mr. Sandri, if I may, Mr. Chairman.

One of the recommendations you suggested is enactment of legislation that would reduce some of the risk incurred by companies if they share network information with Federal agencies that are concerned about security. Can you elaborate on the type of risk you are referring to here?

Mr. COCHETTI. Well, there has been legislation considered in this Congress and even in previous Congresses that would provide some type of protection for companies when they share network or operational data with Federal agencies that is relevant to Internet security. Obviously, Federal agencies are subject to the Freedom of Information Act, and the sharing of information between companies can raise antitrust issues.

At times, because of these two existing legal issues, there has been some reluctance on the part of industries or companies and operators to share information. We think that this is the type of information-sharing which could well be subject to a safe harbor. Obviously, one should not lightly consider modifying either of those existing legal structures, but in order to benefit the specific interest of Internet security, and the need for more information sharing, we need to address those two areas, and I think most government agencies involved in this would probably say much the same thing.

Senator ALLEN. We will need some tweaking of the Freedom of Information Act.

Thank you, Mr. Cochetti.

Mr. Sandri, you mentioned in your statement or that of Mr. Gramm, the Winstar statement, that many companies did not have redundancies they previously believed they had due to the routing of communications through a single local exchange carrier, and granted, it has not even been 3 months since this horrific attack, but have you seen any change in the private sector's approach to

ensuring redundancy in the design of their communication systems?

Mr. SANDRI. There was an article last Friday in *The Wall Street Journal* that talked about Verizon, which is the predominant carrier on the East Coast, and they spoke at length about trying to build redundancy, and so I am seeing them discussing it and putting facilities in place there.

Also, the Federal Government as a user has something called the GovNet proposal. I am not sure the extent to which you focused on that, but an RFI is out, and comments were submitted on November 21 at 4 p.m. by a lot of industries.

The one concern there that we noted in our comments was whether a dominant pro-fiber discrimination existed in those comments, or in the RFI itself. I asked the question of Richard Clark. Was I to presume that the government would connect all of its agencies nationwide that were identified as "key" with fiber, and is fiber the gold standard? The issue is timing, because: (1) They are trying to get this done in initial phase in 6 months; and (2) True redundancy. You cannot get new fiber routes into all the Federal buildings in all our Nation's big cities as a matter of infrastructure.

The conduits and rights-of-way only come in at a certain point in a building. Then you have to go to the City of Chicago and say, "we are going to rip up your conduit map and change your gas lines, your electric lines, everything else, and come in in some other way." It is not going to happen, by any stretch, to have true fiber route redundancy there to come in and out, and therefore the considered opinion was to look at alternative technologies that could deliver redundancy.

In a hard sense, the events of September 11 proved that out. Nobody wanted to see that test made, but the test has been made, and we see what can deliver when the infrastructure is ripped up, and that is predominantly a wireless system.

Senator ALLEN. Thank you. Thank you all so very much.

Ladies and gentlemen, your insights, truly, and information and your comments are truly beneficial, I know to these two Senators here, and we will certainly share it with others, and thank you again for your time and also your bravery as well in some cases. Thank you.

Thank you, Mr. Chairman.

Senator WYDEN. I thank my colleague.

Just a few last questions, and we will wrap up. One question that any of you could be helpful on is, New York obviously has one of the largest forces of police and fire personnel in the country. It is a major hub for technology and communications, so there was lots of expertise right there.

I mean, arguably New York City, it is perhaps the best positioned in the world to deal with this kind of tragedy. My question is, how would the technology-related challenges be different if an event occurred somewhere else?

Ms. COPPERNOLL. It would depend upon the city and the location. For Intel, for example, we had thousands of employees that were all over the country, and mostly on the West Coast, that were willing to go anywhere. I had phone calls from people saying, "I will

give up my sabbatical, I will give up my vacation, I will quit my job, I will take a leave of absence, I will go wherever I need to go." So in that example, if it had happened anywhere across the U.S., we would have been able to mobilize a community of people.

We had a lot of people from New York City that were within the tech community volunteering their time, but they did not necessarily come with equipment or projects necessarily, that they necessarily could immediately deploy, so I think in the example of another city, we would have been able to accomplish what we had accomplished, as long as we could get to it.

Senator WYDEN. A lot of cities rely upon a single communications hub, where all the phone traffic is funneled into a concentrated area, so if a big attack occurs, it seems to me that the city loses its communications entirely, so one of the reasons for my question is, as we think about mobilizing this cadre of volunteers, that is the kind of thing that my sense is we need to consider for the many communities that do not have as many resources as New York City.

Mr. Rohleder.

Mr. ROHLEDER. Senator, just real quickly, I also think that preparedness plays a role, and geography obviously is one impact, but the different level of preparedness will certainly dictate how any community is going to react to this, and having talked to the National Association of Counties, who are the first line of defense, if you will, there are some counties that are very well-prepared that have documented plans, that have telecommunications structures in place to allow them to communicate. There are others that do not even know where to start, and I think the Federal Government, they are looking to the Federal Government to help facilitate some of that preparedness planning.

Ms. COPPERNOLL. The satellite that we brought for our communications came from Wisconsin, so it did not come from within New York City.

Senator WYDEN. Any others want to comment on that?

Mr. SANDRI. Just briefly. The record shows that in, for example, Cleveland, (I do not know about Portland, exactly), if all of the city's telecom is routing through the former incumbent monopolist's area, then in a catastrophic event you are going to see everything going down, Internet-wise almost everything going down, unless you have a separate satellite system in place, or a separate facilities-based system in place.

But to reach out to all of the buildings that were affected, or that would be affected, I do not know how long it would take, but it would probably take a solid year if you really wanted to restore everything, because as you rightly noted in New York there is the highest concentration in the country of competitive carriers, and I think you were talking about the layers. If you lose that basic layer, everything else cannot build off of it, so from that respect, it is pretty daunting.

Ms. ROCHE. If I could quickly comment, too, one thing I did not comment on before when you asked me what would have worked, one thing that worked for us was SMS, which was the text messaging I was referring to, although it does not cover all of the communication needs that are necessary in a disaster situation, I know

that it was hugely helpful in being able to communicate, and it was not impacted at all. I would think no matter where an event like this could have happened across the country, that deploying SMS to communicate I think would be extremely helpful and wise for NETGuard.

Senator WYDEN. One last question for you, Mr. Pelgrin.

Mr. Allbaugh told the Subcommittee that FEMA faces some legal constraints that could prevent it from accepting help from the private sector. Did anybody in New York State or local officials face those kinds of constraints, or was it even considered? I hate to create legal questions after the fact, but I wonder if you had any experience on that?

Mr. PELGRIN. Yes, actually, we did. Right after the event we looked at whether or not the generosity of the vendor community could be accepted by the State. We dealt with our ethics commission immediately and requested an opinion from them relative to that issue. They responded that even though an individual donor is a vendor, they would not automatically be a "disqualified source"; as long as there was not litigation or an investigation involving that vendor, that those services could, in fact, be accepted.

Senator WYDEN. This was under the city?

Mr. PELGRIN. The State.

Senator WYDEN. This was under the State rules?

Mr. PELGRIN. The State Ethics Law.

Senator WYDEN. Did you have any questions with respect to your involvement, say, with the Federal partners?

Mr. PELGRIN. That never came up.

Senator WYDEN. One last question for you, Mr. Rohleder.

We are trying to get some lessons in terms of assisting victims as well, and your Family Center sounds like a very exciting kind of program. I assume at some point this is going to close down.

Mr. ROHLEDER. Yes. My understanding is probably within the next 2 weeks, unfortunately, I think. The city has identified a need to close down the center, and what we have been working with is to try to keep the virtual nature of that center in place, to allow people to have web access to those services, and we are working with the city right now to transition from a physical facility to a virtual facility and allow them to move forward on that basis.

Senator WYDEN. Please keep us apprised of that, because that is exactly the kind of model that I am interested in pursuing. I mean, at some point you are going to see programs or companies that have stepped in needing to close, and the question is, what are you going to do to make sure that those families are not left in the lurch?

I mean, it is fine to talk about all of these whiz-bang technologies, and it is quite another to have those human faces that have been receiving assistance suddenly lost and confused, so I think that is a good model, and we would like you to keep us apprised.

We have been at it well over 3 hours, and you all have been exceptionally patient, but I think it is really appropriate to have you all wrap up, because you have been on the front lines seeing it both from a governmental standpoint, from the standpoint of people try-

ing to help, and have given us some very good suggestions and ideas.

What I want to do is just really be part of an effort to mobilize this army of talent that is out there. We are talking about literally millions of people with expertise in science and technology that could make a difference, and you can debate the details about a NETGuard or cyber security patrol, or however you want to call it, but to me what is not in dispute is that this country will benefit significantly from the ingenuity and talent of people like yourselves and many others who work in the technology sector.

So we thank you for your patience. We are going to follow up on these issues quickly, and as I mentioned, work in concert with the Administration. Is there anything any of you would like to add further?

Mr. COCHETTI. Just briefly, Mr. Chairman, I would hope that as I indicated in my testimony, in addition to looking what can be done after a catastrophe occurs, it is important for the Subcommittee to look at the various things that could be done to prevent and avoid such problems from occurring, and the four suggestions I offered in my testimony were simply examples.

But I would, as you think about the Subcommittee's hearings and investigative work, allocate a good amount of time to sort of the preventive side, a technology, or NETGuard might be something which is used to educate web site operators, or used to educate network operators on what kind of preventive or cautionary activities they might be undertaking, as well as helping after disaster strikes.

So prevention is an important part of the solution.

Senator WYDEN. Well, I appreciate your making that point, because not only is that going to be an essential focus of what we are trying to do with the technology sector and scientists, but you can keep from having to play catch-up ball when a lot of Americans are hurting.

I mean, there are two routes here. You can say, well, shoot, just try to respond, and we will try to eliminate as much suffering as we can after the fact, or you can use this treasure trove, as I call it, of scientific and technological talent to prevent as much as possible.

I mean, you look at fields like biometrics, and mention was made of what we are going to try to do in the future. Biometrics is a very rapidly changing field, an exciting field that is clearly going to be able to play a key role in terms of prevention. I see, for example, the NETGuard concept of using volunteers along the lines that we are talking about, of constantly funneling in to government and local responders all across the country state-of-the-art information and equipment that they can use in a preventive kind of way.

You have been exceptionally patient. We are going to be calling on you often.

The hearing is adjourned.

[Whereupon, at 1 p.m., the hearing was adjourned.]

A P P E N D I X

PREPARED STATEMENT OF THE AMERICAN RADIO RELAY LEAGUE (THE NATIONAL ASSOCIATION FOR AMATEUR RADIO)

PART I: EXECUTIVE SUMMARY

The American Radio Relay League (ARRL) is a national association representing the technical, regulatory and legislative interests of the approximately 675,000 Amateur Radio operators in the United States. We sincerely thank Chairman Wyden and the subcommittee for giving us the opportunity to offer our views on how the Amateur Radio Services (defined in Title 47 C.F.R. Part 97) provide a successful, robust and rapidly mobilized emergency backup to the nation's telecommunications infrastructure. In some ways the service already performs as a technology national guard, albeit not in the context proposed by Senator Wyden.

The Amateur Radio Service is comprised of volunteers who have earned licenses from the Federal Communications Commission. Radio amateurs have provided successful "wireless links" during many major crises dating back to 1913. Amateurs still "get the word out" after storms, floods and other natural disasters. Most recently they provided communication services to relief agencies after the September 11, 2001 terrorist outrages at the World Trade Center and the Pentagon. More than 100 Amateur Radio volunteers provided emergency communication at the Pentagon for about a week after September 11. Another 500 worked for more than 2 weeks helping out at Red Cross and Salvation Army communications sites around the World Trade Center. It is possible that, even as you read this, there continues to be an area of the U.S. where Amateur Radio volunteers are helping emergency relief authorities cover a temporary gap in communication as they cope with flood, tornado, fire or other catastrophe.

Whenever natural catastrophes or acts of terrorism occur in our country, Amateur Radio is available as a tested and organized nationwide network of trained radio experts. These volunteers provide radio communication under longstanding written agreements with major government and private disaster relief organizations.[1] Under the provisions of these agreements they often step forward to help when telephone services, data networks, radio and television broadcasters, police, fire and ambulance two-way radios, or other vital components of local, State or national telecommunications systems are disrupted.

In fact, even during this stressful time other Amateur operators continue to participate in mock disaster drills, national communication contests and operating events that serve as trial runs for fast and effective radio operation under difficult conditions.

As our nationwide system of telecommunication grows increasingly complex and, many would argue, more vulnerable, the existence of this self-supporting, self-managing and flexible system of communication, independent of the national network, appears to be an increasingly important form of insurance.

In addition to enthusiastic and knowledgeable hobbyists, the Amateur Radio community also consists of experienced emergency communicators (some also professionally affiliated with government emergency response entities). But equally important is an impressive number of successful engineers, military leaders, and academic innovators (including Nobel Prize winners) who might easily be considered a reservoir of expertise on all aspects of wireless communication.

The purpose of this testimony is to inform you of some of the ongoing thinking and planning on in this unique community today.

---

[1] In addition to being an active member of the National Voluntary Organizations Active in Disaster, the American Radio Relay League, as the agent of all amateur operators, currently shares active Memoranda of Understanding (MOUs) with The National Communication System, The Federal Emergency Management Agency, The Association of Public-Safety Communication Officials International, The National Weather Service, The American National Red Cross, The Society of Broadcast Engineers, The National Association of Radio and Telecommunications Engineers, The Salvation Army and Radio Emergency Associated Communication Teams (REACT).

PART II: WHAT IS AMATEUR RADIO?

Amateur Radio's contribution to the public good has long been explicitly recognized by Congress through legislation,[2] report language and statements in the *Congressional Record*.[3] Amateur Radio supports emergency communication in times of crisis, acts as a laboratory for Americans in the great tradition of home experimentation to develop vital new technology, and is a spawning ground for each new generation of electronic and communication engineers, who, as youngsters cut their technological teeth tinkering with electronics and radio gear.

In this testimony it is important to note that the word "amateur" is more aligned with the Latin root *amõ* (as "to love") than it is with the contemporary vernacular implying "lack of skill." Indeed, Amateur Radio operators bring a deep love of science and technology to the process of electronic communication. And driven by that love, Amateur Radio operators offer a very high level of emergency communication services supported within an infrastructure of:

(1) *Frequency allocations:* sufficient to allow them to surmount various physical and electromagnetic conditions encountered in emergency communication;

(2) *Organization:* most radio amateurs participate in frequent "on the air" events for enjoyment, but one of the fringe benefits of such events is the creation of formal and informal radio groups that can be mustered in emergencies. In addition, more formal structure exists through groups like Radio Amateur Civil Emergency Services (RACES), which is mobilized by FEMA, and units of the Amateur Radio Emergency Service (ARES) which, while organized by ARRL, are usually self-mobilized at the local level. And finally, *Skywarn,* usually working hand in hand with the National Weather Service to monitor storm activity;

(3) *Expertise:* where technical capability is demonstrated and certified by the FCC licensing system that currently consists of three license "classes" consisting of an "entry-level" license, a mid-level license and a license demonstrating advanced capabilities. These licenses, earned by passing rigorous FCC examinations, require considerable electronics and operating knowledge as well as understanding of Federal rules and regulations. The ARRL, in fact, provides many books, video courses and on-line courses to support not only earning a license, but also to teach special aspects of radio, such as our new on-line "emergency communication" course. And of course, extensive shared experience of the various emergency groups should not be discounted;

(4) *Creativity:* achieved by the experimental and amateur-research driven nature of Amateur Radio, where malfunctioning equipment often can be repaired in the field because of the radio amateur's knowledge of circuitry, and makeshift antennas can be erected on scenes of terrible devastation where a standard antenna might not even function;

(5) *National "Party Line":* while Amateur Radio is, by law, a person to person communication service where "broadcasting" is forbidden, radio frequencies in the Service may be monitored by anyone possessing a suitably equipped receiver. This means that amateur networks can extend to all borders of the country and beyond borders in cases of international crises (hurricanes in the islands, for example). Moreover, the "open" nature of amateur frequencies, and the fact that they are constantly monitored, makes them unsuitable for the sort of stealth communication that social misfits such as hackers or even terrorists might otherwise be able to use more successfully than ordinary telephones. But that same "open" quality makes these frequencies particularly useful for coordination at a national level during large-scale disruptions or disasters.

PART III. EXISTING AMATEUR RADIO RESOURCES FOR HOMELAND SECURITY

As chiliastic anxieties faded after the start of the New Millennium, they were replaced in many Americans' minds by the discovery of authentic threats that could disrupt large segments of our society simply by disrupting telecommunications. As the Subcommittee examines the complex technical issues arising from this hearing, we urge you not to lose track of the national resource of simplicity, experience, ubiquity and redundancy offered by Amateur Radio serving at no cost to the government and entirely on a volunteer basis.

As earlier noted, radio amateurs provided emergency communication at the scenes of the New York Trade Center and the Pentagon terrorist outrages. Also, a number of amateurs have been identified as employed in the Internet infrastructure and

---

[2] *See,* for example, PL 103-408, 108 Stat. 4229 (1994), recognizing the contributions of radio amateurs. *See* also PL 100-594, 102 Stat. 3025 (1988).

[3] *See* for example, p. S12365, Friday August 11, 1995, statement by Senator Nickles on Amateur Radio volunteer communication at the site of the Oklahoma City bombing.

willing to participate in restoration should there be a major collapse of the Internet. They have made some notable technical contributions in these matters, want to do more and are looking for guidance on how they can help.

Existing resources of the Amateur Radio Service as coordinated by ARRL fall into three categories: monitoring, communicating and providing human resources. Information on the full program underlying each category can quickly be supplied to the subcommittee by the ARRL.

(1) *Monitoring:* resources include formal programs to monitor amateur radio bands through the Amateur Auxiliary program with the FCC (P.L. 97–259), and also to help with radiolocation through direction finding. The monitoring process also takes place on international bands through our International Amateur Radio Union Monitoring System;

(2) *Communication*: resources include long-range (HF and satellite) and short-range (VHF/UHF) communications at our headquarters that provide radio amateurs and short wave listeners worldwide with news briefs or emergency bulletins. The National Traffic System (NTS) is a network that practices relaying messages from amateur station to amateur station, and other amateur nets such as the International Assistance and Traffic Net (IATN), The Maritime Mobile Net (MMN), The Intercontinental Traffic Net (ITN) and the Mobile Emergency and County Hunters Net. These nets essentially operate like large open party lines on a particular frequency that can be accessed by those in need. There is also a large number of data networks using packet and digital modes operated by many Amateur Radio emergency groups.

(3) *Human Resources:* The Amateur Radio Service has extensive human resources capabilities in telecommunications and particularly in radio. Some amateurs of military age are already serving. We will continue to study how best to match individual Amateur Radio operators to specific national needs. Those currently available for voluntary service or employment can be identified starting with some ARRL volunteer and "field appointment" data bases.

PART V. RECENT INITIATIVES

Today, the Amateur Radio community is in a State of serious—some might even say urgent—contemplation. We are reviewing how our longstanding and successful volunteer service might continue to provide a high level of communications support in this changing world. We also wish to be considered part of new initiatives where it makes sense to have a flexible, capable and nearly unbreakable "national party line" run by experienced and expert volunteer radio operators standing by to help out.

Our own association has already embarked on a number of initiatives to sustain the high level of service mentioned above. One such project, for example, is a review of the present roles of our short-wave radio station W1AW and its bulletins, the National Traffic Service and the various Amateur Radio networks we sponsor. Part of that effort will also include a review of our procedures for monitoring and reporting suspicious on-the-air activities, as well as international aspects of Amateur Radio disaster communications.

We have also been tentatively contacted by certain computer network security groups for preliminary discussions on whether or not Amateur Radio could be used to help provide supplementary communication to help restore an Internet collapse. Moreover, we continue to be available to consult with various government and private entities such as the U.S. Office of Homeland Security, the FCC, FBI, FEMA, NCS, Red Cross, Salvation Army and State and local governments to assess their needs for new communications support that could be fulfilled by amateurs.

In the absence of specific legislation, we currently have no specific recommendations for the role of Amateur Radio in the NetGuard or any other refinement of our nation's telecommunications system that evolves from the work of this committee. We hope that this testimony will provide sufficient food for thought that committee members or staff will not hesitate to contact our association for any specific information necessary to help you be sure that our long-standing and successful emergency communication backup remains available to all Americans.

Thank you for your attention, and best of luck considering this most difficult topic. The ARRL will be happy to answer any additional questions on Amateur Radio and its role in emergency communication.

PREPARED STATEMENT OF THE UNITED TELECOM COUNCIL

The United Telecom Council (UTC) appreciates this opportunity to provide a statement for the record to the Subcommittee concerning technology issues stemming from the events of September 11, 2001. UTC's statement will focus on telecommunications technology needs of the Nation's critical infrastructure (CI) industries, which have come into sharper focus since the attacks on our society.

INTRODUCTION

Since its inception in 1948, UTC has been the national representative for the nation's electric, gas, water and steam utilities and natural gas pipelines on telecommunications issues, both internal and competitive, and networking issues. Nearly 1,000 such entities are direct members of UTC, ranging in size from large combination electric-water-gas utilities serving millions of customers, to smaller rural electric cooperatives and water districts serving only a few thousand customers each.

Seven national associations are members of UTC, including: the American Gas Association, American Public Power Association, American Water Works Association, Association of Edison Illuminating Companies, Edison Electric Institute, Interstate Natural Gas Association of America, and the National Rural Electric Cooperative Association. This affiliation extends our reach to virtually every CI company in North America.

As part of our federation mission, UTC spearheads the Critical Infrastructure Communications Coalition (CICC). CICC is a policy-focused group which recognizes the commonality of interests among all critical infrastructure industries—energy, water, railroads, petroleum and natural gas production, and oil pipelines—in providing and maintaining the nation's safe, efficient and reliable delivery of essential public services. In addition to the aforementioned organizations, CICC enjoys the support of the Association of American Railroads, the American Petroleum Institute, the National Association of Water Companies, and the Association of Oil Pipe Lines.

USE OF TELECOMMUNICATIONS

While our membership is both broad and diverse, these critical infrastructure entities have at least one common need: they rely on wireless, broadband and other communications systems that they both own and manage—separate and apart from the public telecommunications networks—for real-time control of their systems, as well as for repair and restoration efforts in emergencies.

In addition, the energy, water and railroad industries have unique operational needs that make consistent and immediate access to spectrum a necessity. Disruptions to these industries' communications capabilities through sabotage or otherwise threatens public health, safety and community stability. The safe and reliable operation of the nation's critical infrastructure depends on access to radio spectrum and protection of spectrum-based systems from interference and disruption. While the private internal radio systems these industries maintain may be discrete to their particular company and service territories, this does not preclude the operational interdependencies of the essential public services they provide.

SUBCOMMITTEE ISSUES

One of the questions posed by the Subcommittee focused on the communications services and information technologies that were most helpful and effective on September 11 and the aftermath. Interestingly, it was the lesser-known and somewhat "lower-tech" systems that remained in service. While public cellular and personal communications service (PCS) networks were overloaded completely, thus rendered useless to all users, Consolidated Edison's private land mobile radio (PLMR) system remained operational and provided critical communications among mobile units immediately after the attacks.

Most PLMR systems are used primarily for two-way voice and some data communications using a combination of heavy-duty mobile (vehicle-mounted) and portable (hand-held) equipment. Such systems are licensed to the critical infrastructure entity and are built and maintained by them. It is not unusual that such utility-built systems remain operational in times of emergency—they are designed specifically for that purpose, since restoration of power (both electrical and natural gas) and the safety of water systems are vital needs at such times.

The Subcommittee asks whether a corps of scientists and technologists should be established for emergency purposes. Given the rate of technological change, the wide range of possible services to be included in such an effort, and the increasing specialization among the sciences and technology, establishment of such a corps on an

independent basis appears overwhelming. However, a series of data bases for various purposes related to safety and security might accomplish the Subcommittee's goals at a reasonable cost. One data base might include experts across the country in various areas of science and technology, along with their areas of expertise. In the telecommunications field, a data base of CI entities and their systems, including coverage area, types of equipment (whether wireless or fiber-based) and frequencies used, could help to identify sources of emergency communications coverage.

CHALLENGES TO CRITICAL INFRASTRUCTURE TELECOMMUNICATIONS

An examination of the State of CI communications systems, however, would reveal challenges to a nationwide, interoperable emergency communications network. CI entities use frequencies across a wide range of licensed and unlicensed bands; however, systems are most often found in the 150–512 MHz PLMR frequency bands and 800/900 MHz PLMR frequency pools. Telemetry systems are often found on the 902–928 MHz and 2.4/5 GHz unlicensed bands, and many vital control and monitoring systems on the 928–959 MHz Multiple Address Service (MAS) bands. Many utilities network base stationsites together using microwave links from 2 GHz to 19 GHz or higher. Each of these bands has a slightly different regulatory structure. Importantly, all of these bands are shared with non-CI users.

1. COMMUNICATIONS AND INFORMATION TECHNOLOGY PROBLEMS

Lack of Adequate Spectrum

In accordance with the 1997 Congressional directive, the Federal Communications Commission (FCC) determined in November 2000 that CI non-commercial, internal wireless services should be classified as "public safety radio services." [1] However, the FCC has not identified any spectrum to be made available for such entities, and has not made these entities eligible for traditional public safety (i.e., police and fire) spectrum. Such an exemption is meaningless without access to spectrum. Moreover, the FCC in its Balanced Budget Act (BBA) Decision stated that it believes that it retains the authority to allocate "Public Safety" spectrum according to the former, traditional Public Safety definition, which excludes CI. UTC opposed this conclusion in general.[2]

Among the most serious communications problems of PLMR users is the increasing congestion on various frequency bands, causing harmful interference to critical systems and communications. Notwithstanding the FCC's public safety radio services determination for critical infrastructure, UTC has noted often that adjacent channel interference remains a threat to the safe and reliable operation of utilities and pipelines. As private wireless spectrum grows more congested, there are increasing reports of harmful interference to energy activities, including critical power restoration.

Lack of Protected Spectrum

Additionally, CI has no exclusively allocated or protected spectrum for its essential communications functions. Rather, these entities share many widely dispersed frequency bands with all private wireless users. This means that CI must share access to frequencies critical to operational control with such incompatible users as delivery services, plumbing dispatch and taxicabs—any business or industry using two-way radio or wireless data.

This situation is not exclusive to voice communications, but also is relevant to the 900 MHz bands used for wireless control systems. Instances of interference severe enough to require equipment modifications, or dialog with users generating interference, are frequent. In urban areas and adjacent communities, CI competes with paging services, financial systems, security systems, and other users and finds itself constrained by available resources and the absence of unoccupied spectrum in the MAS band.

2. UNIQUE CHARACTERISTICS OF PRIVATE WIRELESS SYSTEMS

The need for reliable production and transmission led CI to become some of the first users of wireless telecommunications some 50 years ago. Utilities now rely heavily on radio communications systems that they must own and operate themselves to ensure that they meet their needs at all times. Because CI considers the

---

[1] Implementation of Sections 309(j) and 337 of the Communications Act of 1934 as Amended, WT Docket No. 99–87, *Report and Order and Further Notice of Proposed Rulemaking*, 15 FCC Rcd 22309 (2000), at 64 ("BBA decision").

[2] *See, e.g.,* Petition For Reconsideration of the United Telecom Council, WT Docket No. 99–87 (filed February 1, 2001), at 6.

reliable—both constant and consistent—provision of power and water as its primary mission, CI by its very nature, operated the most helpful and effective communications systems available during the early aftermath of the September 11, 2001 tragedy.

Though a catastrophic event such as that of September 11, 2001 is not a normally contemplated contingency, CI systems are designed to withstand severe communications challenges. Therefore, CI entities cannot rely on commercial service providers to meet their unique and varied needs. For instance, control of the communications system is very critical during heavy storms and other serious weather events. In these situations, commercial systems become saturated with traffic or even weather-damaged, and, as a result, experience outages. Thus, discussions of priority access for public safety or CI do not offer a realistic solution. Nor do commercial networks, built to provide service to the largest concentrations of population, provide the complete coverage that utilities must have to restore critical services anywhere within their service areas.

In contrast, private communications networks ensure that utility systems are brought back on line in the most timely manner possible; for example, power utility wireless systems are often located at or near electrical substations, and thus can remain "on the air" when commercial, and even traditional public safety, systems fail.

3. PROPOSED PRIVATE SECTOR CORPS OF SCIENTIST AND INFORMATION SPECIALISTS

In reference to the proposed corps of scientists and information specialists, UTC suggests that part of the Federal Government's effort should be, in concert with industry, compilation of an up-to-date data base on the locations, frequencies and types of equipment used in critical infrastructure internal telecommunications systems. CI also needs a small, exclusive spectrum allocation that would be protected and uniform across the country, allowing for introduction of advanced technology, interoperability among systems and greater productivity in times of national or natural disaster.

The Subcommittee should be aware that utilities and other CI entities across the country are currently engaged in analyses of their vulnerabilities, including those of internal communications systems. UTC's Homeland Security Task Force is aiding our members in this process. Much of the discussion of vulnerabilities of CI have centered mostly on the potential destruction or damage to the physical infrastructure itself. However, physical damage or plant infiltration would not be necessary should the communications networks that control and maintain that physical plant be disabled.

The events of September 11 have brought an entirely new focus to efforts to provide adequate protection of these vital communications networks. UTC formed its Homeland Security Task Force to address this issue. Our efforts are aimed at providing a source of additional information for ALL CI organizations relating to the security of their communications systems and the potential role of those communications systems in homeland security. One of the task force's first projects has been the development of a CI communications security audit checklist, so that our members may conduct an internal analysis of their operations to determine what additional protection measures are needed.

Communications networks form the backbone of all CI industries in this country, including railroads, electric and gas utilities, gas and oil pipelines, energy production and water systems. Thus, the vulnerabilities of one radio system would be common to all the CI industries. An attack on one could easily be translated into an attack on all others. Deregulation and the continued growth in demand for reliable critical infrastructure service will inevitably result in increased dependence on the spectrum-based systems. Therefore, we would recommend that a data base of CI communications networks should range across all critical infrastructure industries.

Finally, one important point is worth immediate note. The National Telecommunications and Information Administration (NTIA) is now completing a congressionally mandated study of radio spectrum use by critical infrastructure entities. The study report is due to be submitted to Congress in late December. This report and its recommendations will be crucial to the future safety and security of the nation's energy, water and transportation infrastructure. While the study was undertaken as a result of legislation passed by Congress last year, it now takes on increased significance given the events of September 11 and the Executive Order on Critical Infrastructure Protection in the Information Age, signed by President Bush on October 16, 2001. UTC looks forward to discussing the study and its recommendations with the Subcommittee as part of its important work in this area.

UTC appreciates the opportunity to provide this statement to the Subcommittee on Science, Technology, and Space. We would be pleased to provide any additional material that the Subcommittee may require for its deliberations.

○